jurisprudência.pt

Tribunal da Relação de Évora
Processo nº 379/21.0T8FAR.E1

Relator: CRISTINA DÁ MESQUITA
Sessão: 12 Julho 2023
Votação: UNANIMIDADE

HOMEBANKING **AUTORIZAÇÃO** **TRANSFERÊNCIA DE FUNDOS**

FRAUDE

Sumário

1 – De acordo com o regime previsto no D/L n.º 317/2009, de 30.10 (RSP) que veio regular a atividade dos prestadores de serviço de pagamento que tenham como atividade principal a prestação de serviços de pagamento a utilizadores desses serviços, o consentimento para a execução da operação tem de ser dado pelo ordenante nos termos acordados e terá que ser prévio à operação, salvo convenção em contrário entre as partes. Não tendo sido prestado nos termos referidos, a operação considera-se não autorizada.
2 – A execução da ordem pressupõe ainda que o cliente tenha sido autenticado pelo prestador do serviço através de um procedimento que lhe permite verificar a identidade de um utilizador de serviços de pagamento ou a validade da utilização de um instrumento de pagamento específico, incluindo a utilização das credenciais de segurança personalizadas do utilizador.
3 – Quando o utilizador do serviço de pagamento negue ter dado consentimento para a execução da operação, o ónus de prova da existência de consentimento, da verificação do procedimento de autenticação, registo e contabilidade da operação e de que esta não foi afetada por avaria técnica ou qualquer outra deficiência recai sobre o prestador do serviço.
(Sumário da Relatora)

Texto Integral

Apelação n.º 379/21.0T8FAR.E1

(2.ª Secção)

Relatora: Cristina Dá Mesquita

Acordam os Juízes do Tribunal da Relação de Évora:

I. RELATÓRIO
I.1.
Banco (…), SA, réu nos autos que lhe foram movidos por (…) – Companhia de (…) do Algarve, Lda. interpôs recurso da sentença que foi proferida pelo Juízo Central Cível de Faro, Juiz 3, do Tribunal Judicial da Comarca de Faro, o qual julgou a ação parcialmente procedente e, em consequência, condenou o réu a pagar à autora a quantia de cinquenta e quatro mil, trezentos e noventa e dois euros e noventa cêntimos (€ 54.392,90), acrescida de 10% e de juros de mora, à taxa legal dos juros civis, contados desde 16 de julho de 2020, até efetivo e integral pagamento.

Na ação a autora pedira a condenação do réu a pagar-lhe a quantia de € 61.064,89 a título de indemnização por danos patrimoniais, acrescida de juros calculados à taxa legal, contados desde a citação e até integral pagamento, bem como o pagamento da quantia de € 3.000,00, a título de indemnização por danos não patrimoniais, acrescida de juros calculados à taxa legal e contados desde a data da citação e até integral pagamento.
Para tal desiderato, a autora alegou que foi titular de uma conta bancária na agência do réu e que no dia 16 de julho de 2020 tentou variadas vezes iniciar a sessão na plataforma *on line* disponibilizada pelo banco réu e, quando o conseguiu, verificou que haviam sido realizados pagamentos e transferências bancárias, num total de € 56.990,00, para destinatários que desconhece e as quais não autorizou. Mais alegou que de imediato se dirigiu à sucursal do Banco réu, em Faro, onde a informaram tratar-se de fraude, aconselhando-a a apresentar queixa; reclamou os montantes alvo das operações efetuadas tendo o banco réu devolvido apenas o montante de € 2.597,10.
Na sua contestação o réu defendeu-se por exceção, invocando a exceção dilatória inominada de violação do princípio da adesão ao processo crime que foi instaurado pelos factos supra descritos, e por impugnação, alegando que as transferências e pagamentos foram validados com as credenciais da autora e que cumpriu todas as obrigações técnicas de segurança, sendo a autora responsável pela segurança física dos equipamentos e dos códigos de acesso e que ao fazer uso de um serviço através de um computador desprotegido e obsoleto violou os deveres que sobre si impendem.

I.2.

A recorrente formula alegações que culminam com as seguintes conclusões:
«I. A douta sentença proferida, pese embora a bondade da sua fundamentação e clareza expositiva e decisória, incorre e sofre, ao nível da apreciação da prova, de imprecisões, incorreções, contradições e notórios erros na apreciação da prova, não podendo tal ser relevado, sem que haja grave prejuízo para a justa composição do mérito da causa.
II **-** Existindo assim factos erroneamente dados como provados e não provados, não tendo a Douta Sentença, atendido à totalidade dos factos relatados pelas testemunhas no seu depoimento, no sentido de os atender ou afastar, ou seja, o Tribunal *a quo*, na análise conjugada e crítica da prova produzida, quer documental, quer testemunhal, incorreu em notório erro na apreciação da prova produzida, bem como das regras da experiência comum e da normalidade da vida.
III – Devem ainda ser aditados aos factos já dados como provados pelo Tribunal *a quo* o seguinte:
A) A operação de transferência e / ou pagamento de serviços só se deu após introdução do código rececionado no telemóvel da Autora, sem o qual a operação jamais teria ocorrido.
Este tão importante, fundamental e determinante facto, não se dá no sistema do Banco, mas sim na operacionalidade da Autora, o telemóvel é da Autora, junto da operadora que a Autora escolheu, sem que o Banco seja parte nessa relação contratual entre a Autora e a sua operadora de telemóvel. Após receção da mensagem com o código que foi visualizado apenas e só pela Autora e introduzido pela Autora é que ocorre a transferência. O Banco cumpre uma instrução de pagamento ou de transferência, quando estão reunidos todos os requisitos para tal. O que aconteceu.
B) Não obstante o facto provado em 23, o que é certo é que nos factos provados de 13 a 21, nunca foi referida intervenção direta da Autora na introdução do código de acesso que lhe chegou pelo seu telemóvel, código esse que apenas a Autora podia visualizar e introduzir na plataforma do Banco.
Assim:
C) Deve ser dado como provado no facto 13, que – às 11:15:46 a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.
D) Deve ser dado como provado no facto 14, que – às 11:29:02 a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.

E**)** Deve ser dado como provado no facto 15, que – às 11:31:48h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato continuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.
F) Deve ser dado como provado no facto 16, que – às 11:35:05h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.
G) Deve ser dado como provado no facto 17, que – às 11:39:02h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.
H) Deve ser dado como provado no facto 18, que – às 11:43:33h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.
I) Deve ser dado como provado no facto 19, que – às 11:46:00h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.
J) Deve ser dado como provado no facto 20, que – às 11:47:58h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.
K) Deve ser dado como provado no facto 21, que – às 11:58:22h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.
L) Deve ser dado como provado no facto 22, que – às 12:01:30h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.
IV – Factos que devem ser dados como provados, mas com merecimento de outra interpretação / outra “letra”:
A) Facto dado como provado em 10 dos factos provados, em que a própria gerente da Autora o confessa de maneira distinta – declarações de parte da Legal representante da Autora – ouvida a 20/10/2022 – gravação entre as 14:57:59h e as 15:39:28h – ao minuto 25.38 m e seguintes – Devendo em consequência ser dado como provado mas com indicação de 3 ou 4 tentativas.
B) O facto vertido em 34, foi devidamente explicado pelas testemunhas (…) –

ouvida a 19/10/2021 – entre as 15:48:04 H e as 16:48:47 H e (…) – ouvido a 19/10/2021 – entre as 16:50:27H e as 17:19:12H.
C) A apreciação e consideração do uso da palavra "fraude" foi feita assumindo que as palavras da Cliente, a ora Autora, eram verdadeiras e que esta não tinha tido qualquer intervenção do que aconteceu. Como já se referiu ao Balcão não se fazem apreciações técnicas que na realidade ocorrem na área Operacional e de Segurança do Banco.
Factos que tem que ser introduzidos e dados como provados.
A) E ainda como facto provado 44, que "A autora nunca questionou a operadora de telemóvel Vodafone sobre a possibilidade de clonagem ou acesso indevido ao seu telemóvel, no período em que ocorreram todas operações identificadas nos números 13 a 22 dos factos dados como provados".
B) Deve ser dado como Facto provado e passar a constar da factualidade assente o seguinte facto: A - *a Autora teve acesso às recomendações de segurança feitas pelo réu Banco referentes ao acesso ao seu portal para uso do serviço "homebanking "*;
VI – Factos que foram dados como provados e que não estão provados por total ausência de prova:
A) Facto dado como provado em 11 dos factos provados - Não resulta de qualquer prova produzida nos autos, que a gerente da Autora ao aceder a plataforma do Banco lhe tenha aparecido "uma página em branco".
Como se sabe a prova tem por função a demonstração da realidade dos factos alegados - artigos 341º do CC e 410º do CPC.
B) O facto dado como provado em 27, embora alegado pela Autora, mas resultou não provado, nem documentalmente, nem testemunhalmente – artigos 341º do CC e 410º do CPC.
C) Os factos dados como provados em 28 e 29, terão que ser dados como não provados, uma vez que a Autora não fez qualquer prova, nem testemunhal, nem documental, do alegado. O facto de aos Banco caber uma parte do ónus da prova em ações com o objeto da presente, ónus de prova esses devidamente delimitados na lei, não é extensível a toda e qualquer prova, ou seja, à prova que cabe à autora fazer dos factos que alega. Não são todos enquadráveis no ónus do Banco. Em consequência os factos elencados não estão provados.
D) O facto 29 tem que ser dado como não provado uma vez que apropria operadora Vodafone – fls. 122/123 e 318 – afirma que não foi emitida segunda via do cartão inserido no telemóvel ou que exista noticia de ter sido clonado esse cartão, o que permitiria a receção daquelas mensagens por outro aparelho. Não tendo existido clonagem de cartão, não tendo também a Autora referido qualquer anomalia no seu telemóvel, e tendo sido as mensagens

rececionadas no telemóvel da Autora introduzidas uma a uma, desencadeando as diversas operações realizadas na conta, não pode este facto resultar provado.
F) Bem esteve o Tribunal *a quo* ao dar como não provado que apenas a gerente da A. tinha na sua posse as credenciais que lhe permitiam o acesso à plataforma informática do Banco – sistema de Homebanking, podendo as mesmas ser usadas com o conhecimento de terceiros.
G) Estes factos não provados são essenciais para a figura da responsabilidade do próprio lesado, nos termos do disposto no artigo 570.º do Código Civil.
H) Não resultou provado nos autos que a A. não tenha contribuído, também, para o que veio a acontecer sobre a sua conta bancária.
VII – Factos que merecem apreciação diferente e que em conjugação com os demais levam
à absolvição do Banco Recorrente
A) Relevante para, em sede de apreciação de mérito se poder apreciar ou não da existência de comportamento culposo ou negligente, e respetivo grau de culpa, por parte da Autora, que levaram às transferências efetuadas, bem como para efeitos de apreciação repartição do ónus da prova, igualmente deverá ser dado como provada a seguinte factualidade:
B) Que foram cumpridos todos os mecanismos de processamento e validação de segurança utilizados pelos sistemas informáticos do Banco;
C) Que foram respeitados pelo Banco todas as regras de segurança e de proteção do cliente, que lhe são exigíveis em termos de segurança relativamente à utilização do homebanking;
D) A Autora, voluntariamente, facultou os seus dados pessoais acedendo sucessivamente à área de homebanking, mesmo que avisada de que existiam e existem todos os dias tentativas de fraude, conforme avisos do Banco, que a Autora não impugnou porque os conhecia, mas preferiu ignorá-los.
E) Que o site de homebanking do Banco não sofreu, no período em que foram feitas as transferências da conta do Autor nenhum ataque informático ou qualquer tentativa de intrusão ou utilização ilícita por parte de terceiros.
F) O caso da Autora, trazido ao Tribunal, não se enquadra na definição e requisitos legais do Phishing;
G) O caso da Autora, trazido ao Tribunal não se enquadra na definição e requisitos legais do Pharming;
H) Todos os movimentos efetuados na conta da Autora estão devidamente documentados no sistema informático do Banco e juntos aos autos;
I) O Banco é alheio à relação contratual da Autora com a operadora de telefone que lhe facultou o acesso aos códigos de acesso, que a Autora introduziu no sistema do Banco e desencadeou as operações ocorridas na

conta.
J) A Autora tem total responsabilidade na concretização das operações, porquanto as mensagens iam para o seu telemóvel e daí é que eram conhecidas para serem digitadas a partir do computador da Autora na plataforma do Banco.
K) Existe a Culpa do Lesado, a culpa da Autora é manifesta. Tal como já se identificou *supra*, as diversas insistências da Autora em entrar na plataforma do Banco, bem conhecendo os inúmeros avisos de possibilidade de fraudes nesses mesmos acessos, conjugado com os presentes factos não provados, de que a gerente da Autora poderá não ser a única pessoa conhecedora das credenciais de acesso à plataforma do Banco, fazem o Banco Recorrente entender que é inquestionável a culpa do lesado, não cabendo ao Banco suportar uma condenação, pelo que recorre dela.
L) Quanto aos pagamentos de serviços, e conforme foi a Autora informada teria esta que procedam ao registo de reclamação sobre os montantes da alegada fraude, através do site da entidade de Pagamento (...) em https://onlinepaymentplatform.com/en/contact" (cfr. doc. de fls. 29/30, cujo teor se dá por reproduzido), o que a Autora não fez. Cabendo à A. a responsabilidade de procurar junto desta entidade de recuperar o dinheiro que alegadamente perdeu.
Devendo nesta parte também o Banco ser absolvido do pagamento de tais quantias.
M) A testemunha do Banco, quando se deslocou às instalações da A., bem viu os Códigos de acesso à plataforma do Banco escritos numa folha, que não os documentos originais do Banco, que haviam sido em tempos entregues à gerente da Autora. Ora, tal como os viu o Colaborador do Banco identificado, também bem os poderia ter visto qualquer outra pessoa que tivesse acesso às instalações da Autora.
N) O sistema de segurança do réu consegue identificar as movimentações não consentidas pelo titular da conta resultantes da intromissão de "piratas informáticos"; o sistema do Banco identifica, ou assume como não consentidas as operações que não reúnam os requisitos legais e impostos de acesso à conta. Estando todos os requisitos reunidos, como é o caso dos acessos ocorridos na conta da Autora, não se pode dar qualquer bloqueio. O Banco não tem como identificar antecipadamente as intenções ou não dos seus clientes, senão por via do cumprimento de um conjunto de passos que se consubstanciam na introdução de diversos códigos e informações, tal como ocorreu.
O) Não se pode afastar a culpa do lesado, ou seja, da Autora porquanto não se podendo ignorar tão importante ferramenta que foi o telemóvel da Autora,

usado pela sua gerente.
P) Também por esta via, não pode ser o Banco carregado de responsabilidade legal, quando não a tem, como à frente melhor se voltará a falar, pelo que entende o Banco não poder deixar de recorrer da sentença proferida, esperando melhor apreciação dos factos e do direito, por parte do Venerando Tribunal da Relação.
Q) Com efeito, o que decorre do que foi contratualizado com o Banco e o que decorre, de tais cláusulas contratuais e do disposto no artigo 67.° do DL 317/2009 é que é sobre o cliente/utilizador que incumbe a obrigação de tudo fazer para que os elementos de segurança não cheguem ao conhecimento de terceiros.
R) A Autora não cuidou de o fazer, chamando a sua si a responsabilidade pela sua relação com a Operadora de Telemóvel Vodafone.
S) Pelo que violou não somente as condições gerais de utilização dos canais telefónicos, internet e SMS, constantes do contrato de *homebanking* celebrado com o Banco, nomeadamente o n.° 2/b), referente às condições de acesso, que impede que o cliente permita a sua utilização por terceiros do código multicanal, do código do utilizador e da chave de confirmação por SMS.
T) Bem como violou a Autora o disposto non artigo 67.º do DL n.° 317/2009, de 30 de outubro, nomeadamente as obrigações do utilizador de serviços de pagamento bem como do artigo 72.º do mesmo diploma legal, referente à responsabilidade do ordenante por operações de pagamento não autorizadas.
U) O Banco provou que o cliente fez uma utilização imprudente, negligente e descuidada do serviço de *homebanking* o que afasta a responsabilidade do Banco pelos movimentos efetuados por terceiros.
V) Pelo que ilidiu a presunção de culpa prevista no artigo 799.º, n.° 1, do CC, e que o Tribunal *a quo* aplicou erradamente.
W) O Douto Tribunal, aplicou assim erradamente, as referidas disposições legais, bem como a aplicação do disposto no regime jurídico dos serviços de pagamento e da moeda eletrónica.
Nestes termos e nos mais de Direito que Vossas. Excelências Doutamente suprirão, requer:
Seja reconhecida a razão do ora recorrente, atendida a impugnação da matéria de facto efetuada, bem como revogada a douta sentença proferida, nos termos referidos, com as demais consequências legais;
Aguarda-se prolação de Acórdão, que revogue a decisão proferida, absolvendo o Banco e
fazendo o Venerando Tribunal da Relação Justiça!».

I.3.
Não houve resposta às alegações de recurso.
O recurso foi recebido pelo tribunal *a quo*.
Corridos os vistos em conformidade com o disposto no artigo 657.º, n.º 2, do Código de Processo Civil, cumpre decidir.

II. FUNDAMENTAÇÃO
II.1.
As conclusões das alegações de recurso (cfr. *supra* I.2) delimitam o respetivo objeto de acordo com o disposto nas disposições conjugadas dos artigos 635.º, n.º 4 e 639.º, nº 1, ambos do CPC, sem prejuízo das questões cujo conhecimento oficioso se imponha (artigo 608.º, n.º 2 e artigo 663.º, n.º 2, ambos do CPC), não havendo lugar à apreciação de questões cuja análise se torne irrelevante por força do tratamento empreendido no acórdão (artigos 608.º, n.º 2, e 663.º, n.º 2, do CPC).

II.2.
No caso as questões que importa decidir são as seguintes:
1 – Impugnação da decisão de facto.
2 – Reapreciação do mérito da decisão.

II.3.
FACTOS
II.3.1.
O Tribunal de primeira instância julgou provada a seguinte factualidade:
«1 - A autora é uma sociedade que tem por objeto a colocação de isolamentos e revestimentos na indústria da construção civil (cfr. certidão a fls. 21/23, cujo teor se dá por reproduzido).
2 - Era titular da conta de depósitos à ordem com o n.º (…), domiciliada junto do réu na Sucursal Sotavento Negócios com o código n.º (…).
3 - Há pelo menos 10 anos a gerente da autora solicitou ao réu a adesão ao serviço por este prestado através de plataforma eletrónica (área empresa do Banco) que lhe permitia aceder aos movimentos daquela conta e realizar pagamentos e transferências. 4 - Para o efeito foi-lhe fornecido pelo réu o Certificado Digital, composto por um Código de Adesão com 15 dígitos e que foi instalado no computador que a autora possuía na sua sede, o Código de Utilizador e a Password de acesso.
5 - Para a entrada na referida plataforma era ainda pedida a introdução, de forma aleatória, de duas posições do Número de Identificação Fiscal da

autora.
6 - Para confirmação de operação de pagamento ou transferência era pedida a introdução de um Código de Autorização, o qual era enviado para o telemóvel com o n.º (…), que fora indicado pela gerente da autora ao réu.
7 - A gerente da autora mantinha na sua posse as credenciais de acesso e utilizava quase diariamente aquela plataforma para consultar movimentos da conta bancária, efetuar pagamentos ou transferências bancárias.
8 - No dia 16.07.2020, por volta das 11h03m39ss, a gerente da autora iniciou o acesso à referida plataforma através do computador existente na sede da empresa, que utilizava o sistema operativo Windows 7, tendo como browser o Internet Explorer 11.
9 - Após a gerente da autora introduzir o Código de Utilizador (…), a Password de acesso e dois números do NIF apareceu no ecrã do computador uma página em branco que a impossibilitou de efetuar qualquer operação.
10 - A gerente da autora realizou duas tentativas de entrar novamente na plataforma, desligando e voltando a ligar o computador.
11 - Após voltar a aceder à plataforma, introduziu o Código de Utilizador, a Password e dois números do NIF, voltando a aparecer uma página em branco.
12 - Supôs que o serviço estaria indisponível e foi almoçar.
13 - Pelas 11:15:46h foi efetuado o Envio de Ficheiros PSM no valor de € 2.997,00 e para confirmar esta operação foi emitido pelo réu, às 11:13:39h, um Código de Autorização para o n.º de telemóvel (…) (com o seguinte conteúdo: “MBCP Emp – Envio Ficheiro – Cta Deb: … – Tipo: PSM – N. reg: 3 – Mont.: 2.997,00 EUR – Data Proc: 16/07/2020 – Codigo Autorizacao: …).
14 - Pelas 11:29:01h foi efetuada uma Transferência Nacional no valor de € 1.000,00 para o IBAN PT (…), com o beneficiário “(…)”, o descritivo “PAGAMENTOS” e para confirmar esta operação foi emitido pelo réu às 11:27:32h um Código de Autorização para o n.º de telemóvel … (com o seguinte conteúdo: “MBCP Emp – Transferencia Nacional – Cta Debito: … – IBAN Destino: PT … – Montante: 1.000,00 EUR – Codigo Autorizacao: …).
15 - Pelas 11:31:48h foi efetuada uma Transferência Nacional no valor de € 9.999,00 para o IBAN (…), com o beneficiário “(…)”, o descritivo “PAGAMENTOS” e para confirmar esta operação foi emitido pelo réu, às 11:30:58h, um Código de Autorização para o nº de telemóvel … (com o seguinte conteúdo: “MBCP Emp – Transferencia Nacional – Cta Debito: … – IBAN Destino: PT (…) – Montante: 9.999,00 EUR – Codigo Autorizacao: …).
16 - Pelas 11:35:05h foi efetuada uma Transferência Nacional Imediata no valor de € 9.998,00 para o IBAN PT (…), com o beneficiário “(…)”, o descritivo “PAGAMENTOS” e para confirmar esta operação foi emitido pelo réu, às 11:34:25h, um Código de Autorização para o n.º de telemóvel … (com o

seguinte conteúdo: “MBCP Emp – Transferencia Nacional – Cta Debito: … – IBAN Destino: PT (…) – Montante: 9.998,00 EUR – Codigo Autorizacao: …).
17 - Pelas 11:39:02h foi efetuado um pagamento de serviços no valor de € 999,00 para a entidade 21800 – (…) com a referência (…) e esta transação foi confirmada com o Código de Autorização enviado por SMS, às 11:38:17h, para o n.º de telemóvel … (com o seguinte conteúdo: “MBCP Emp – Pagamento Servicos – Cta/Cartao: … – Entidade: … – Referencia: (…) – Montante: 999,00 EUR – Codigo Autorizacao: …).
18 - Pelas 11:43:33h foi efetuada uma Transferência Nacional Imediata no valor de € 10.000,00 para o IBAN PT (…), tendo com o beneficiário “(…)”, o descritivo “PAGAMENTOS” e para confirmar esta operação foi emitido pelo réu, às 11:42:55h, um Código de Autorização para o n.º de telemóvel … (com o seguinte conteúdo: “MBCP Emp – Transferencia Nacional – Cta Debito: … – IBAN Destino: PT (…) – Montante: 10.000,00 EUR – Codigo Autorizacao: …).
19 - Pelas 11:46:00h foi efetuada uma Transferência Nacional no valor de € 10.000,00 para o IBAN PT (…), com o beneficiário “(…)”, o descritivo “PAGAMENTOS” e para confirmar esta operação foi emitido pelo réu, às 11:45:14h, um Código de Autorização para o n.º de telemóvel … (com o seguinte conteúdo: “MBCP Emp – Transferencia Nacional – Cta Debito: … – IBAN Destino: PT (…) – Montante: 10.000,00 EUR – Codigo Autorizacao: …).
20 - Pelas 11:47:57h foi efetuado um pagamento de serviços no valor de € 998,00 para a entidade (…) – (…), com a referência (…) e esta transação foi confirmada com o Código de Autorização enviado por SMS, às 11:47:20h, para o n.º de telemóvel … (com o seguinte conteúdo: “MBCP Emp – Pagamento Servicos – Cta/Cartao: … – Entidade: … – Referencia: … – Montante: 998,00 EUR – Codigo Autorizacao: …).
21 - Pelas 11:58:21h foi efetuado um pagamento de serviços no valor de € 999,00 para a entidade (…) – (…) com a referência (…) e esta transação foi confirmada com o Código de Autorização enviado por SMS, às 11:57:47h, para o n.º de telemóvel … (com o seguinte conteúdo: “MBCP Emp – Pagamento Servicos – Cta/Cartao: … – Entidade: … – Referencia: … e – Montante: 999,00 EUR – Codigo Autorizacao: …).
22 - Pelas 12:01:29h foi efetuada uma Transferência Nacional no valor de € 10.000,00, para o IBAN PT (…), com o beneficiário “(…)”, o descritivo “PAGAMENTOS” e para confirmar esta operação foi emitido pelo réu, às 12:00:09h, um Código de Autorização para o n.º de telemóvel … (com o seguinte conteúdo: “MBCP Emp – Transferencia Nacional – Cta Debito: (…) – IBAN Destino: PT (…) – Montante: 10.000,00 EUR – Codigo Autorizacao: …).
23 - Os pagamentos e transferências referidos em 13 a 22 foram efetuados com utilização do Código de Utilizador da autora, confirmados com duas

posições aleatórias do NIF e com a introdução dos Códigos de Autorização enviados por “SMS” para o telemóvel n.º (…).
24 - Pelas 11:18:41h foi tentada uma Transferência Nacional, no valor de € 10.000,00 para o IBAN PT (…), com o beneficiário “(…)” e para confirmar esta transação foram enviados pelo réu, às 11:19:00h, dois Códigos de Autorização para o n.º de telemóvel (…), os quais não foram introduzidos na plataforma (com os seguintes conteúdos: “MBCP Emp – Transferencia Nacional – Cta Debito: (…) – IBAN Destino: PT (…) – Montante: 10.000,00 EUR – Codigo Autorizacao: …” e “MBCP Emp – Transferencia Nacional – Cta Debito: (…) – IBAN Destino: PT (…) – Montante: 10.000,00 EUR – Codigo Autorizacao: …).
25 - Foi tentado o Envio de Ficheiros PSM, no valor de € 1.998,00, com Códigos de Autorização enviados para o n.º de telemóvel (…), pelas 12:07:04h (com o seguinte conteúdo: “MBCP Emp – Envio Ficheiro – Cta Deb: … – Tipo: PSM – N. reg: 2 – Mont: 1.998,00 EUR – Data Proc: 16/07/2020 - Codigo Autorizacao: …), pelas 12:07:08h (com o seguinte conteúdo: “MBCP Emp – Envio Ficheiro – Cta Deb: … – Tipo: PSM – N. reg: 2 – Mont: 1.998,00 EUR – Data Proc: 16/07/2020 – Codigo Autorizacao: …), pelas 12:08:04h (com o seguinte conteúdo: “MBCP Emp – Envio Ficheiro – Cta Deb: (…) – Tipo: PSM – N. reg: 2 – Mont: 1.998,00 EUR – Data Proc: 16/07/2020 – Codigo Autorizacao: …) e pelas 12:08:05h (com o seguinte conteúdo: “MBCP Emp – Envio Ficheiro – Cta Deb: … e – Tipo: PSM – N. reg: 2 – Mont: 1.998,00 EUR – Data Proc: 16/07/2020 – Codigo Autorizacao: …).
26 - Estas operações não foram realizadas porque não foram introduzidos na plataforma os Códigos de Autorização que haviam sido enviados para o telemóvel n.º (…).
27- Pelas 15h50m58ss a gerente da autora acedeu à plataforma e conseguiu verificar que haviam sido realizadas as transferências e os pagamentos referidos em 13 a 22.
28 - Os quais não foram por si efetuados, nem consentidos, desconhecendo os respetivos destinatários.
29 - Nesse momento constatou que havia recebido no seu telemóvel várias mensagens contendo os Códigos de Autorização para realização dessas operações que não havia utilizado.
30 - Perante o referido em 28 deslocou-se à Sucursal Sotavento Negócios do réu, onde chegou por volta das 16h00m, em estado de ansiedade e quase pânico.
31 - Ao contar o sucedido os colaboradores do banco réu comunicaram-lhe que se tratava de um caso de fraude e que deveria apresentar queixa.
32 - Pelas 14h37m daquele dia havia sido enviado um e-mail por (…), do Gabinete de Gestão Aplicacional e Segurança do réu, para a Sucursal

Sotavento Negócios, referindo que na sequência de um alerta Paywatch (SIBS) verificaram-se 3 transações suspeitas na conta da autora, solicitando o contato do cliente e que se aferisse se se tratavam de transações fidedignas (cfr. doc. de fls. 23vº/24, cujo teor se dá por integralmente reproduzido).
33 - O qual não obteve resposta por parte dos colaboradores da Sucursal Sotavento Negócios.
34 - Após o referido em 31 os colaboradores da Sucursal Sotavento Negócios bloquearam os movimentos na conta bancária e pelas 16h47m comunicaram que se tratava de fraude e solicitaram a devolução de todas as transferências realizadas naquele dia (cfr. doc. de fls. 24 verso, cujo teor se dá por integralmente reproduzido).
35 - Nesse mesmo dia a gerente da autora apresentou reclamação junto do réu relativa aos débitos realizados sem o seu consentimento (cfr. doc. de fls. 25, cujo teor se dá por integralmente reproduzido).
36 - E apresentou denuncia na Divisão Policial de Faro da Polícia de Segurança Pública à qual foi atribuído o NUIPC … (cfr. doc. de fls. 25vº/26, cujo teor se dá por integralmente reproduzido).
37 - Em 28.07.2020 foi restituído à autora o montante de € 2.597,10.
38 - Em 11.09.2020 a autora enviou carta registada ao réu, solicitando a devolução do restante montante (cfr. doc. de fls. 26vº/28vº, cujo teor se dá por reproduzido).
39 - Em 11.11.2020 o réu respondeu referindo que "*não tem o Banco qualquer responsabilidade nas transações em causa, considerando que todos os mecanismos de processamento e validação utilizados encontram-se no Banco registados em nome da Sra. D. (…) e da (…) Algarve Lda., nomeadamente o Código de Adesão, o Certificado Digital, o Código de Utilizador, a Password, duas posições do Número Fiscal, número de telemóvel para a receção dos Códigos de Autorização com a identificação clara e inequívoca da operação a realizar e respetiva confirmação com esse código*" (cfr. doc. de fls. 29/30, cujo teor se dá por reproduzido).
40 - Referindo, ainda, que "*quanto aos pagamentos de serviços, e conforme oportunamente transmitido por contato telefónico, é necessário que procedam ao registo de reclamação sobre os montantes da fraude, através do site da entidade de Pagamento (…) em https://onlinepaymentplatform.com/en/contact* " (cfr. doc. de fls. 29/30, cujo teor se dá por reproduzido).
41 - O banco réu tem no seu site, à disposição dos clientes, diversos avisos de segurança e recomendações para acesso ao portal do banco e segurança no acesso ao portal de empresa, onde se detalham aspetos para prevenir fraudes.
42 - Alertando os clientes para eventuais tentativas de uso indevido dos dados dos clientes, páginas que têm semelhança com a do banco de entre outras.

II.3.2.
O Tribunal de primeira instância julgou não provada a seguinte factualidade:
«a) Apenas a gerente da autora tem acesso às credenciais que lhe permitem o acesso à plataforma informática.
b) Era impossível a utilização das credenciais sem o conhecimento da gerente da autora.
c) O réu efetuou o bloqueio das operações realizadas antes das 14h37m e das 16h00m.
d) O sistema de segurança do réu consegue identificar as movimentações não consentidas pelo titular da conta resultantes da intromissão de "piratas informáticos".
e) O computador utilizado pela gerente da autora encontrava-se vulnerável a ataques cibernéticos e era obsoleto.
f) A autora sofreu constrangimentos e transtornos devido à indisponibilidade na conta bancária dos montantes referidos em 13 a 22».

II.4.
Impugnação da decisão de facto
Neste plano o apelante defende o seguinte:
1 – Deve ser dado como provado no **facto 13** que – *às 11:15:46 a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência*;
- Deve ser dado como provado no **facto 14** que – *às 11:29:02 a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência*;
- Deve ser dado como provado no **facto 15** que – *às 11:31:48h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato continuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência*;
- Deve ser dado como provado no **facto 16** que – *às 11:35:05h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência*;
- Deve ser dado como provado no **facto 17** que – *às 11:39:02h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de*

movimentação cumpriu a instrução de transferência;
- Deve ser dado como provado no **facto 18** que – *às 11:43:33h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência*;
- Deve ser dado como provado no **facto 19** que – *às 11:46:00h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência*;
- Deve ser dado como provado no **facto 20** que – *às 11:47:58h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência*;
- Deve ser dado como provado no **facto 21** que – *às 11:58:22h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência*;
- Deve ser dado como provado no **facto 22** que – *às 12:01:30h a Autora introduziu o código de autorização que recebeu no seu telemóvel e em ato contínuo o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu a instrução de transferência.*
2 – Deve ser julgado como não provado que «a gerente da Autora ao aceder a plataforma do Banco lhe tenha aparecido "uma página em branco"».
3 – Os **factos dados como provados em 27, 28 e 29** devem transitar para o elenco dos factos não provados.
4 – O **facto provado 10** dos factos provados deve ser dado como provado mas com indicação de "3 ou 4 tentativas".
5 – No **facto provado 34** devem ser introduzidos os seguintes factos: que a apreciação e consideração do uso da palavra "fraude" foi feita assumindo que as palavras da Cliente, a ora Autora, eram verdadeiras e que esta não tinha tido qualquer intervenção do que aconteceu.
6 – Deve ser aditado à factualidade provada **–** como **facto provado 44 –** que " *A autora nunca questionou a operadora de telemóvel Vodafone sobre a possibilidade de clonagem ou acesso indevido ao seu telemóvel, no período em que ocorreram todas operações identificadas nos números 13 a 22 dos factos dados como provados*".
5 – Deve ser aditado à factualidade provada que «*A Autora teve acesso às recomendações de segurança feitas pelo réu Banco referentes ao acesso ao seu portal para uso do serviço "homebanking"*».
6 – Deverá ser dado como provada a seguinte factualidade:

- Que foram cumpridos todos os mecanismos de processamento e validação de segurança utilizados pelos sistemas informáticos do Banco;
- Que foram respeitados pelo Banco todas as regras de segurança e de proteção do cliente, que lhe são exigíveis em termos de segurança relativamente à utilização do homebanking;
- A Autora, voluntariamente, facultou os seus dados pessoais acedendo sucessivamente à área de homebanking, mesmo que avisada de que existiam e existem todos os dias tentativas de fraude, conforme avisos do Banco, que a Autora não impugnou porque os conhecia, mas preferiu ignorá-los.
- Que o site de homebanking do Banco não sofreu, no período em que foram feitas as transferências da conta do Autor nenhum ataque informático ou qualquer tentativa de intrusão ou utilização ilícita por parte de terceiros.

Apreciando.
A impugnação da decisão de facto visa obter uma reapreciação da decisão proferida pelo tribunal de primeira instância, ou seja, apurar se no confronto com os meios de probatórios produzidos determinados factos foram incorretamente julgados, quer por terem sido indevidamente considerados assentes devendo julgar-se não provados, quer por terem sido considerados não provados quando deveriam ter sido considerados assentes (cfr. artigo 662.º, n.º 1, do CPC).
O Tribunal de segunda instância deve formar a sua própria convicção acerca dos elementos probatórios disponíveis (os indicados pelas partes e os obtidos oficiosamente), sendo tal convicção firmada a partir de uma ponderação crítica dos referidos meios probatórios quando sujeitos ao princípio da livre apreciação da prova (como sucede no caso vertente). Ou, dito de outra forma, a segunda instância deve funcionar como um efetivo segundo grau de jurisdição em sede de matéria de facto. Como se salienta no Ac. STJ de 11.02.2016[1] «*Certo é que a Relação, em sede de apreciação do recurso sobre a decisão da matéria de facto, tendo acesso a todos os meios de prova que foram produzidos e aos que foram prestados oralmente (que, por isso foram gravados, nos termos do artigo 155.º, n.º 1, do NCPC), estará apta a reapreciar a decisão e o correspondente juízo probatório formulado relativamente as factos principais. Tal possibilidade está agora praticamente garantida em todas as circunstâncias, na medida em que o artigo 155.º prescreve a gravação de todas as audiências finais, depois de o artigo 422.º garantir a gravação de todos os depoimentos antecipados ou por carta. O confronto com a generalidade dos meios de prova oralmente produzidos aproxima, assim, a Relação da situação em que se encontrava o tribunal de 1.ª instância quando proferiu a decisão recorrida. […] Afinal, as circunstâncias em*

que se inscreve a sua atuação são praticamente idênticas às que existiam quando o tribunal de 1.ª instância proferiu a decisão impugnada, apenas cedendo nos fatores da imediação e da oralidade».
Prescreve o artigo 607.º, n.º 5, do Código de Processo Civil que «O juiz aprecia livremente as provas segundo a sua prudente convicção acerca de cada facto; a livre apreciação não abrange os factos cuja prova a lei exija formalidade especial, nem aqueles que só possam ser provados por documentos ou que estejam plenamente provados, quer por documentos, quer por acordo ou confissão das partes».
No normativo acima citado está consagrado o *princípio da livre convicção do julgador* o qual postula que o julgador deve decidir com base na sua prudente convicção acerca de cada facto, ponderadas as particularidades do caso, as regras da experiência humana e da normalidade do acontecer, bem como as regras da lógica, não se bastando, pois, com um mero convencimento íntimo do foro subjetivo do juiz. Mas, por outro lado, há que ter presente que o convencimento do julgador se basta com uma certeza relativa, com um grau de probabilidade adequado às exigências práticas da vida e que enquanto no processo penal se exige que o tribunal do julgamento decida para além de toda a dúvida com base em meios de prova efetivamente produzidos, por necessidade de respeito dos princípios da culpa e da presunção de inocência, no âmbito do processo civil o princípio da igualdade das partes impõe um equilíbrio entre estas, com a consequente diminuição do grau de convicção exigível. Como se sublinha no acórdão da Relação de Lisboa de 17.20.2017, processo n.º 585/13.1TCFUN-A.L1-7, relator Luís Filipe Pires de Sousa, publicado em www.dgsi.pt: «*Em processo civil o standard de prova é o da probabilidade prevalecente, segundo o qual deve escolher-se a hipótese fáctica que receba apoio (grau de confirmação lógica) relativamente maior dos elementos de prova conjuntamente disponíveis*».
O princípio da livre apreciação da prova tem aplicação, designadamente, no âmbito da prova testemunhal e, de forma mais circunscrita, quer no âmbito da valoração da prova documental, nos casos em que essa prova seja desprovida de força probatória plena (*v.g.* artigo 371.º, n.º 1, *in fine*, do CC) quer no da prova por confissão de parte – quando esta não possa valer como tal (artigo 361.º do CC) ou quando se trate de confissão extrajudicial não constante de documento (artigo 358.º, n.º 3, do CC) ou de confissão judicial não escrita e de confissão extrajudicial feita a terceiro ou contida em testamento (artigo 358.º, n.º 4, do CC). Casos há em que a lei fixa certa espécie de prova para determinada categoria de factos ou que atribui a um meio de prova determinado valor probatório, não deixando ao julgador qualquer margem de apreciação casuística.

Feitas estas considerações de ordem geral, retornemos ao caso concreto.
Começando pela alteração à redação dos factos provados n.ºs 13 a 22, o que o apelante pretende é que se adite a cada um deles que *foi a autora quem introduziu o código de autorização que recebeu no seu telemóvel* e que *«em ato contínuo o sistema do banco, por estarem reunidos todos os requisitos de movimentação, cumpriu a instrução de transferência».* Pretende, também, que seja aditada a hora em que foi introduzido no sistema o código de autorização recebido no telemóvel.
Basicamente, o apelante sustenta que cada uma das operações de transferência / pagamento em discussão nos autos só se deu após a introdução do código que foi rececionado no telemóvel da autora, tendo sido visualizado apenas e só pela autora, pelo que foi ela que os introduziu na plataforma do Banco.
Estamos perante factualidade – aquela o apelante pretende ver aditada – que está dentro dos poderes de cognição do tribunal de segunda instância em matéria de facto porque foi alegada pela parte na sua contestação (cfr. artigo 5.º/1, alínea a), do Código de Processo Civil). Efetivamente, no artigo 49.º daquele articulado o réu alegou que «*Mas adicionalmente, para além de todos os requisitos de segurança elencados supra, e por forma a garantir a segurança das operações, é enviado um código de 7 dígitos diretamente para o telemóvel do utilizador, o qual tem que ser introduzido na página web do Banco, em uso para ordenar a transação, de maneira a que esta seja processada*» e no artigo 50.º que «*No caso, constata-se que a autora introduziu os códigos, um a um, para cada uma das operações que foram processadas pelo banco*».
Trata-se de factualidade relativamente à qual as partes dissentem: por um lado, temos a versão da autora segundo a qual *não foi ela quem utilizou os códigos de autorização das várias operações em causa nos autos* e, por outro, a versão que o apelante pretende ver plasmada no elenco dos factos provados, ou seja, que *foi a autora quem introduziu os códigos de autorização que foram enviados para o número de telemóvel acima mencionado e, por conseguinte, quem validou aquelas operações*.
Para julgar provado que não foi autora quem efetuou e autorizou as transferências e pagamentos em discussão nos autos (o que pressupõe, como veremos, a introdução dos códigos de autorização) o julgador *a quo* fundou-se, em larga medida, nas declarações da legal representante da autora, Lucinda Jacinto, as quais considerou credíveis.
Os enunciados de facto provados n.ºs 13 a 22 contêm a descrição de cada uma das operações bancárias em discussão (designadamente o tipo de operação bancária, o montante envolvido e o destinatário/beneficiário da mesma) e bem

assim a hora de emissão, pelo banco apelante, dos respetivos códigos de autorização e do seu envio para o n.º (…) de telemóvel.
A factualidade que o apelante pretende ver aditada aos factos provados n.ºs 13 a 22 prende-se com a **introdução dos códigos de autorização recebidos no número de telemóvel (…)**, **sem a qual o banco apelante não realizaria as operações em discussão nos autos, como resulta da conjugação dos factos provados n.ºs 4, 5, 6**: o banco apelante cumpre as instruções de pagamento/transferência ordenadas a partir da plataforma eletrónica do Banco quando estão reunidos todos os requisitos enunciados naqueles factos provados.
Não é controvertido que os códigos de autorização necessários à confirmação de qualquer operação bancária de transferência ou pagamento através da dita plataforma eletrónica, eram enviados para o telemóvel com o n.º (…), o qual fora indicado pela gerente da autora ao réu (cfr. facto provado n.º 6).
Nas declarações de parte que prestou perante o tribunal (…), que é sócia-gerente da autora (como resulta da certidão de registo comercial da autora anexa à petição inicial) afirmou perentoriamente que no dia 16.07.2020 (data em que foram realizadas as transferências / pagamentos em discussão nos autos) o telemóvel ao qual está associado aquele número (…) esteve sempre ao seu lado, em cima da sua secretária, acrescentando, ainda, que aquele telemóvel está sempre consigo, ou no trabalho, ou em casa, inferindo-se do seu depoimento que, para além dela, e numa situação de normalidade, apenas o seu marido terá acesso àquele telemóvel. (…) afirmou, também, que naquele concreto dia só ela se encontrava nos escritórios da autora, em frente ao computador e, repete-se, com o referido telemóvel em cima da secretária, ao seu lado. Sendo assim, na versão por ela apresentada, seria inverosímil que, naquele dia quando as operações bancárias foram ordenadas, autorizadas e executadas, algum terceiro se tivesse apoderado fisicamente do referido telemóvel de forma a poder visualizar os códigos de autorização (que efetivamente foram enviados pelo banco réu para o número de telemóvel acima referido) e a introduzi-los na plataforma eletrónica do banco réu. E note-se que *quem porventura o pudesse ter feito, teria ainda de se ter apoderado das credenciais de acesso ao serviço de homebanking,* as quais a sócia-gerente da autora afirmou estariam em seu poder, não identificáveis por terceiros, nem a estes acessíveis, e, depois, tê-las introduzido no computador existente na sede da autora, o único que estava certificado digitalmente para a realização das transações aqui em discussão.
Naturalmente que não se olvida que uma coisa é o *acesso físico ao telemóvel* e outra a *visualização das mensagens* enviadas para um determinado número de um telemóvel; é possível a um terceiro visualizar à distância mensagens

enviadas para um determinado número de telemóvel se tiver havido intrusão no telemóvel. Como explicou a testemunha (…) pode haver uma "clonagem" do cartão telefónico que permitirá a um terceiro receber no cartão clonado as mensagens dirigidas ao cartão original e pode ser instalada num telemóvel uma aplicação que permite a leitura, por um terceiro, das mensagens nele recebidas. Todavia, em qualquer uma dessas situações, a pessoa que faz a fraude eletrónica terá de ter tido *acesso físico* ou contacto com o telemóvel, ou para efetuar a clonagem do cartão telefónico ou para instalar no telemóvel a dita aplicação. Refira-se, ainda, que resulta do documento junto a fls. 318 dos autos, emitido pela Vodafone, e cujo teor não foi impugnado, que aquela operadora informou que «*não dispomos de registo de qualquer situação/ reclamação referente à clonagem do número de telefone (…)*», o que significará, no mínimo, que após os acontecimentos dos autos, a autora não reportou à operadora uma eventual clonagem do referido telemóvel. Tal como resulta do documento de fls. 122/123, também ele não impugnado, que não foi emitida segunda via do cartão inserido no telemóvel.
No caso a execução pelo banco réu das ordens de transações em discussão nos autos implicava a reunião de vários requisitos melhor explicitados nos pontos de facto provados n.ºs 4, 5, e 6, a saber: a utilização de um computador onde tivesse sido instalado um certificado digital, a introdução de um código de utilizador, de uma *password* de acesso e de duas posições do número de identificação fiscal do utilizador – tudo para garantir a entrada na plataforma digital do banco – e, finalmente, a introdução de um código de autorização, que era enviado para o número de telemóvel indicado pelo utilizador do serviço, *in casu*, pela autora através da sua sócia-gerente. Em suma, a execução das operações de pagamento implicava a utilização de dois equipamentos – o computador e o telemóvel – os quais, contudo, são autónomos entre si no sentido de que não estão conectados um com o outro, pelo que uma eventual violação de um deles não compromete a fiabilidade e o funcionamento do outro: o acesso à plataforma digital do banco e a introdução da ordem de execução não dependem do uso telemóvel, o qual só se torna necessário para veicular as mensagens contendo os códigos de utilização de cuja introdução no sistema depende a execução, pelo banco, das ordens do utilizador do serviço de *homebanking*.
No caso está provado que os pagamentos e transferências em discussão nos autos foram efetuados com a utilização do código de utilizador da autora, confirmadas com duas posições aleatórias do seu NIF e com a introdução dos códigos de autorização e enviados por SMS para o telemóvel n.º … (cfr. facto provado n.º 23), número esse que fora indicado pela gerente da autora (cfr. facto provado n.º 6), isto é, resulta da matéria de facto provada que as

operações referidas nos factos 13 a 22 derivaram da introdução de credenciais e códigos através do computador da autora, incluindo, a *introdução dos código de autorização que foram recebidas no telemóvel da autora e, em ato contínuo, o sistema do Banco por estarem reunidos todos os requisitos de movimentação cumpriu sucessivas instruções de transferência ao longo de um período de cerca de 45 minutos*. Pelo que foram utilizados os dois artefactos, computador e telemóvel da autora, sendo ainda incontroverso que as mensagens foram efetivamente enviadas para o telemóvel da autora e as operações exigiram a inserção dos códigos remetidos por essa via.
Acresce que os documentos juntos aos autos a fls. 47 a 49 verso – cujo teor não foi impugnado – revelam o visor do telemóvel em causa nos autos com a mensagem contendo o código de autorização da operação bancária bem como a hora de receção da mensagem no telemóvel (e a testemunha … corroborou que o visor do telemóvel mostra a hora de receção da mensagem), revelando pois que a hora do envio daquelas mensagens não podia ter sido aquela em que a sócia-gerente da autora declarou ouvir «as mensagens a cair». Ademais, quer as horas de envio dos códigos de autorização quer a hora de introdução dos mesmos na plataforma digital estão registadas no documento de fls. 143 e seguintes do qual resulta que a introdução do código de autorização na plataforma digital para cada uma das transações em discussão nos autos ocorre no curto intervalo de tempo em que tinham de ser introduzidos para a autorização da operação, para o que tinham de ser necessariamente visualizados nessa breve fração temporal e inseridos no mesmo dispositivo informático em que tinham sido executados os outros comandos necessários para cada uma das operações.
A autora é uma pessoa coletiva, pelo que, independentemente das equivalências jurídicas com pessoas singulares, não é suscetível de antropomorfização. Existem ações humanas juridicamente imputáveis à pessoa coletiva, mas no plano factual não existe uma osmose entre pessoas humanas e as ficções jurídicas constituídas pelas pessoas coletivas. Consequentemente, apenas se pode considerar provado que as operações foram precedidas pela introdução por uma pessoa humana dos códigos de autorização recebidos no telemóvel propriedade da autora, estando ambos (a pessoa humana que visualizou as mensagens e o telemóvel) nas instalações da autora e com domínio sobre os dois equipamentos necessários para a realização das transações em discussão nos autos.
Diremos, pois, que está provado que foi introduzido o código de autorização que foi recebido no telemóvel com o n.º (…) para validar cada uma das transações realizadas e descritas nos factos provados n.ºs 13 a 22 e que essa prova resulta quer das declarações de parte da legal representante da autora

que afirmou que só ela é que utilizava o *homebanking*, que mantinha na sua posse as credenciais de acesso à plataforma, que no dia dos eventos em causa nos autos só ela é que estava no escritório da autora, em frente ao computador que tem instalado o certificado digital que permite a realização *on line* das transações em discussão nos autos, e que o telemóvel com o n.º (…) estava ao seu lado, em cima da secretária, e também dos factos provados n.ºs 4, 5, 6, 7, 8 e 23, os quais revelam cada uma das operações em causa só se concretizaram e só se podiam ter concretizado após a introdução do código de autorização rececionado no referido telemóvel.
Quanto ao enunciado «por estarem reunidos todos os requisitos de movimentação», tendo em atenção a dimensão factual específica que está em causa deve ser reformulada limitando-o à componente relevante em termos de conclusão das operações informáticas, as mesmas foram precedidas da receção no telemóvel com o cartão SIM relativo ao número de comunicações móveis (…) que era detido pela gerente da Autora e se encontrava no mesmo local do computador que tinha o Certificado Digital para as operações bancárias e só depois da visualização dos códigos de autorização e respetiva inserção o sistema informático do Banco cumpriu a instrução de cada uma das referidas operações (transferência/pagamento).
Os factos em análise foram provados a partir de inferências diretas de elementos de prova constantes de documentos admitidos e cuja veracidade não foi posta em causa, sendo ainda essa conclusões corroboradas pelos elementos do depoimento da testemunha (…) que depôs de forma credível e se revelou isento e com conhecimentos e experiência relevantes para o efeito e, ainda, pelas próprias declarações da gerente da Autora que confirma a detenção, no período em que ocorreram as operações, do equipamento telemóvel, no mesmo local onde se encontrava o computador e mesmo essa fonte de prova reconheceu que os códigos de autorização das operações foram recebidos no dispositivo em causa. Desta forma, a alegação da sócia-gerente da autora de que as mensagens só teriam sido recebidas entre as 15.00 e as 15.30 é desmentida por aquelas provas, padecendo de incongruência extrínseca, para além de se apresentar intrinsecamente pouco verosímil.
Procede, pois, parcialmente este segmento da impugnação de facto pelo que de determina o aditamento ao elenco dos factos provado de um novo facto com o seguinte teor e numeração:
«**23-a** - *O código de autorização para cada uma das operações bancárias referidas nos pontos de facto n.ºs 13 a 22 foi recebido no telemóvel com o número ali identificado que era detido e se encontrava sob o domínio de pessoa humana que estava no mesmo local que o computador que tinha o Certificado Digital para as operações bancárias e só depois da introdução*

tempestiva dos códigos de autorização emitidos para cada uma daquelas operações (transferência/pagamento) o sistema informático do Banco cumpriu a instrução de cada uma das referidas operações».

*

O facto provado 23-a implica julgar **não provado** que:
- O segundo segmento do facto provado n.º 27: «e conseguiu verificar que haviam sido realizadas as transferências e os pagamentos referidos em 13 a 22».
- O facto provado n.º 28: «As transferências e os pagamentos referidos em 13 a 22 não foram efetuados, nem consentidos, pela gerente da autora desconhecendo os respetivos destinatários»;
- O facto provado n.º 29: «Nesse momento constatou que havia recebido no seu telemóvel várias mensagens contendo os códigos de autorização para a realização dessas operações que não havia utilizado».
*

Defende o apelante que não foi feita prova alguma de que «ao aceder à plataforma do Banco apareceu à gerente da autora "uma página em branco». Vejamos se lhe assiste razão.
Previamente se dirá que aquela alegada "anomalia" só tem respaldo nas declarações de parte da sócia-gerente da autora, cujo interesse no desfecho da ação é evidente.
Na motivação do facto provado 23-a já se constatou que parte das declarações daquela fonte de prova contrariam o que resulta de forma direta da prova documental bem como da apreciação dos vários dados sobre as operações informáticas. Importa, ainda, ter presente que a pegada digital inviabilizava uma eventual tentativa de desmentido sobre a localização do telemóvel e do computador e ainda sobre a circunstância de as operações terem sido realizadas a partir do computador (pelo que a forma de contornar as respetivas implicações nunca poderia ser negar esses factos).
De acordo com o relato de (…), entre as 11.00 e 11.30 do dia 16.07.2020, aquela terá introduzido as devidas credenciais na plataforma eletrónica para aceder ao sistema de *homebanking* do banco réu (o que é confirmado pelo documento de fls. 143 e ss., donde consta que foi efetuado um *login* na plataforma digital do réu às 11.03.39) e fê-lo através do computador existente na sede da autora (computador onde está instalado o *certificado digital* fornecido pelo banco réu, o qual juntamente com credenciais a que já aludimos *supra* permite ao banco verificar a identidade do utilizador da plataforma). Disse, pois, a sócia-gerente da autora que introduziu o código de utilizador, a *password* de acesso e duas posições no número de identificação

fiscal da autora e que conseguiu entrar no *site* pretendido (pois referiu que ainda conseguiu ver os movimentos da conta bancária) mas que logo de seguida «o écran ficou todo branco», o computador ficou bloqueado, donde se infere que, na sua versão dos factos, terá ficado impedida de realizar qualquer operação. Acrescentou que fez mais três, quatro tentativas, desligando e voltando a ligar o computador e introduzindo de novo as devidas credenciais (mas não os códigos de autorização), sem sucesso, e que estava sozinha na empresa, não existindo, portanto, prova testemunhal para corroborar o dito "*aparecimento de uma página em branco no écran do computador*", o que terá sucedido só depois da introdução das credenciais de acesso na plataforma do banco, ou seja, depois de efetuado o *login*. Sucede que sobre esta alegada "anomalia" as testemunhas (…) e (…), ambos funcionários do réu, limitaram-se a relatar aquilo que lhes foi transmitido pela sócia-gerente da autora quando esta se deslocou à agência do réu no dia dos eventos em causa nos autos; como referiu a testemunha (…), a cliente contou-lhes que alguém estava a usar os códigos dela e a fazer transferências que ela não autorizou; tinha acedido ao *homebanking on line* e tinha introduzido os códigos e a password e que «depois ficou tudo branco no écran», adiantando que a cliente lhes disse que se tratava de uma fraude, mas que ele não sabe se foi fraude e que as providências de imediato tomadas – o bloqueio das contas – foram medidas cautelares. Ou seja, o que aquelas testemunhas relataram sobre o alegadamente sucedido no écran do computador da autora foi apenas o que lhes havia sido relatado pela sócia-gerente da autora.
(…) afirmou perante o tribunal que terá tentado comunicar telefonicamente para um número fixo do banco réu para indagar o que se estaria a passar, mas que ninguém lhe atendeu o telefone. Não está, contudo, comprovado nos autos, quer documentalmente quer por outro meio probatório, que aquelas tentativas telefónicas foram efetivamente empreendidas pela sócia-gerente da autora.
Refira-se, ainda, que a testemunha (…), funcionário do réu, declarou que nunca tiveram queixas de clientes quanto ao aparecimento de «uma página em branco após a introdução das credenciais de acesso».
Por último, na versão dos factos apresentada pela sócia-gerente da autora, ela terá feito, duas, três ou quatro tentativas de desbloqueamento do computador, desligando-o, voltando a ligá-lo, e que em cada uma das tentativas voltava a inserir as credenciais de acesso. Porém, analisando o documento de fls. 134 e ss. o qual consiste num extrato com todos os movimentos realizados na conta no dia dos eventos em discussão nos autos, verificamos que nele não estão registados um login às 11:03:39, outro às 11:24:36 e o último às 15:50:58.
Por todo o exposto, tem razão o apelante ao defender que não deve ser julgado

provado que apareceu no écran do computador da autora uma página em branco, quando a sua sócia gerente pretendeu aceder à plataforma do banco.
Pese embora o apelante apenas impugne o facto provado n.º 11 – onde é referido que «voltou a aparecer uma página em branco» –, também no facto provado n.º 10 consta que «após a gerente da autora introduzir o código de utilizador (…), a password de acesso e dois números do NIF, apareceu no computador uma página em branco que a impossibilitou de efetuar qualquer operação».
Assim, há que julgar não provado quer o facto provado n.º 11, quer a segunda parte do ponto de facto provado n.º 9 – «apareceu no ecrã do computador uma página em branco que a impossibilitou efetuar qualquer operação» e, ainda, os factos provados n.ºs 10 e 12 o primeiro porque conexionado com o último segmento do facto provado n.º 9 (este último parcialmente não provado) e o segundo porque conexionado com o facto provado n.º 11 (não provado).
Em face do exposto, procede este segmento da impugnação da decisão de facto e, em conformidade, elimina-se do elenco da factualidade provada os factos provados n.ºs 10, 11 e 12 e a segunda parte do enunciado de facto n.º 9, o qual passará a ter o seguinte teor: «após, a gerente da autora introduziu o código de utilizador (…), a password de acesso e dois números do NIF».
*

Quanto ao **facto provado n.º 34**, diremos que o apelante não cumpriu na respetiva impugnação o ónus que lhe é imposto pelo artigo 640.º, n.º 1, alínea c), do Código de Processo Civil, ou seja, «especificar a decisão que, no seu entender deve ser proferida sobre a concreta questão de facto impugnada».
Com efeito, o apelante afirma que ele foi «devidamente explicado pelas testemunhas (…) e (…)» e que «a apreciação e consideração do uso da palavra "fraude" foi feita assumindo que as palavras da Cliente, a ora Autora, eram verdadeiras e que esta não tinha tido qualquer intervenção do que aconteceu», mas, depois, não indica o resultado que pretende que fique consignado naquele facto provado.
Extrai-se do disposto no artigo 640.º, n.º 1, do CPC que a consequência da falta de cumprimento dos ónus previstos naquele normativo é a «imediata rejeição do recurso na parte relativa à impugnação da matéria de facto», logo sem possibilidade de convite ao aperfeiçoamento.
Em face do exposto, rejeita-se o segmento da impugnação da decisão de facto relativa ao enunciado de facto provado n.º 34.
*

Defende o apelante que deve ser aditado à factualidade provada **–** como **facto**

provado 44 – que "*A autora nunca questionou a operadora de telemóvel Vodafone sobre a possibilidade de clonagem ou acesso indevido ao seu telemóvel, no período em que ocorreram todas operações identificadas nos números 13 a 22 dos factos dados como provados*" e que «*A Autora teve acesso às recomendações de segurança feitas pelo réu Banco referentes ao acesso ao seu portal para uso do serviço "homebanking "*».
Pois bem, quanto à factualidade – *A autora nunca questionou a operadora de telemóvel Vodafone sobre a possibilidade de clonagem ou acesso indevido ao seu telemóvel, no período em que ocorreram todas operações identificadas nos números 13 a 22 dos factos dados como provados* – ela resulta da informação prestada pela operadora Vodafone, que consta de fls. 318, e sobre o qual as partes tiveram oportunidade de exercer o contraditório.
Por conseguinte, e ao abrigo do disposto no artigo 5.º, n.º 1, alínea b), do CPC, o seu conhecimento pelo tribunal de segunda instância insere-se no âmbito do seu conhecimento em termos de matéria de facto, pelo que tal factualidade – comprovada documentalmente nos autos – deve ser aditada ao elenco da factualidade provada.
Relativamente à factualidade – *A Autora teve acesso às recomendações de segurança feitas pelo réu Banco referentes ao acesso ao seu portal para uso do serviço "homebanking "* – trata-se de matéria abrangida pelos factos provados n.ºs 41 e 42, pelo que se indefere o pretendido aditamento.
*
Finalmente, defende o apelante que deve ser aditado ao elenco da factualidade provada que:
(i) «*Foram cumpridos todos os mecanismos de processamento e validação de segurança utilizados pelos sistemas informáticos do Banco»;*
(ii) «Foram respeitados pelo Banco todas as regras de segurança e de proteção do cliente, que lhe são exigíveis em termos de segurança relativamente à utilização do homebanking»;
(iii) «A Autora, voluntariamente, facultou os seus dados pessoais acedendo sucessivamente à área de homebanking, mesmo que avisada de que existiam e existem todos os dias tentativas de fraude, conforme avisos do Banco, que a Autora não impugnou porque os conhecia, mas preferiu ignorá-los»;
(iv) «O site de homebanking do Banco não sofreu, no período em que foram feitas as transferências da conta do Autor nenhum ataque informático ou qualquer tentativa de intrusão ou utilização ilícita por parte de terceiros».
Relativamente aos enunciados descritos em (i) e (ii) dir-se-á que não estamos perante "factos" do ponto de vista processual, isto é, de «ocorrências concretas da vida real e o estado, a qualidade ou situação real das pessoas e das coisas», mas antes perante juízos de valor, com natureza conclusiva,

extraíveis de factos que não estão plasmados no enunciado em questão. Além do mais, tais juízos conclusivos integram o *thema decidendum*.
Por conseguinte, não pode, qualquer um deles, integrar o elenco da factualidade provada.
Quanto aos demais enunciados, o primeiro ficou prejudicado pela transição para o elenco dos factos provados dos enunciados de facto n.ºs 10 e 11.
Relativamente ao último enunciado – *o site de homebanking do Banco não sofreu, no período em que foram feitas as transferências da conta do Autor nenhum ataque informático ou qualquer tentativa de intrusão ou utilização ilícita por parte de terceiros* – dir-se-á que o mesmo abrange matéria de facto que foi alegada na contestação do réu pelo que se insere no âmbito dos poderes de cognição deste tribunal de segunda instância e termos de matéria de facto.
A factualidade em apreço infere-se, na verdade, dos factos provados n.ºs 8, 9, 13 a 22, 23, 23ª, 24, 25 e 26, os quais revelam que a gerente da autora acedeu *diretamente à página web do banco* (e não a uma página em branco como afirmou em julgamento) após ter inserido na plataforma eletrónica do banco réu as devidas credenciais de acesso, que estavam em seu poder, e que todas as operações que foram efetivamente realizadas foram-no depois da introdução do respetivo código de autorização recebido no número de telemóvel que fora indicado pela gerente da autora, a qual tinha o domínio e a posse do mesmo (do telemóvel), após o que o sistema do banco cumpriu as ordens de pagamento. Os factos em apreço revelam que as ordens de transferência / pagamento só foram realizadas/cumpridas pelo banco porque para além de terem sido cumpridos todos os requisitos do procedimento de autenticação, todas e cada uma das operações executadas pelo banco réu foram autorizadas através da introdução dos respetivos códigos enviados pelo banco réu para um equipamento escolhido pela autora, detido por ela, e sobre o qual o banco réu não tem qualquer domínio. O que, aliás, foi também corroborado pelas testemunhas (…) e (…).
Atento o exposto, deve ser aditado ao elenco dos factos provados um novo enunciado com o seguinte teor e numeração:
«44 - O site de homebanking do Banco não sofreu, no período em que foram feitas as transferências da conta do Autor nenhum ataque informático ou qualquer tentativa de intrusão ou utilização ilícita por parte de terceiros».
*

DECISÃO
Em face do exposto:
1) Rejeita-se liminarmente a impugnação da decisão de facto quanto ao facto

provado n.º 34.
2) Julga-se parcialmente procedente a impugnação da decisão de facto e, em consequência:
2.1. Adita-se um novo facto ao elenco dos factos provado com o seguinte teor e numeração:
«**23-a -** ***O código de autorização para cada uma das operações bancárias referidas nos pontos de facto n.ºs 13 a 22 foi recebido no telemóvel com o número ali identificado que era detido e se encontrava sob o domínio de pessoa humana que estava no mesmo local que o computador que tinha o Certificado Digital para as operações bancárias e só depois da introdução tempestiva dos códigos de autorização emitidos para cada uma daquelas operações (transferência/pagamento) o sistema informático do Banco cumpriu a instrução de cada uma das referidas operações.***
2.2. Ordena-se a transição para o elenco dos factos não provados da seguinte factualidade:
- «As transferências e os pagamentos referidos em 13 a 22 não foram efetuados, nem consentidos, pela gerente da autora desconhecendo os respetivos destinatários», ou seja, o facto provado n.º 28;
- «Nesse momento constatou que havia recebido no seu telemóvel várias mensagens contendo os códigos de autorização para a realização dessas operações que não havia utilizado», ou seja, o facto provado n.º 29;
- E o segundo segmento do facto provado n.º 27: «e conseguiu verificar que haviam sido realizadas as transferências e os pagamentos referidos em 13 a 22».
2.3. Elimina-se do elenco da factualidade provada os factos provados n.ºs 10, 11 e 12 e a segunda parte do enunciado de facto n.º 9, o qual passará a ter o seguinte teor: «após, a gerente da autora introduziu o código de utilizador (…), a password de acesso e dois números do NIF».
2.4. Adita-se ao elenco da factualidade provada, sob o n.º 43 a seguinte factualidade:
«A autora nunca questionou a operadora de telemóvel Vodafone sobre a possibilidade de clonagem ou acesso indevido ao seu telemóvel, no período em que ocorreram todas operações identificadas nos números 13 a 22 dos factos dados como provados».
2.5. Adita-se ao elenco da factualidade provada, sob o n**.º 44**, a seguinte factualidade:
«O site de homebanking do Banco não sofreu, no período em que foram feitas as transferências da conta do Autor nenhum ataque informático ou qualquer tentativa de intrusão ou utilização ilícita por parte de terceiros».

3) Indefere-se o aditamento ao elenco dos factos provados dos seguintes enunciados:
- «*Foram cumpridos todos os mecanismos de processamento e validação de segurança utilizados pelos sistemas informáticos do Banco»;*
- «*Foram respeitados pelo Banco todas as regras de segurança e de proteção do cliente, que lhe são exigíveis em termos de segurança relativamente à utilização do homebanking»;*
- «*A Autora, voluntariamente, facultou os seus dados pessoais acedendo sucessivamente à área de homebanking, mesmo que avisada de que existiam e existem todos os dias tentativas de fraude, conforme avisos do Banco, que a Autora não impugnou porque os conhecia, mas preferiu ignorá-los».*
*
Por uma questão de clareza passa-se a enunciar os factos julgados provados após a apreciação da impugnação da decisão de facto:
«1 - A autora é uma sociedade que tem por objeto a colocação de isolamentos e revestimentos na indústria da construção civil.
2 - Era titular da conta de depósitos à ordem com o n.º (…), domiciliada junto do réu na Sucursal Sotavento Negócios com o código n.º (…).
3 - Há pelo menos 10 anos a gerente da autora solicitou ao réu a adesão ao serviço por este prestado através de plataforma eletrónica (área empresa do Banco) que lhe permitia aceder aos movimentos daquela conta e realizar pagamentos e transferências. 4 - Para o efeito foi-lhe fornecido pelo réu o Certificado Digital, composto por um Código de Adesão com 15 dígitos e que foi instalado no computador que a autora possuía na sua sede, o Código de Utilizador e a Password de acesso.
5 - Para a entrada na referida plataforma era ainda pedida a introdução, de forma aleatória, de duas posições do Número de Identificação Fiscal da autora.
6 - Para confirmação de operação de pagamento ou transferência era pedida a introdução de um Código de Autorização, o qual era enviado para o telemóvel com o n.º (…), que fora indicado pela gerente da autora ao réu.
7- A gerente da autora mantinha na sua posse as credenciais de acesso e utilizava quase diariamente aquela plataforma para consultar movimentos da conta bancária, efetuar pagamentos ou transferências bancárias.
8 - No dia 16.07.2020, por volta das 11h03m39ss, a gerente da autora iniciou o acesso à referida plataforma através do computador existente na sede da empresa, que utilizava o sistema operativo Windows 7, tendo como browser o Internet Explorer 11.
9- Após a gerente da autora introduziu o Código de Utilizador (…), a Password de acesso e dois números do NIF.

10 - eliminado.
11 - eliminado.
12 - eliminado.
13 - Pelas 11:15:46h foi efetuado o Envio de Ficheiros PSM no valor de € 2.997,00 e para confirmar esta operação foi emitido pelo réu, às 11:13:39h, um Código de Autorização para o n.º de telemóvel (...) (com o seguinte conteúdo: "MBCP Emp – Envio Ficheiro – Cta Deb: ... – Tipo: PSM – N. reg: 3 – Mont.: 2.997,00 EUR – Data Proc: 16/07/2020 – Codigo Autorizacao: ...).
14 - Pelas 11:29:01h foi efetuada uma Transferência Nacional no valor de € 1.000,00 para o IBAN PT (...), com o beneficiário "(...)", o descritivo "PAGAMENTOS" e para confirmar esta operação foi emitido pelo réu às 11:27:32h um Código de Autorização para o n.º de telemóvel ... (com o seguinte conteúdo: "MBCP Emp – Transferencia Nacional – Cta Debito: ... – IBAN Destino: PT ... – Montante: 1.000,00 EUR – Codigo Autorizacao: ...).
15 - Pelas 11:31:48h foi efetuada uma Transferência Nacional no valor de € 9.999,00 para o IBAN (...), com o beneficiário "(...)", o descritivo "PAGAMENTOS" e para confirmar esta operação foi emitido pelo réu, às 11:30:58h, um Código de Autorização para o nº de telemóvel ... (com o seguinte conteúdo: "MBCP Emp – Transferencia Nacional – Cta Debito: ... – IBAN Destino: PT (...) – Montante: 9.999,00 EUR – Codigo Autorizacao: ...).
16 - Pelas 11:35:05h foi efetuada uma Transferência Nacional Imediata no valor de € 9.998,00 para o IBAN PT (...), com o beneficiário "(...)", o descritivo "PAGAMENTOS" e para confirmar esta operação foi emitido pelo réu, às 11:34:25h, um Código de Autorização para o n.º de telemóvel ... (com o seguinte conteúdo: "MBCP Emp – Transferencia Nacional – Cta Debito: ... – IBAN Destino: PT (...) – Montante: 9.998,00 EUR – Codigo Autorizacao: ...).
17 - Pelas 11:39:02h foi efetuado um pagamento de serviços no valor de € 999,00 para a entidade 21800 – (...) com a referência (...) e esta transação foi confirmada com o Código de Autorização enviado por SMS, às 11:38:17h, para o n.º de telemóvel ... (com o seguinte conteúdo: "MBCP Emp – Pagamento Servicos – Cta/Cartao: ... – Entidade: ... – Referencia: (...) – Montante: 999,00 EUR – Codigo Autorizacao: ...).
18 - Pelas 11:43:33h foi efetuada uma Transferência Nacional Imediata no valor de € 10.000,00 para o IBAN PT (...), tendo com o beneficiário "(...)", o descritivo "PAGAMENTOS" e para confirmar esta operação foi emitido pelo réu, às 11:42:55h, um Código de Autorização para o n.º de telemóvel ... (com o seguinte conteúdo: "MBCP Emp – Transferencia Nacional – Cta Debito: ... – IBAN Destino: PT (...) – Montante: 10.000,00 EUR – Codigo Autorizacao: ...).
19 - Pelas 11:46:00h foi efetuada uma Transferência Nacional no valor de € 10.000,00 para o IBAN PT (...), com o beneficiário "(...)", o descritivo

"PAGAMENTOS" e para confirmar esta operação foi emitido pelo réu, às 11:45:14h, um Código de Autorização para o n.º de telemóvel … (com o seguinte conteúdo: "MBCP Emp – Transferencia Nacional – Cta Debito: … – IBAN Destino: PT (…) – Montante: 10.000,00 EUR – Codigo Autorizacao: …).
20 - Pelas 11:47:57h foi efetuado um pagamento de serviços no valor de € 998,00 para a entidade (…) – (…), com a referência (…) e esta transação foi confirmada com o Código de Autorização enviado por SMS, às 11:47:20h, para o n.º de telemóvel … (com o seguinte conteúdo: "MBCP Emp – Pagamento Servicos – Cta/Cartao: … – Entidade: … – Referencia: … – Montante: 998,00 EUR – Codigo Autorizacao: …).
21 - Pelas 11:58:21h foi efetuado um pagamento de serviços no valor de € 999,00 para a entidade (…) – (…) com a referência (…) e esta transação foi confirmada com o Código de Autorização enviado por SMS, às 11:57:47h, para o n.º de telemóvel … (com o seguinte conteúdo: "MBCP Emp – Pagamento Servicos – Cta/Cartao: … – Entidade: … – Referencia: … e – Montante: 999,00 EUR – Codigo Autorizacao: …).
22 - Pelas 12:01:29h foi efetuada uma Transferência Nacional no valor de € 10.000,00, para o IBAN PT (…), com o beneficiário "(…)", o descritivo "PAGAMENTOS" e para confirmar esta operação foi emitido pelo réu, às 12:00:09h, um Código de Autorização para o n.º de telemóvel … (com o seguinte conteúdo: "MBCP Emp – Transferencia Nacional – Cta Debito: (…) – IBAN Destino: PT (…) – Montante: 10.000,00 EUR – Codigo Autorizacao: …).
23 - Os pagamentos e transferências referidos em 13 a 22 foram efetuados com utilização do Código de Utilizador da autora, confirmados com duas posições aleatórias do NIF e com a introdução dos Códigos de Autorização enviados por "SMS" para o telemóvel n.º (…).
23-a - ***O código de autorização para cada uma das operações bancárias referidas nos pontos de facto n.ºs 13 a 22 foi recebido no telemóvel com o número ali identificado que era detido e se encontrava sob o domínio de pessoa humana que estava no mesmo local que o computador que tinha o Certificado Digital para as operações bancárias e só depois da introdução tempestiva dos códigos de autorização emitidos para cada uma daquelas operações (transferência/pagamento) o sistema informático do Banco cumpriu a instrução de cada uma das referidas operações.***
24 - Pelas 11:18:41h foi tentada uma Transferência Nacional, no valor de € 10.000,00 para o IBAN PT (…), com o beneficiário "(…)" e para confirmar esta transação foram enviados pelo réu, às 11:19:00h, dois Códigos de Autorização para o n.º de telemóvel (…), os quais não foram introduzidos na plataforma (com os seguintes conteúdos: "MBCP Emp – Transferencia Nacional – Cta

Debito: (…) – IBAN Destino: PT (…) – Montante: 10.000,00 EUR – Codigo Autorizacao: …" e "MBCP Emp – Transferencia Nacional – Cta Debito: (…) – IBAN Destino: PT (…) – Montante: 10.000,00 EUR – Codigo Autorizacao: …).
25 - Foi tentado o Envio de Ficheiros PSM, no valor de € 1.998,00, com Códigos de Autorização enviados para o n.º de telemóvel (…), pelas 12:07:04h (com o seguinte conteúdo: "MBCP Emp – Envio Ficheiro – Cta Deb: … – Tipo: PSM – N. reg: 2 – Mont: 1.998,00 EUR – Data Proc: 16/07/2020 - Codigo Autorizacao: …), pelas 12:07:08h (com o seguinte conteúdo: "MBCP Emp – Envio Ficheiro – Cta Deb: … – Tipo: PSM – N. reg: 2 – Mont: 1.998,00 EUR – Data Proc: 16/07/2020 – Codigo Autorizacao: …), pelas 12:08:04h (com o seguinte conteúdo: "MBCP Emp – Envio Ficheiro – Cta Deb: (…) – Tipo: PSM – N. reg: 2 – Mont: 1.998,00 EUR – Data Proc: 16/07/2020 – Codigo Autorizacao: …) e pelas 12:08:05h (com o seguinte conteúdo: "MBCP Emp – Envio Ficheiro – Cta Deb: … e – Tipo: PSM – N. reg: 2 – Mont: 1.998,00 EUR – Data Proc: 16/07/2020 – Codigo Autorizacao: …).
26 - Estas operações não foram realizadas porque não foram introduzidos na plataforma os Códigos de Autorização que haviam sido enviados para o telemóvel n.º 914044962.
27 - Pelas 15h50m58ss a gerente da autora acedeu à plataforma.
28 - (eliminado).
29 - (eliminado)
30 - Deslocou-se à Sucursal Sotavento Negócios do réu, onde chegou por volta das 16h00m, em estado de ansiedade e quase pânico.
31 - Ao contar o sucedido os colaboradores do banco réu comunicaram-lhe que se tratava de um caso de fraude e que deveria apresentar queixa.
32 - Pelas 14h37m daquele dia havia sido enviado um e-mail por Susana Rocha, do Gabinete de Gestão Aplicacional e Segurança do réu, para a Sucursal Sotavento Negócios, referindo que na sequência de um alerta Paywatch (SIBS) verificaram-se 3 transações suspeitas na conta da autora, solicitando o contato do cliente e que se aferisse se se tratavam de transações fidedignas (cfr. doc. de fls. 23vº/24, cujo teor se dá por integralmente reproduzido).
33 - O qual não obteve resposta por parte dos colaboradores da Sucursal Sotavento Negócios.
34 - Após o referido em 31 os colaboradores da Sucursal Sotavento Negócios bloquearam os movimentos na conta bancária e pelas 16h47m comunicaram que se tratava de fraude e solicitaram a devolução de todas as transferências realizadas naquele dia (cf. doc. de fls. 24 verso, cujo teor se dá por integralmente reproduzido).
35 - Nesse mesmo dia a gerente da autora apresentou reclamação junto do réu

relativa aos débitos realizados sem o seu consentimento (cfr. doc. de fls. 25, cujo teor se dá aqui por integralmente reproduzido).
36 - E apresentou denúncia na Divisão Policial de Faro da Polícia de Segurança Pública à qual foi atribuído o NUIPC … (cfr. doc. de fls. 25 vº/26, cujo teor aqui se dá por integralmente reproduzido).
37 - Em 28.07.2020 foi restituído à autora o montante de € 2.597,10.
38 - Em 11.09.2020 a autora enviou carta registada ao réu, solicitando a devolução do restante montante (cfr. doc. de fls. 26vº/28vº, cujo teor se dá por reproduzido).
39 - Em 11.11.2020 o réu respondeu referindo que "*não tem o Banco qualquer responsabilidade nas transações em causa, considerando que todos os mecanismos de processamento e validação utilizados encontram-se no Banco registados em nome da Sra. D. (…) e da (…) Algarve Lda., nomeadamente o Código de Adesão, o Certificado Digital, o Código de Utilizador, a Password, duas posições do Número Fiscal, número de telemóvel para a receção dos Códigos de Autorização com a identificação clara e inequívoca da operação a realizar e respetiva confirmação com esse código*" (cfr. doc. de fls. 29/30, cujo teor se dá por reproduzido).
40 - Referindo, ainda, que "*quanto aos pagamentos de serviços, e conforme oportunamente transmitido por contato telefónico, é necessário que procedam ao registo de reclamação sobre os montantes da fraude, através do site da entidade de Pagamento (…) em https://onlinepaymentplatform.com/en/contact* " (cfr. doc. de fls. 29/30, cujo teor se dá por reproduzido).
41 - O banco réu tem no seu site, à disposição dos clientes, diversos avisos de segurança e recomendações para acesso ao portal do banco e segurança no acesso ao portal de empresa, onde se detalham aspetos para prevenir fraudes.
42 - Alertando os clientes para eventuais tentativas de uso indevido dos dados dos clientes, páginas que têm semelhança com a do banco de entre outras.
43 - A autora nunca questionou a operadora de telemóvel Vodafone sobre a possibilidade de clonagem ou acesso indevido ao seu telemóvel, no período em que ocorreram todas operações identificadas nos números 13 a 22 dos factos dados como provados.
44 - O *site* de *homebanking* do Banco não sofreu, no período em que foram feitas as transferências da conta do Autor nenhum ataque informático ou qualquer tentativa de intrusão ou utilização ilícita por parte de terceiros.

II.5.
Reapreciação do mérito da decisão recorrida
Está em causa no presente recurso a sentença proferida pelo tribunal de primeira instância a qual julgou a ação parcialmente procedente e, em

consequência, condenou o réu a pagar à autora a quantia de € 54.392,90, acrescida de juros de mora, à taxa de juros civis, contados desde 16.07.2020.
Na sentença recorrida foi considerado que «ocorreu uma fraude informática na medida em que **a gerente da autora não consentiu nas transferências e pagamentos realizados**, desconhecendo os respetivos destinatários, mas ficou desembolsada do valor de € 56.990,00 (dos quais apenas foram recuperados € 2.597,10)» (sic) e que «não se comprovou nenhum facto que demonstre que atuou fraudulentamente» ou que «a gerente da autora tenha agido intencionalmente ou por negligência grave tenha fornecido a terceiros as credenciais de acesso e os códigos de autorização» e que o réu, por sua vez, «não logrou demonstrar o cumprimento do dever de garantir a confidencialidade e integridade do sistemas informático que colocou à disposição da autora». Concluindo que «não se apurando qualquer violação por parte da autora dos artigos 67.º e 72.º do RSP o réu terá de a reembolsar conforme determina o artigo 71.º, n.º 1, do mesmo diploma (…)».
A questão que o julgador *a quo* foi chamado a resolver e que agora o tribunal de segunda instância terá também de resolver é a de saber se o réu/apelante deve ser considerado responsável pelo pagamento da referida quantia, quantia correspondente a montantes que resultaram de movimentos bancários (transferências e pagamentos) registados na conta bancária à ordem da autora com o n.º (…), os quais a autora disse nunca ter ordenado ou autorizado.
Estamos no âmbito da responsabilidade civil contratual.
Não vem posto em causa no presente recurso que entre a autora e o réu foi celebrado um contrato de abertura de conta, com o qual se iniciam (ou podem vir a ser iniciados) toda uma série de contratos entre o banco e o cliente. Dito de outro modo, o contrato de abertura constitui um negócio bancário nuclear ao abrigo do qual se vão realizando outras operações entre o banco e o cliente. Com a abertura de conta é atribuído ao cliente o número da conta de pagamento (IBAN) a qual pode ser mobilizada ou através de assinatura ou através de mecanismos de acesso eletrónico (os códigos e as palavras passe).
No caso está provado que, à data dos factos, a autora era titular de uma conta de depósitos à ordem com o n.º (…), domiciliada junto do réu, e que, há pelo menos 10 anos, aderira ao serviço prestado por aquele através de plataforma eletrónica, o qual lhe permitia aceder aos movimentos da conta e realizar pagamentos e transferências. Isto é, ordenar e autorizar ordens de pagamento (por exemplo, transferências) de *forma remota*.
Esta possibilidade de emitir ordens de pagamento de forma remota é característica do chamado *homebanking*, que, na palavras do Acórdão do Supremo Tribunal de Justiça de 18.12.2013, processo n.º 6479/09.8TBBRG.G1.S1, consultável em www.dgsi.pt., «se concretiza pela

possibilidade conferida pela entidade bancária aos seus clientes, mediante a aceitação de determinados condicionalismos, de utilizar uma panóplia de operações bancárias, *on line*, relativamente às contas de que sejam titulares, utilizando para o efeito, canais telemáticos que conjugam os meios informáticos com os meios de comunicação à distância (canais de telecomunicação), por meio de uma página segura do banco».
À data em que a autora aderiu ao *homebanking* encontrava-se em vigor o D/L n.º 317/2009, de 30.10, doravante referido como RSP, o qual transpôs para a ordem jurídica interna a Diretiva 2007/64/CE, do Parlamento Europeu e do Conselho, de 13 de novembro relativa aos serviços de pagamento no mercado interno e que veio regular a atividade dos prestadores de serviço de pagamento que tivessem como atividade principal a prestação de serviços de pagamento a utilizadores desses serviços.
Não vem posto em causa que o contrato que nos ocupa está sujeito ao regime jurídico contemplado naquele diploma legal, sem prejuízo da aplicação das disposições contidas no novo regime previstos no D/L n.º 91/2018, de 12.11[2], que se mostrem mais favoráveis aos utilizadores de serviços de pagamento (cfr. artigo 159.º do D/L n.º 91/2018, de 12.11).
O prestador de serviços de pagamento só pode executar uma operação ou um conjunto de operações que tenha sido *devidamente autorizado*.
Dispõe o artigo 65.º do D/L n.º 317/2009, de 30.10.[3], epigrafado de *Consentimento e retirada do consentimento*, o seguinte:
«1 – Uma operação de pagamento ou um conjunto de operações de pagamento só se consideram autorizadas **se o ordenante consentir na sua execução**.
2 – O consentimento deve ser dado **previamente** à execução da operação, salvo se for acordado entre o ordenante e o respetivo prestador do serviço de pagamento que o mesmo seja prestado em momento posterior.
3 – O consentimento referido nos números anteriores deve ser dado na forma acordada entre o ordenante e o respetivo prestador do serviço de pagamento, sendo que, **em caso de inobservância da forma acordada, se considera que a operação de pagamento não foi autorizada**.
4 – (…)
5 – (…)
6 – Os procedimentos de comunicação e de retirada do consentimento são acordados entre o ordenante e o prestador de serviço de pagamentos.»
Em síntese, o consentimento para a execução da(s) operação tem de ser dado pelo ordenante nos termos acordados e terá que ser prévio à operação, salvo convenção em contrário entre as partes. Não tendo sido prestado nos termos referidos, a operação considera-se **não autorizada**.
A execução da ordem exige também que o cliente tenha sido *autenticado* pelo

prestador do serviço através de um procedimento que lhe permite verificar a identidade de um utilizador de serviços de pagamento ou a validade da utilização de um instrumento de pagamento específico, incluindo a utilização das credenciais de segurança personalizadas do utilizador.
Do referido regime decorrem um feixe de obrigações para o prestador do serviço de pagamento e também para o utilizador de serviços de pagamento com direito a utilizar um instrumento de pagamento. Este último tem de tomar todas as medidas razoáveis, em especial ao receber o instrumento de pagamento, para preservar a eficácia dos seus dispositivos de segurança personalizados (cfr. artigo 67.º/2) e o primeiro tem, nomeadamente, a obrigação de assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento (cfr. artigo 68.º, n.º 1, alínea a)).
O **artigo 70.º**, sob a epigrafe *Prova de autenticação e execução das operações de pagamento*, dispõe o seguinte:
«1 – Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada, **incumbe ao respetivo prestador do serviço de pagamento fornecer prova de que a operação foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência**.
2 – 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, por si só, não é necessariamente suficiente para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 67.º» (negritos nossos).
Como se diz no acórdão do STJ de 14.12.2016[4] «compreende-se este regime: por um lado, só o prestador do serviço de pagamentos, também fornecedor deste serviço, pode assegurar a operacionalidade do complexo sistema informático utilizado e a regularidade do seu funcionamento, garantindo também a confidencialidade dos dispositivos de segurança que permitem aceder ao instrumento de pagamento. Daí que recaiam sobre o banco prestador do serviço o risco das falhas e do deficiente funcionamento do sistema (como decorreria também do disposto no artigo 796.º do CC), impendendo sobre este o ónus da prova de que a operação de pagamento não foi afetada por avaria técnica ou qualquer outra deficiência. (…) Por outro lado, o utilizador do serviço de pagamento tem de dispor de um conjunto de

dispositivos de segurança (código de acesso, cartão matriz, etc.) que lhe vão permitir aceder a esse serviço. Esses dispositivos de segurança personalizados têm uma função de autenticação (cfr. artigo 2.º, alínea t), do RSP), permitindo identificar o utilizador e verificar se este é efetivamente o cliente que contratou o serviço de *homebanking*. Exige-se, por isso, ao utilizador que tome todas as medidas razoáveis em ordem a preservar a eficácia desses dispositivos de segurança personalizados».
Assim, se o utilizador de serviços negar ter autorizado a operação, ou alegar que ela foi incorretamente efetuada, cabe ao prestador dos serviços de pagamento provar 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.
Incumbe, pois, ao prestador de serviços de pagamento o ónus de provar que todas as transações que executou foram devidamente autorizadas.
Nos autos está em causa um conjunto de operações de pagamento (cfr. artigo 2.º, alínea g), do D/L n.º 317/2009) que tinham de ser autorizadas pela autora, titular da conta bancária a partir da qual as transações em discussão nos autos foram realizadas.
O banco réu logrou fazer a prova que lhe é imposta pelo supra citado artigo 70.º do RSP, ou seja, que todas as transações que executou e que estão em discussão nos autos foram realizadas a partir do computador da autora, com as credenciais da autora e foram confirmadas pelos códigos enviados para o número de telemóvel indicado pela gerente da autora, pelo que foram por ela autorizadas, e que só após a introdução dos códigos de autorização respetivos é que o sistema do banco – que não foi acometido de qualquer avaria técnica ou de intrusão ilícita de terceiros durante o período em causa – deu cumprimento às instruções da ordenante.
Em face do exposto, naturalmente que se impõe a absolvição do réu do pedido em que foi condenado, com a consequente revogação da sentença a qual se baseara num pressuposto que não se verificou: a falta de consentimento da autora para a realização das operações de pagamento em discussão nos autos.

Sumário:
(…)

III.
DECISÃO
Em face do exposto acordam em julgar a apelação procedente e, em conformidade, revogam a sentença proferida pela primeira instância,

absolvendo o réu Banco (…), SA do pedido em que ali foi condenado.
As custas da ação são da responsabilidade da autora/recorrida.
Notifique.
DN.
Évora, 12 de julho de 2023
Cristina Dá Mesquita
Rui Machado e Moura (1.º Adjunto)
Eduarda Branquinho (2.ª Adjunta)

---

[1] Processo n.º 907/13.5TBPTG.E1.S1, relator Abrantes Geraldes, publicado em www.dgsi.pt.
[2] O qual aprovou o Regime Jurídico dos Serviços de Pagamento e de Moeda Eletrónica, transpondo para a ordem jurídica interna a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 e veio revogar o D/L n.º 317/2009, de 30.10.
[3] A redação do artigo 103.º do D/L n.º 91/2018, de 12.11 é idêntica.
[4] Processo n.º 1063/12.1TVLSB.L1.S1, consultável em www.dgsi.pt.