Acórdão do Tribunal da Relação de Lisboa

Processo:	**347/23.8T8CDN.L1-7**
Relator:	**ALEXANDRA DE CASTRO ROCHA**
Descritores:	**CONTRATO DE ABERTURA DE CONTA** **HOMEBANKING** **MEIOS DE PAGAMENTO ELECTRÓNICOS** **FRAUDE** **UTILIZADOR DO SERVIÇO** **NEGLIGÊNCIA GROSSEIRA**
Nº do Documento:	**RL**
Data do Acordão:	**13-01-2026**
Votação:	**UNANIMIDADE**
Texto Integral:	**S**
Texto Parcial:	**N**
Meio Processual:	**APELAÇÃO**
Decisão:	**PROCEDENTE**

Sumário:

I – O contrato de abertura de conta bancária, constituindo a génese da relação bancária, dá origem à rede negocial que constitui aquela relação, onde se inserem outras figuras contratuais, tais como o depósito, a abertura de crédito, a emissão de cartão e o *home banking*, figuras essas associadas ao contrato de abertura de conta e com o mesmo interligadas, constituindo uma união de contratos.

II – Considerados os riscos da utilização de meios de pagamento electrónico, a segurança do sistema estará dependente da actuação diligente de todos os seus utilizadores e intervenientes, o que levou o RJSPME (DL 91/2018 de 12-11) a estabelecer especiais obrigações do utilizador dos serviços e do seu prestador, repartindo depois aqueles riscos e respectivos prejuízos entre ambos, tendo em consideração a actuação de cada um deles no cumprimento dos deveres que lhes são impostos.

III – Deve considerar-se decorrer de negligência grosseira o comportamento do utilizador que se configure totalmente incompreensível do ponto de vista de uma pessoa minimamente informada, perspicaz, cuidadosa e diligente, contrariando frontalmente o mais elementar senso comum.

Decisão Texto Parcial:

Decisão Texto Integral:

Acordam na 7.ª Secção do Tribunal da Relação de Lisboa:

RELATÓRIO:

D… intentou acção declarativa, com processo comum, contra Caixa Geral de Depósitos, S.A., formulando o seguinte pedido: «(…) ser a Ré condenada, a pagar/reembolsar à Autora a quantia de 4.950,00€ relativa ao valor que indevidamente foi sacado da sua conta bancária, acrescida dos juros moratórios, à taxa legal, desde o final do 1º dia útil seguinte àquele em que teve conhecimento da indevida movimentação, ou seja, desde 23/11/2022 até efectivo e integral pagamento, juros estes que até ao momento estão contabilizados em 156,23€; Ser também a R. condenada a pagar à Autora a quantia de 1.000,00€ a título de danos não patrimoniais, quantia a que devem acrescer juros moratórios, à taxa legal, desde a citação até efectivo e integral

pagamento».
Para tanto, alega ser cliente depositária da R., junto da qual é titular de uma conta à ordem, na qual existiu um movimento não realizado nem ordenado por si, no valor de € 4.950,00. Apesar da reclamação da A., a R. não procedeu à restituição do montante correspondente àquela operação. Pretende que a R. deverá entregar-lhe tal valor, bem como compensá-la pelas preocupações e transtornos por si sofridos.
A R. contestou, alegando que foi a A. quem agiu descuidadamente, com negligência grosseira, permitindo que terceiros pudessem ter acesso à sua conta através do serviço Caixadireta e efectuar um pagamento com cartão, tendo-lhes a A. fornecido as suas credenciais de segurança de acesso e de autenticação de operações, isto é, o cartão matriz e SMS Token.
Dispensada a realização de audiência prévia, o processo foi tabelarmente saneado, após o que foram dispensadas a identificação do objecto do litígio e a enunciação dos temas da prova.
Procedeu-se a audiência final, tendo depois sido proferida sentença, que concluiu com o seguinte dispositivo:
«(…) o Tribunal julga a acção parcialmente improcedente, por provada, e em consequência condena a ré, Caixa Geral de Depósitos, S.A., no pagamento à autora, D…:
- da quantia de €4.950,00 (quatro mil novecentos e cinquenta euros) a título de danos
patrimoniais, acrescida de juros, à taxa de 4%, desde 23.11.2022 até efectivo e integral pagamento;
- da quantia de €500,00 (quinhentos euros) a título de danos não patrimoniais, acrescida de juros, à taxa de 4%, desde a data da citação, ocorrida em 12.09.2023, até efectivo e integral pagamento.
*****
Custas por autora e ré na proporção do respectivo decaimento aritmético (cfr. artigo 527º, nº 1 do CPC)».

Não se conformando com esta decisão, dela apelou a R., formulando, no final das suas alegações, as seguintes conclusões:
« 1. O tribunal a quo sustenta a decisão proferida no âmbito dos presentes autos em factos que a ora Recorrente entende não encontrarem qualquer correspondência com a prova produzida, nomeadamente, com a prova testemunhal e muito menos com a prova documental junta aos autos, pelo que deveria ter dado resposta diferente à matéria de facto provada e não provada.
2. o Tribunal a quo julgou incorretamente os pontos 7, 9, 11 e 38 dos Factos Provados.
3. O ponto 7. não poderia ter sido dado como provado na medida em que foi.
4. Da prova produzida não resultou que tendo a Autora

carregado no link que lhe era transmitido, o mesmo tivesse dado acesso uma página falsificada, graficamente igual á da Ré, mas sim que esta não era de todo semelhante à da ora Recorrente.
5. Das declarações da Autora não resulta que a página fraudulenta que se apresentou após carregar no link fosse graficamente igual à da Ré. A Autora disse o que se passa a transcrever:
[…]
6. A Autora nunca referiu que a página fraudulenta para a qual foi reencaminhada era graficamente igual à da ora Recorrente.
7. Quando novamente questionada pela Mª Juiz de Direito refere inclusivamente que para entrar no homebanking da Recorrente os dados que tem que introduzir não são os mesmos cuja introdução lhe foi solicitada pela página fraudulenta.
8. Esta página fraudulenta pedia que fosse introduzido o número do cartão de débito, dado que como é do conhecimento geral e também da Autora, nunca é solicitado no homebanking da Recorrente.
9. A propósito deste assunto referiu a testemunha E… Trabalha com a segurança de informação e também na componente da prevenção de fraude, na banca online, que analisou esta campanha de phishing em concreto e bem assim a referida página fraudulenta:
[…]
10. Atenta a prova produzida e acima indicada, no caso concreto, o tribunal a quo não poderia ter incluído neste ponto 7. dos factos provados, que a página falsificada era graficamente igual à da Ré, porque efetivamente resultou, inclusivamente das declarações da Autora, que a página em causa era diferente, nunca sendo solicitado pela Recorrente no seu homebanking a introdução dos dados que foram pedidos à Autora no âmbito da página fraudulenta, nomeadamente o número de telemóvel e dados do seu cartão de débito.
11. Consta deste facto 7 da matéria de facto provada juízo de Direito que contém em si desde logo a decisão do pleito e que por essa mesma razão não deveria constar da mesma.
12. É que este facto 7 começa por dizer o seguinte: "Confiante, face ao nº de telefone utilizado…" e assim contém um juízo conclusivo, pelo que deverá ser excluído deste ponto 7 da matéria de facto provada, atendendo a que traduz um juízo de Direito sobre o thema decidendum, mais concretamente sobre o requisito da culpa da Recorrida, em obediência ao disposto no artigo 607º nºs 3 e 4 do CPC.
13. Isto significa que o referido ponto 7. dos factos provados, deveria dizer antes o seguinte, sugerindo-se para o mesmo a redação que segue: "A autora clicou naquele link que lhe era transmitido e que deu acesso a uma página falsificada que não era semelhante à página de homebanking da Ré e na qual foi

pedido para indicar o nº de contrato com a CGD, código de acesso (password) e de seguida o nº e nome do cartão de débito, dando de seguida indicação de erro."
14. O facto 9 dos factos provados também não podia te sido dado como provado na medida em que o foi.
15. Este facto além de conter em si mesmo também um juízo de Direito, não deveria dizer que a conversa com a Autora se iniciou com os procedimentos normais e autenticação presente a Ré, uma vez que de acordo com a descrição que é feita pela Autora desta conversa, não terá ocorrido quaisquer procedimentos de autenticação.
16. A afirmação contida neste facto de que "não levantou qualquer suspeita de que a chamada pudesse não provir da ré," trata-se de juízo conclusivo no que concerne ao requisito da culpa da Autora, motivo pelo qual o facto 9 deverá ser expurgado dos factos provados.
17. Das declarações da Autora não resulta que a conversa se tenha iniciado com qualquer procedimento de autenticação, muito menos normais. Vejamos o que esta disse: […]
18. Este foi o relato que a Autora, fez da conversa telefónica que manteve com o burlão, não resulta da mesma qualquer menção à realização de qualquer procedimento de autenticação.
19. Pelas duas razões acima expostas, não devia o tribunal a quo ter dado como provado o facto 9 dos factos provados, pelo que se requer que o mesmo deixe de constar de tais factos.
20. No que diz respeito ao facto 11 dos factos provados, salvo o devido respeito, o mesmo também não poderia ter sido dado como provado nos exatos termos em que o foi, ou melhor, com a redação que lhe foi atribuída.
21. Este facto deveria ter a seguinte redação: "Em continuação, a autora recebeu daquele mesmo número telefónico, por SMS, códigos para autorização da operação, tudo à semelhança dos procedimentos normal e usualmente seguidos pela ré para a confirmação de operações."
22. É que os códigos Token que a Recorrente envia por SMS para o telemóvel associado ao contrato de Caixa Direta, servem para confirmar operações, pelo que tal facto deve ficar espelhado no ponto 11 da matéria de facto.
23. Que tal é o propósito de tais códigos, é do conhecimento geral e público, resultando também da prova produzida.
24. Veja-se o que disse a este respeito a testemunha G..., da Direção de Compliance - Gabinete de Prevenção e Fraude da Recorrente, que se transcreve: […]
25. Finalmente, no que concerne ao facto 38 da matéria de facto provada o mesmo deveria ter diferente redação atenta a prova documental e testemunhal que foi produzida.
26. Do documento a que tal facto se reporta é do documento 10 junto da Contestação apresentada pela ora Recorrente e trata-se

de alerta/notícia publicada no site institucional da Recorrente (como refere o ponto 38 dos factos privados), cuja redação não é penas aquele que consta do facto 38 (que apenas reproduz a sua segunda página), do qual consta como data de publicação a data de 10.07.2022.
27. Do facto 38, deveria, pois, constar, por resultar igualmente do documento, a sua data de publicação, ou seja, 10.07.2022.
28. Dprova testemunhal produzida também resulta que tal alerta/ notícia foi efetivamente publicada naquela data, tendo sido disponibilizado pela da Recorrente para consulta pelos seus Clientes, previamente às data dos factos ora em causa (22.11.2022). Vejamos o que disse a testemunha G… sobre este assunto: […]
29. O facto 38 dos factos provados deveria conter não só o texto integral do anúncio/alerta publicado, mas igualmente a data da sua publicação, isto é, 11.07.2022.
30. O que significa que este facto deveria ter a seguinte redação: "Em 10.07.2022, a ré publicou no seu site institucional acessível ao público, na área relativa à segurança, um anúncio que alertava para este tipo de fraude, com os seguintes avisos:
Dá-se conhecimento de tentativas de "Phishing" que recorrem a um esquema fraudulento de mensagens SMS e chamadas telefónicas supostamente em nome da CGD, passíveis de comprometer a privacidade e a segurança de Clientes.
Os destinatários deste esquema fraudulento são induzidos a acederem incautamente a links que remetem para páginas fraudulentas na Internet, totalmente alheias à CGD, as quais visam a recolha de dados bancários e de outra informação pessoal e confidencial de clientes, para uso ilícito.
Recebem, ainda, telefonemas de burlões que, apresentando-se falsamente como colaboradores da CGD, procuram recolher códigos de autorização para validação ilícita de operações bancárias em nome dos Clientes vítimas do esquema fraudulento.
▪ Não aceda à CGD através de links em mensagens de email, SMS, endereços gravados nos "Favoritos" ou no "Histórico", nem através de anúncios ou outros resultados de pesquisas internet.
▪ Digite sempre o endereço https://www.cgd.pt no seu browser, e confirme o certificado digital da CGD. Proteja-se online e preserve as suas credenciais e os seus dados pessoais.
▪ Suspeite sempre de links e ficheiros em mensagens eletrónicas. Um email, um SMS ou uma notificação nas redes sociais, cuja origem lhe pareça familiar, pode ter propósitos fraudulentos!
▪ Não instale aplicações/software que não solicitou ou de origem desconhecida.
▪ Suspeite de solicitações sobre o seu telemóvel associado ao Caixadirecta ou a outros serviços online da Caixa. Não forneça online dados sobre o seu telemóvel (ex. número, marca, IMEI).
▪ Nunca permita a instalação de aplicações de fabricantes

desconhecidos. Desative, ou restrinja ao mínimo necessário, a conetividade bluetooth e wi-fi
▪ Suspeite da origem e do teor de mensagens e chamadas não solicitadas, e nunca forneça dados confidenciais e bancários em resposta às mesmas. Se adequado, contacte diretamente a entidade em causa através de um meio de contacto confiável.
▪ Suspeite sempre de mensagens que lhe peçam qualquer ação ou interação urgente. Não responda, não clique nos links nem abra anexos dessas mensagens.
▪ A Caixa não envia emails, sms ou notificações nas redes sociais a solicitar dados de segurança ou outra informação confidencial.
▪ A CGD não simula a execução de transações nem simula procedimentos de sincronização.
Desconfie de solicitações inusitadas da CGD.
▪ Nunca valide a adesão a serviços ou operações bancárias que não solicitou, nem forneça incautamente, num qualquer esquema fraudulento quaisquer dados de validação que lhe sejam eventualmente dirigidos por SMS ou por outra via.
▪ Em caso de dúvida ou suspeita de tentativa de fraude, contacte-nos de imediato, e não hesite em reportar eventuais burlas ou fraudes também às autoridades policiais. Consulte contactos CGD e condições em https://www.cgd.pt/Ajuda/Pages/Contactos.aspx"
31. De tudo o supra exposto, data venia, resulta que, face à prova documental e testemunhal produzida, deveriam ter sido dados como provados os pontos 7, 11 e 38 da matéria de facto provada, mas não com a redação que o foram atendendo ao acima explanado, sugerindo-se para os mesmos as redações anteriormente indicadas.
32. O facto 9 dos factos provados, não deveria ter sido como provado, pelas razões acima expostas.
33. Face à prova produzida e ao Direito aplicável o tribunal a quo deveria ter considerado que a Recorrida atuou in casu com negligência grosseira.
34. É certo que efetivamente da prova produzida, para a qual contribuiu a Recorrente em abono e sempre em favor da verdade material, a Autora sido alvo de phishing na modalidade de smishing atenta a SMS recebida que continha o link fraudulento e que terá sido utlizada pelos burlões a técnica de spoofing.
35. Contudo, contrariamente ao referido pelo tribunal a quo, o link constante da dita mensagem não era efetivamente possível verificar que este não correspondia minimamente ao site da CGD.
36. Veja-se que, como consta do ponto 6 dos factos provados, o referido link era o seguinte: atentdcgd.com, sendo que o site da CGD é www.cgd.pt, não se verificando, por isso, a mínima semelhança entre os dois domínios de internet.
37. Era, pois, com todo o respeito, possível para uma pessoa

minimente diligente descortinar a evidente diferença.
38. Pese embora a mensagem recebida pudesse aparecer no encadeamento das mensagens anteriormente rececionadas da CGD, tal como número de telefone pudesse ter aparente origem na CGD, era possível à Autora ter-se precavido deste tido de fraude em concreto atentos os alertas e avisos previamente publicados pela Recorrente.
39. Foi produzida prova de que à data dois factos ora em causa, a CGD havia alertado os seus clientes para esta fraude em concreto, isto é, para que deveriam desconfiar de SMS e telefonemas com aparente origem na CGD e mediante os quais lhes fosse pedida qualquer interação urgente nomeadamente que clicar em links.
40. A Recorrente não compreende porque motivo o tribunal a quo (o tribunal a quo não faculta explicação para tal) pode entender que a prova produzida foi suficiente para dar como provado que a Recorrente emitiu e publicou tais alertas, mas não para dar como provada a data da sua publicação data, sendo que tal prova foi efetuada nos mesmo moldes, em particular quanto ao documento 10 da Contestação, que, tratando-se de uma publicação, contém em si, como qualquer notícia, a data da sua publicação.
41. Além disso, a testemunha G… explicou que à data dos factos havia sido publicado um alerta específico para este tipo de fraude e quando confrontado com o documento 10 da Contestação, confirmou que se tratava deste anúncio que havia sido publicado em 10.07.2022.
42. Face à prova produzida tribunal a quo deveria ter considerado que em 10.07.2022 a CGD havia publicado um alerta/notícia que alertava para este tipo de fraude e com o teor que se sugere que ponto 38 dos factos provados passe a ter.
43. Caso Autora tivesse atentado no mesmo, ter-se-ia prevenido quanto a esta fraude.
44. A própria Autora admite, no contacto telefónico entre si e o Caixa Contact Center da Recorrente e consta dos factos provados, que facultou os SMS Token que foi recebendo no seu telemóvel e que não leu as mensagens concernentes à associação de outro dispositivo e consulta de saldo, mas confessa e consta do facto 39 dos factos provados que leu a mensagem a relativa à concretização da operação pagamento.
45. A autora teve capacidade presença de espírito para compreender o texto da SMS em causa tendo percebido que o que código que lhe estava a ser solicitado servia para confirmar uma operação e não para a cancelar, contrariamente ao que o burlão lhe transmitia na chamada telefónica tendo dito ao burlão que a mensagem dizia servir para efeito diferente do que aquele lhe estava a transmitir. Ainda assim a Recorrida optou por facultar esse código o que permitiu a concretização da operação de

pagamento em causa.
46. Todos os factos acima indicados, data venia, permitem concluir que contrariamente ao referido pelo tribunal a quo, a Recorrida, não agiu, com a diligência que lhe é exigida na proteção dos dados do serviço Caixa Direta que são facultados pela Recorrente aos seus Clientes utilizadores deste serviço e que são os únicos que permitem a confirmação de operações bancárias.
47. Foi gravemente negligente o comportamento adotado pela Recorrida no caso concreto.
48. Descurando todos os alertas emitidos pela CGD para situações como a ora em apreço, a Recorrida carregou no link constante da mensagem recebida para alegado bloqueio da associação de um dispositivo ao contrato e, de seguida, quando contactada telefonicamente por terceiros, lhes facultou vários elementos pessoais e intransmissíveis, como dados do seu cartão bancário e ainda os códigos SMS Token, sem a introdução dos quais a operação de pagamento em causa não teria sido validada.
49. Além disso, os SMS com códigos Token, indicavam, expressamente, visar, respetivamente, a associação de outro dispositivo móvel (desconhecido para a Reclamante) ao seu contrato de Caixa Direta, e a concretização de uma operação de pagamento que Recorrida não pretendia realizar.
50. A Recorrida, incumpriu clamorosamente com as regras de segurança amplamente divulgadas pela Ré CGD para acesso e utilização do Serviço Caixa Direta.
51. A Recorrente tem vindo a apresentar, sistematicamente, aos seus Clientes, sob a forma de janela do tipo "pop-up", na página de autenticação do Serviço (página de login), diversa informação de segurança, alertando-os para os diversos riscos de fraude de que os clientes podem ser alvo.
52. Na área de Segurança do Serviço, também estão identificados outros exemplos de fraude que têm vindo a ser conhecidas do Banco, envolvendo os ataques de "phishing" de que os Clientes são alvo para que este possam consultar tais alertas e exemplos e se possam precaver e evitar ser alvo de fraudes semelhantes.
53. A CGD publicou um específico alerta de segurança no seu site institucional, onde refere explicitamente: "…. Desconfie de solicitações inusitadas da CGD. Suspeite da origem e do teor de mensagens e chamadas não solicitadas, e nunca forneça dados confidenciais e bancários em resposta às mesmas. … Nunca valide a adesão a serviços ou operações bancárias que não solicitou, nem forneça incautamente, num qualquer esquema fraudulento quaisquer dados de validação que lhe sejam eventualmente dirigidos por SMS ou por outra via…Suspeite sempre de mensagens que lhe peçam qualquer ação ou interação urgente. Não responda, não clique nos links nem abra anexos dessas mensagens"

54. Do alerta que a Recorrente publicou no seu site institucional em 10.07.2022, constava, nomeadamente que os Clientes não devem fornecer dados do cartão matriz, nem carregar em links e que devem desconfiar sempre de massagens ou chamadas não solicitadas, incluindo das com aparente origem na CGD, nem a fornecer dados confidenciais e bancários em resposta a mensagens ou telefonemas mesmo que passam ter origem supostamente na CGD.
55. A operação ora reclamada resulta da atuação gravemente negligente da Recorrida, que colocou em causa a segurança dos elementos de identificação e de validação do Serviço Caixa Direta.
56. A CGD nunca contacta ou envia SMS'S aos clientes para os fins e nos termos descritos pela Autora e os clientes são para isso copiosamente alertados, pelo que o SMS ou o telefonema a que se refere a Recorrida nunca poderia ser considerado natural à luz do padrão do homem médio.
57. Caso a Recorrida, tivesse atentado nos avisos previamente levados a cabo pela CGD, mormente no de 10.07.2022, que alertava para uma fraude em tudo semelhante à em causa, não teria clicado no link que constava da mensagem recebida e muito menos facultado a terceiros os elementos que permitiram a concretização da fraude, nem teria introduzido dados numa página fraudulenta que, como resultou a prova produzida e acima referida, não era em nada semelhante à página de homebanking da Recorrente, pois que solicitava elementos para login que esta nunca solicita, como o numero de telemóvel e dados do cartão bancário.
58. Foi, por isso, unicamente a atuação direta da Recorrida que permitiu a concretização da fraude ora reclamada.
59. Sobre esta matéria, a da responsabilidade por operações de pagamento não autorizadas rege o Decreto-lei nº 91 /2018 de 12 de novembro, mais concretamente os seus artigos 113º e 114º, introduzindo o seu art.º 115 derrogações importantes ao regime-regra, redistribuindo o risco de utilização dos instrumentos de pagamento, através da apreciação de novos critérios.
60. Terá aplicabilidade ao caso em apreço, o disposto no nº 4 do artigo 115º do referido diploma, uma vez que, face à prova produzida, mormente a atuação direta da Recorrida, resulta evidente que a mesma agiu com negligência grosseira, motivo pelo qual, data maxima venia, deve suportar as perdas resultantes desta operação de pagamento
61. Para um bom pai de família é medianamente claro que, se não pretende realizar uma determinada operação de pagamento, então não deve introduzir os elementos de confirmação da referida operação, elementos esses que indicam, expressamente e sem margem para dúvidas, qual a operação de pagamento em concreto que visam confirmar.

62. Sobre a Recorrida enquanto utilizadora do serviço impedem não só os deveres estabelecidos no artigo 110º do acima referido Decreto-Lei, mas ainda deveres acessórios.
63. Sobre os deveres acessórios que impedem sobre os utilizadores, refere o seguinte o Acórdão do Tribunal da Relação do Porto, proferido no processo nº 16900/21.1T8PRT.P1, datado de 18.04.2023, cujo Relator foi João Ramos Lopes e que se encontra disponível em www.dgsi.pt e que em parte diz que se transcreve com particular relevância para o caso concreto: (…)
64. Também acerca do assunto e no mesmos sentido, veja-se o que refere o Acórdão do Tribunal da Relação do Porto, proferido no processo nº 22158/17.0T8PRT.P1, datado de 14.07.202 cujo Relator foi Fernando Baptista e que também se encontra disponível em, www.dgsi.pt: (…)
65. A situação sobre a qual versou ao Acórdão do STJ de 12.12.2023, proferido no processo 9240720.5T8LSB.L1.S1., trata-se de situação com contornos bem diversos e que por essa razão conduziram a que o Supremo Tribunal de Justiça entendesse naquele caso que a Cliente não havia atuado com negligência grosseira.
66. É que no caso do Acórdão foram determinantes para tal conclusão os seguintes aspetos:
• A circunstância de a Cliente ter rececionado mensagem acerca do mesmo assusto que já teria anteriormente tratado com o banco estando a ser abordada precisamente nos mesmos moldes para sua resolução, como havia sido em duas outras ocasiões passadas.
No caso ora em apreço, não existiam tais antecedentes. A Autora não alegou podia alegar que anteriormente a CGD já a havia contactado para o mesmo efeito e nos mesmo moldes, relativamente a associação de um outro dispositivo ao contrato e para carregar num link .
• Além disso o site fraudulento no caso do Acórdão era graficamente igual ao do Banco, o que não acontecia no caso concreto, como resultou a da prova produzida e do que acima se expôs.
• Acresce que o Acórdão salienta que, naquele caso, haviam sido utlizados os artifícios eletrónicos, que no caso concreto não se descortinam, resultando da prova produzida que foi usada no caso concreto engenharia social.
• O Acórdão esclarece que no caso havia sido solicitada pelos burlões uma segunda via do cartão de telemóvel da Cliente para que pudessem ter acesso direto aos SMS Token, que não lhes foram assim facultados pela Cliente, contrariamente ao caso ora em apreço.
• Por fim, o Acórdão salienta que a Cliente habitualmente só usava o homebanking para consulta, o que não é caso da ora Recorrida.

67. Face a tudo o exposto, data venia andou mal o tribunal a quo.
68. Deveria ter dado como provados os factos, 7, 11 e 38, mas com a redação acima sugerida.
69. Por sua vez, não deveria ter dado como provado o facto 9 dos factos provados pelas razões acima explanadas.
70. Atenta a prova produzida, deveria ter considerado a atuação da Autora, ora Recorrida, in casu, como grosseiramente negligente nos termos e para os efeitos do nº 4 do artigo 115º do Decreto-Lei nº 91/2018 de 12 de novembro, responsabilizando-a assim pelas perdas nos termos do ali disposto.
71. Pelas razões acima expostas, pese embora se compreenda dos prejuízos não patrimoniais que a Autora possa ter sofrido, os mesmos não são imputáveis a Recorrente, que não pode assim ser condenada como foi a suportá-los.
Nestes termos e nos demais de Direito que forem doutamente supridos pelo superior critério de V.Exªs., deve o presente Recurso ser considerado procedente, revogando-se a Sentença ora Recorrida, sendo a Recorrente absolvida dos pagamentos a que foi condenada.
Assim farão Vossas Excelências, Venerandos Juízes Desembargadores, a verdadeira e costumada Justiça! ».
A A. contra-alegou, pugnando pela improcedência da apelação.

QUESTÕES A DECIDIR
Conforme resulta dos arts. 635.º n.º4 e 639.º n.º1 do Código de Processo Civil, o objecto do recurso é delimitado pelas conclusões do recorrente, as quais desempenham um papel análogo ao da causa de pedir e do pedido na petição inicial. Ou seja, este Tribunal apenas poderá conhecer da pretensão e das questões formuladas pela recorrente nas conclusões, sem prejuízo da livre qualificação jurídica dos factos ou da apreciação das questões de conhecimento oficioso (garantido que seja o contraditório e desde que o processo contenha os elementos a tanto necessários – arts. 3.º n.º3 e 5.º n.º3 do Código de Processo Civil). Note-se que «as questões que integram o objecto do recurso e que devem ser objecto de apreciação por parte do tribunal *ad quem* não se confundem com meras considerações, argumentos, motivos ou juízos de valor. Ao tribunal *ad quem* cumpre apreciar as questões suscitadas, sob pena de omissão de pronúncia, mas não tem o dever de responder, ponto por ponto a cada argumento que seja apresentado para sua sustentação. Argumentos não são questões e é a estes que essencialmente se deve dirigir a actividade judicativa». Por outro lado, não pode o tribunal de recurso conhecer de questões novas que sejam suscitadas apenas nas alegações / conclusões do recurso – estas apenas podem incidir sobre questões que tenham sido anteriormente apreciadas, salvo os já referidos casos de questões de conhecimento oficioso, uma vez que os recursos são meros meios de impugnação das decisões

judiciais pelos quais se visa a sua reapreciação e consequente alteração e/ou revogação [cfr. António Santos Abrantes Geraldes, *Recursos em Processo Civil*, Almedina, 2022 – 7.ª ed., págs. 134 a 142; Ac. STJ de 7/7/2016, proc. 156/12, disponível em http://www.dgsi.pt].
Nessa conformidade, são as seguintes as questões que cumpre apreciar:
- impugnação da decisão acerca da matéria de facto;
- mérito da sentença recorrida, quanto à obrigação da R. de reembolso, à A., do valor de pagamento efectuado a partir da conta de depósitos à ordem de que esta era titular junto daquela;
- mérito da sentença recorrida, quanto à obrigação da R. de compensar a A. por preocupações e transtornos que a mesma tenha sofrido.

FUNDAMENTAÇÃO DE FACTO
A sentença sob recurso considerou como provados os seguintes factos:
«1. A ré é uma sociedade que tem por objecto o exercício da actividade bancária.
2. A autora era cliente da ré, titular da conta bancária à ordem a que corresponde o número …, da agência de Condeixa-a-Nova.
3. A Autora era ainda titular do Contrato de Caixadireta nº …, ao qual aderiu em 06.04.2018.
4. O número de telemóvel associado a este contrato era o número ….
5. Pelas 11h29 do dia 22/11/2022, a autora recebeu uma mensagem de texto (SMS) provinda de número de telefone identificado como pertencente à ré e que surgiu na sequência de anteriores comunicações da ré, nomeadamente com códigos para autorizar transacções ou pagamentos.
6. Tal SMS transmitia à autora o seguinte texto: "CGD: Um dispositivo desconhecido acedeu a sua conta no dia 22/11/22 se não foi você siga: atentdcgd.com".
7. Confiante, face ao nº de telefone utilizado, a autora clicou naquele link que lhe era transmitido e que deu acesso a uma página falsificada, graficamente igual à da ré, e na qual foi pedido para indicar o nº de contrato com a CGD, código de acesso (password) e de seguida o nº e nome do cartão de débito, dando de seguida indicação de erro.
8. Pelas 12h07 do mesmo dia, a autora recebeu chamada telefónica do número identificado como …, pertencente à ré, tendo-se o seu interlocutor identificado como funcionária da ré e que estaria a contactar a autora na sequência de esta ter indicado, ao carregar no link enviado, que não seria ela a aceder à conta bancária meia hora antes.
9. Aquela conversa iniciou-se com os procedimentos normais de autenticação perante a ré o que, associado ao facto de a chamada

telefónica provir de número identificado como pertencente à CGD, não levantou qualquer suspeita de que a chamada pudesse não provir da ré.
10. A conversa desenrolou-se com informação de que tinha ocorrido acesso à conta da autora e pretenderiam proceder a uma transacção no valor de 4.950,00€, mais informando que para cancelar e evitar a transacção iria receber SMS.
11. Em continuação, a autora recebeu daquele mesmo número telefónico, por SMS, códigos para autorização da operação, tudo à semelhança dos procedimentos normal e usualmente seguidos pela ré.
12. Concretamente, às 12:09:24, a autora recebeu SMS, enviada para o telemóvel associado ao Contrato de Caixadireta, com o seguinte conteúdo: "Para confirmar Associação de dispositivo ao contrato, introduza o código (…)", que a autora forneceu.
13. Este código validou a operação realizada por terceiros, às 12:09:24, correspondente à associação do dispositivo com o código ID Apple iPhone 12,1 (Nome do produto iPhone 11) ao contrato …, o contrato ora em causa.
14. Esse dispositivo ficou registado com o Token Id ….
15. E, às 12:10:29, foi realizada, na mesma sessão, a Desfidelização do Apple iPhone13,3 (desassociação do dispositivo ao contrato), que tinha o Token ….
16. Após, já com acesso à conta da autora, estes terceiros acedem ao menu de consulta de dados de segurança de cartão, onde consultam data de validade e código CVV2, solicitando para este efeito ao Cliente que faculte as coordenadas da matriz, cuja inserção o serviço solicita e ainda o código sms token, o que autora fez.
17. Com estes dados de cartão, os terceiros, através do comércio online, efectuam a compra, a qual é encaminhada para a APP, a fim de ser aprovada e solicitam ao Cliente as 3 coordenadas da matriz que estão a ser novamente aleatoriamente pedidas pelo sistema e o código sms token, o que autora forneceu.
18. Os códigos SMS Token foram enviados para o número de telemóvel com a indicação concreta das operações a que se destinavam: a associação de outro dispositivo móvel ao seu contrato de Caixadireta, a consulta dos dados de segurança do seu cartão de débito e, por fim, a concretização de uma operação de pagamento no valor de 4.950,00 €.
19. Após, terminaram a chamada telefónica com informação de que iriam passar a chamada para o departamento de segurança da ré, tendo então a chamada caído.
20. Com vista a melhor se inteirar da situação, a autora dirigiu-se nesse mesmo dia ao balcão da ré em Condeixa-a-Nova.
21. Da consulta de conta realizada nessa altura, o valor de 4.950,00€ encontrava-se identificado como cativo.
22. A autora solicitou que tal transacção não fosse concretizada

tendo-lhe sido dito pelo funcionário da ré que o cancelamento já não era possível.
23. A autora deslocou-se então às instalações de Coimbra da Polícia Judiciária onde efectuou participação do sucedido tendo enviado à ré, nesse mesmo dia 22/11/2022, comprovativo da presença naquela entidade.
24. Nessa sequência, a ré comunicou à autora que iria iniciar o processo de fraude mas não podia inibir o pagamento, esclarecendo que se trata de pagamento associado a cartão de crédito, já realizado ao fornecedor, e que o valor aparecia cativo na conta mas o pagamento já havia sido concretizado.
25. Após informação da ré de que o pagamento tinha sido realizado à plataforma Binance, a autora solicitou que a ré contactasse tal entidade de modo a que cativassem o valor, pedido este em que insistiu em 28/11/2022 e em 29/11/2022, sem que obtivesse qualquer resposta.
26. Em 25.11.2022, foi inserido um processo de fraude a que coube o n.º…, pela agência de Vila Nova de Gaia.
27. Na sequência da instauração do processo de fraude, a ré creditou na conta da autora o valor correspondente à operação sobre a qual incidia a indicação de tratar-se de fraude.
28. Contudo, após conclusão do processo, verificou que a transação tinha sido autenticada através da APP Caixadireta, pelo que procedeu novamente ao débito do respetivo valor, por ter considerado que a Autora foi responsável pela mesma.
29. O movimento em causa trata-se de um pagamento com cartão, no valor de 4.950,00 € e não de uma transferência bancária.
30. O pagamento em apreço não é passível de recuperação a partir do momento em que é imputado ("em autorização" ou "cativo"), uma vez que, nesse momento, já foi pago à Entidade destinatária e debitado ao cartão do Cliente, in casu, ao cartão da Autora.
31. O processamento de compras com as Redes (VISA e Mastercard) é feito via sistema de Dual Message, isto é, no momento da compra é efetuado um pedido de autorização ao banco emissor que valida o cartão e os saldos disponíveis e cativa esse montante.
32. Desde o momento da aprovação da autorização, o banco emissor (no caso concreto a CGD) é responsável pelo pagamento do montante à rede, uma vez que esta já adiantou o montante ao comerciante.
33. A operação em causa não foi afectada por avaria técnica ou qualquer outra deficiência do serviço.
34. A Ré realiza diversas campanhas de alerta de fraudes informáticas, alertando para a circunstância de que mensagens com aspecto e teor em tudo semelhantes à ora em causa e que terá sido rececionada pela Autora, não são da sua proveniência.

35. A Ré tem vindo a apresentar, sistematicamente, aos Clientes, sob a forma de janela do tipo "pop-up", na página de autenticação do Serviço (página de login), diversa informação de segurança, alertando-os para os diversos riscos de fraude de que os clientes podem ser alvo.
36. Na área de Segurança do Serviço, também estão identificados outros exemplos de fraude que têm vindo a ser conhecidas do Banco, envolvendo os ataques de "phishing" de que os Clientes são alvo.
37. A ré publicou um específico alerta de segurança no seu site institucional, onde refere explicitamente: "…. Desconfie de solicitações inusitadas da CGD. Suspeite da origem e do teor de mensagens e chamadas não solicitadas, e nunca forneça dados confidenciais e bancários em resposta às mesmas. … Nunca valide a adesão a serviços ou operações bancárias que não solicitou, nem forneça incautamente, num qualquer esquema fraudulento quaisquer dados de validação que lhe sejam eventualmente dirigidos por SMS ou por outra via…Suspeite sempre de mensagens que lhe peçam qualquer ação ou interação urgente. Não responda, não clique nos links nem abra anexos dessas mensagens"
38. A ré publicou no seu site institucional acessível ao público, na área relativa à segurança um anúncio que alertava para este tipo de fraude, com os seguintes avisos:
- Não aceda à CGD através de links em mensagens de email, SMS, endereços gravados nos "Favoritos" ou no "Histórico", nem através de anúncios ou outros resultados de pesquisas internet.
- Digite sempre o endereço https://www.cgd.pt no seu browser, e confirme o certificado digital da CGD. Proteja-se online e preserve as suas credenciais e os seus dados pessoais.
- Suspeite sempre de links e ficheiros em mensagens eletrónicas. Um email, um SMS ou uma notificação nas redes sociais, cuja origem lhe pareça familiar, pode ter propósitos fraudulentos!
- Suspeite da origem e do teor de mensagens e chamadas não solicitadas, e nunca forneça dados confidenciais e bancários em resposta às mesmas. Se adequado, contacte diretamente a entidade em causa através de um meio de contacto confiável.
- Para sua proteção, não aceda a links enviados por SMS ou e-mail.
- Suspeite sempre de mensagens que lhe peçam qualquer ação ou interação urgente.
- Não responda, não clique nos links nem abra anexos dessas mensagens.
- A Caixa não envia emails, sms ou notificações nas redes sociais a solicitar dados de segurança ou outra informação confidencial
- A CGD não simula a execução de transações nem simula procedimentos de sincronização.
- Desconfie de solicitações inusitadas da CGD.

- Nunca valide a adesão a serviços ou operações bancárias que não solicitou, nem forneça incautamente, num qualquer esquema fraudulento quaisquer dados de validação que lhe sejam eventualmente dirigidos por SMS ou por outra via.
39. No contacto telefónico realizado pela autora para a ré, a mesma assumiu que facultou os SMS Token que foi recebendo no seu telemóvel e que não leu as mensagens concernentes à associação de outro dispositivo e consulta de saldo, mas que leu a mensagem relativa à concretização da operação pagamento, nos seguintes termos:
"A única mensagem que eu li foi a última e, foi a mensagem que eu estive mesmo para não dar o código e, disse três vezes à senhora que isto dizia exatamente o oposto do que ela me estava a dizer. Mas lá me deixei persuadir na mesma á quarta vez e acabei por dar o código e, foi o derradeiro, mas foi a única mensagem que eu li na altura. Portanto só depois de desligar a chamada é que comecei a ler as outras mensagens e percebi que … pronto, que alguma coisa tinha acontecido"
"Facultei sim, apesar de ter achado estranho e, na altura ter dito à senhora que isto dizia exatamente … pronto isto dizia… que eu ia aprovar um pagamento e que eu não queria aprovar pagamento nenhum. Pronto mas não me valeu de nada, não é? Aaa… acabei por dar na mesma."
40. A situação em causa, o facto de se ver privada da quantia de €4.950,00, e a posição da ré quanto ao sucedido, em muito tem preocupado e transtornado a autora».
A decisão recorrida considerou como não provados os seguintes factos:
«1. A A. nunca indicou ao seu interlocutor a password de acesso à sua área pessoal, password que sempre seria necessária à movimentação de valores efectuada nem nunca indicou qualquer outra informação que autorizasse a transacção efectuada.
2. Apesar de autora ter comunicado à ré não ter realizado a operação, tratando-se de fraude, a ré persistiu em não cancelar a operação, vindo a autorizar a mesma, autorizando assim a saída da conta bancária da autora daquela quantia de 4.950,00€.
3. A ré poderia ter mantido o valor cativo até ao esclarecimento da situação».

APRECIAÇÃO DO MÉRITO DO RECURSO:

<u>Da impugnação da decisão acerca da matéria de facto</u>
Nos termos do art. 662.º n.º1 do Código de Processo Civil, a Relação deve alterar a decisão proferida sobre a matéria de facto, se os factos tidos como assentes, a prova produzida ou um documento superveniente impuserem decisão diversa.
Como refere António Santos Abrantes Geraldes (*Recursos em Processo Civil*, 7.ª ed., págs. 333 e ss.), «sem embargo da

correcção, mesmo a título oficioso, de determinadas patologias que afectam a decisão da matéria de facto (*v.g.* contradição) e também sem prejuízo do ónus de impugnação que recai sobre o recorrente e que está concretizado nos termos previstos no art. 640.º, quando esteja em causa a impugnação de determinados factos cuja prova tenha sido sustentada em meios de prova submetidos a livre apreciação, a Relação deve alterar a decisão da matéria de facto sempre que, no seu *juízo autónomo*, os elementos de prova que se mostrem acessíveis determinem uma solução diversa, designadamente em resultado da reponderação dos documentos, depoimentos e relatórios periciais, complementados ou não pelas regras de experiência». A modificação deverá, ainda, ocorrer sempre que «o tribunal recorrido tenha desrespeitado a força plena de certo meio de prova» ou «quando for apresentado pelo recorrente *documento superveniente* que imponha decisão diversa».

Conforme resulta dos arts. 341.º do Código Civil e 607.º n.º5 do Código de Processo Civil, tendo as provas por função «a demonstração da realidade dos factos», «o juiz aprecia livremente as provas segundo a sua prudente convicção acerca de cada facto», embora a livre apreciação não abranja «os factos para 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».

Assim, desde que para a prova não exista norma legal que exija formalidade especial ou prova documental, e desde que não se trate de matéria provada plenamente, seja por documento, confissão ou acordo das partes, as provas produzidas estão sujeitas ao princípio da livre apreciação pelo tribunal.

Claro que livre apreciação não equivale a arbitrariedade, e é por isso que o n.º4, do mesmo art. 607.º, exige que o juiz analise criticamente a prova e indique todos os elementos que foram decisivos, assim objectivando [e tornando sindicável] a sua convicção.

Nesse sentido, para que um facto se considere provado, tem-se vindo a exigir que a prova produzida preencha o chamado *standard da prova* (nível mínimo de corroboração de uma hipótese para que esta possa ser aceite como verdadeira) que vigora em processo civil, que é o da probabilidade prevalecente[1]. Ou seja, consideradas as regras do ónus da prova (art. 342.º do Código Civil), é necessário que, a partir das provas produzidas, a versão constante destes pontos da sentença mereça uma confirmação lógica maior do que a versão contrária. Se assim não for, tais factos têm de considerar-se não provados (cfr. art. 414.º do Código de Processo Civil).

Acresce que, como se refere no Ac. RP de 21/6/2021 (proc.

2479/18, disponível em http://www.dgsi.pt), «mantendo-se em vigor, em sede de Recurso, os princípios da imediação, da oralidade, da concentração e da livre apreciação da prova, e guiando-se o julgamento humano por padrões de probabilidade e nunca de certeza absoluta, o uso, pelo Tribunal da Relação, dos poderes de alteração da decisão da 1.ª instância sobre a matéria de facto só deve ser efectuado quando seja possível, com a necessária segurança, concluir pela existência de erro de apreciação relativamente a concretos pontos de facto impugnados. Assim, a alteração da matéria de facto só deve ser efectuada pelo Tribunal da Relação, quando este Tribunal, depois de proceder à audição efectiva da prova gravada, conclua, com a necessária segurança, no sentido de que os depoimentos prestados em audiência final, conjugados com a restante prova produzida, apontam em direcção diversa, e delimitaram uma conclusão diferente daquela que vingou na primeira Instância». Particularmente no caso da prova testemunhal e por declarações de parte (e desde que não estejamos perante factos de prova vinculada), é de salientar que, havendo vários depoimentos / declarações contraditórios entre si, as regras da sua apreciação não são matemáticas, ou seja, um facto não é considerado provado ou não provado consoante exista um maior ou menor número de pessoas a afirmá-lo ou a contrariá-lo. Ainda que apenas uma pessoa afirme um facto, enquanto todas as outras o negam, e ainda que várias pessoas afirmem um facto, enquanto apenas uma o nega, esse facto pode ser considerado provado / não provado, conforme a apreciação que seja feita dos depoimentos / declarações, com base na sua credibilidade, coerência, isenção, razão de ciência, distanciamento, conjugação com outros meios de prova (v.g., documental) e conjugação com as regras da experiência. Aliás, ainda que todas as pessoas ouvidas afirmem determinado facto, o mesmo pode ser considerado não provado - basta que os depoimentos / declarações não sejam credíveis (porque, por exemplo, as pessoas têm interesse na decisão da causa e não se mostraram objectivas na sua narração, o seu conhecimento não é directo, os depoimentos / declarações foram contraditórios ou foram de tal forma coincidentes que se afiguram «ensaiados», não é possível que aquelas pessoas, nas circunstâncias concretas, tivessem conhecimento daqueles factos…). E não se pode olvidar que o tribunal de primeira instância se encontra em posição privilegiada para levar a cabo tal tarefa de apreciação, ponderação e discernimento, uma vez que contacta directa e presencialmente (ou, mesmo que à distância, com imagem) com as pessoas ouvidas e, portanto, pode aperceber-se dos aspectos relevantes da linguagem não verbal – expressões faciais, postura, gestos, hesitações. Significa isto que, salvo casos de flagrante erro de avaliação por parte do tribunal de primeira instância (*v.g.*, uma testemunha em que o tribunal se

baseou claramente está a efabular, o seu depoimento é contrariado por prova documental ou pericial fiável, os factos que narrou não podiam – de acordo com as regras da experiência ou outras – ter acontecido daquela forma, aquilo que disse não foi o que o tribunal entendeu…), não há que alterar a matéria de facto fixada na sentença. Dito de outra forma, em caso que não seja de prova legal, deve confiar-se na avaliação efectuada em primeira instância, a não ser que a prova produzida implique, necessariamente, decisão diversa.
Note-se, também, que «quando a apreciação da impugnação deduzida contra a decisão de facto da 1.ª instância seja, de todo, irrelevante para a solução jurídica do pleito, ainda que a tal impugnação satisfaça os requisitos formais prescritos no art. 640.º n.º1 do Código de Processo Civil, não se justifica que a Relação tome conhecimento dela, à luz do disposto no art. 608.º n.º2 do Código de Processo Civil» (cfr. Ac. STJ de 23/1/2020, proc. 4172/16, disponível em https://jurisprudencia.csm.org.pt) [2]. Caso contrário, estaríamos a praticar um acto inútil, proibido à luz do art. 130.º, do mesmo diploma.
Balizadas que estão as regras que nos orientarão, passemos à apreciação da pretensão do recorrente, que é a seguinte:
A - A redacção do ponto 7 dos factos provados [«Confiante, face ao nº de telefone utilizado, a autora clicou naquele link que lhe era transmitido e que deu acesso a uma página falsificada, graficamente igual à da ré, e na qual foi pedido para indicar o nº de contrato com a CGD, código de acesso (password) e de seguida o nº e nome do cartão de débito, dando de seguida indicação de erro»] seja alterada para «A autora clicou naquele link que lhe era transmitido e que deu acesso a uma página falsificada que não era semelhante à página de homebanking da Ré e na qual foi pedido para indicar o nº de contrato com a CGD, código de acesso (password) e de seguida o nº e nome do cartão de débito, dando de seguida indicação de erro»;
B - Seja considerada não provada a matéria constante do ponto 9 dos factos provados [«Aquela conversa iniciou-se com os procedimentos normais de autenticação perante a ré o que, associado ao facto de a chamada telefónica provir de número identificado como pertencente à CGD, não levantou qualquer suspeita de que a chamada pudesse não provir da ré»];
C - O ponto 11 dos factos provados [«Em continuação, a autora recebeu daquele mesmo número telefónico, por SMS, códigos para autorização da operação, tudo à semelhança dos procedimentos normal e usualmente seguidos pela ré»] passe a ter a seguinte redacção: «Em continuação, a autora recebeu daquele mesmo número telefónico, por SMS, códigos para autorização da operação, tudo à semelhança dos procedimentos normal e usualmente seguidos pela ré para a confirmação de operações»;

D - O ponto 38 dos factos provados [«A ré publicou no seu site institucional acessível ao público, na área relativa à segurança um anúncio que alertava para este tipo de fraude, com os seguintes avisos:
- Não aceda à CGD através de links em mensagens de email, SMS, endereços gravados nos "Favoritos" ou no "Histórico", nem através de anúncios ou outros resultados de pesquisas internet.
- Digite sempre o endereço https://www.cgd.pt no seu browser, e confirme o certificado digital da CGD. Proteja-se online e preserve as suas credenciais e os seus dados pessoais.
- Suspeite sempre de links e ficheiros em mensagens eletrónicas. Um email, um SMS ou uma notificação nas redes sociais, cuja origem lhe pareça familiar, pode ter propósitos fraudulentos!
- Suspeite da origem e do teor de mensagens e chamadas não solicitadas, e nunca forneça dados confidenciais e bancários em resposta às mesmas. Se adequado, contacte diretamente a entidade em causa através de um meio de contacto confiável.
- Para sua proteção, não aceda a links enviados por SMS ou e-mail.
- Suspeite sempre de mensagens que lhe peçam qualquer ação ou interação urgente.
- Não responda, não clique nos links nem abra anexos dessas mensagens.
- A Caixa não envia emails, sms ou notificações nas redes sociais a solicitar dados de segurança ou outra informação confidencial
- A CGD não simula a execução de transações nem simula procedimentos de sincronização.
- Desconfie de solicitações inusitadas da CGD.
- Nunca valide a adesão a serviços ou operações bancárias que não solicitou, nem forneça incautamente, num qualquer esquema fraudulento quaisquer dados de validação que lhe sejam eventualmente dirigidos por SMS ou por outra via»] passe a ter a seguinte redacção: «Em 10.07.2022, a ré publicou no seu site institucional acessível ao público, na área relativa à segurança, um anúncio que alertava para este tipo de fraude, com os seguintes avisos:
Dá-se conhecimento de tentativas de "Phishing" que recorrem a um esquema fraudulento de mensagens SMS e chamadas telefónicas supostamente em nome da CGD, passíveis de comprometer a privacidade e a segurança de Clientes.
Os destinatários deste esquema fraudulento são induzidos a acederem incautamente a links que remetem para páginas fraudulentas na Internet, totalmente alheias à CGD, as quais visam a recolha de dados bancários e de outra informação pessoal e confidencial de clientes, para uso ilícito.
Recebem, ainda, telefonemas de burlões que, apresentando-se falsamente como colaboradores da CGD, procuram recolher códigos de autorização para validação ilícita de operações

bancárias em nome dos Clientes vítimas do esquema fraudulento.
▪ Não aceda à CGD através de links em mensagens de email, SMS, endereços gravados nos "Favoritos" ou no "Histórico", nem através de anúncios ou outros resultados de pesquisas internet.
▪ Digite sempre o endereço https://www.cgd.pt no seu browser, e confirme o certificado digital da CGD. Proteja-se online e preserve as suas credenciais e os seus dados pessoais.
▪ Suspeite sempre de links e ficheiros em mensagens eletrónicas. Um email, um SMS ou uma notificação nas redes sociais, cuja origem lhe pareça familiar, pode ter propósitos fraudulentos!
▪ Não instale aplicações/software que não solicitou ou de origem desconhecida.
▪ Suspeite de solicitações sobre o seu telemóvel associado ao Caixadirecta ou a outros serviços online da Caixa. Não forneça online dados sobre o seu telemóvel (ex. número, marca, IMEI).
▪ Nunca permita a instalação de aplicações de fabricantes desconhecidos. Desative, ou restrinja ao mínimo necessário, a conetividade bluetooth e wi-fi
▪ Suspeite da origem e do teor de mensagens e chamadas não solicitadas, e nunca forneça dados confidenciais e bancários em resposta às mesmas. Se adequado, contacte diretamente a entidade em causa através de um meio de contacto confiável.
▪ Suspeite sempre de mensagens que lhe peçam qualquer ação ou interação urgente. Não responda, não clique nos links nem abra anexos dessas mensagens.
▪ A Caixa não envia emails, sms ou notificações nas redes sociais a solicitar dados de segurança ou outra informação confidencial.
▪ A CGD não simula a execução de transações nem simula procedimentos de sincronização.
Desconfie de solicitações inusitadas da CGD.
▪ Nunca valide a adesão a serviços ou operações bancárias que não solicitou, nem forneça incautamente, num qualquer esquema fraudulento quaisquer dados de validação que lhe sejam eventualmente dirigidos por SMS ou por outra via.
▪ Em caso de dúvida ou suspeita de tentativa de fraude, contacte-nos de imediato, e não hesite em reportar eventuais burlas ou fraudes também às autoridades policiais. Consulte contactos CGD e condições em https://www.cgd.pt/Ajuda/Pages/Contactos.aspx».
Vejamos.
Quanto à matéria referida em A) supra, a mesma foi alegada no art. 6.º da petição inicial («Confiante, face ao nº de telefone utilizado, a A. clicou naquele link que lhe era transmitido e que deu acesso a uma página graficamente igual à da R. (…)»), que a R. impugnou, por desconhecimento (cfr. art. 9.º da contestação).
A este respeito, o tribunal *a quo* justificou a sua convicção da seguinte forma:
«A prova dos factos n.ºs 5 a 26 e 40 resultou da análise dos

elementos probatórios produzidos pela autora e pela ré, os quais conjugados permitiram apreender a sucessão dos eventos que levaram à concretização do movimento não reconhecido pela autora.
A autora prestou declarações de parte através da quais relatou a sequência de acontecimentos ocorridos no dia 22.11.2022 e que levaram à realização da transacção aqui em causa. Relatou também as diligências que realizou seguidamente na tentativa de resolver a questão e recuperar o valor que foi debitado na sua conta, contudo, sem sucesso.
Transmitiu igualmente a preocupação e transtorno que toda a situação acarretou, quer pelo valor que lhe foi subtraído, que para si é muito relevante, quer pela actuação da ré e ausência de resposta às suas solicitações.
O seu depoimento foi confirmado pela testemunha, H…, seu amigo, com quem partilhou de imediato o sucedido e que a acompanhou na resolução da questão.
A sucessão dos acontecimentos e diligências realizadas pela autora são igualmente corroboradas pela documentação junta aos autos, concretamente pelos documentos n.ºs 1 e 2 juntos com a petição inicial - comprovativos das SMS e contacto telefónico recebidos, bem como do pagamento realizado; pelos documentos n.ºs 4 e 5 - comprovativos da apresentação da queixa na Policia Judiciária e resposta da ré quanto à impossibilidade de reversão da transacção, e pelos documentos n.ºs 10 e 11 - comprovativos da reclamação apresentada junto da ré e das insistências por resposta às questões colocadas.
O esquema fraudulento de que a autora foi vítima, as SMS recebidas, e as concretas operações realizados na conta de homebanking da autora foram também relatados pelas testemunhas G… e E…, funcionários da ré, que esclareceram a actuação e mecanismos utilizados pelos terceiros na concretização da fraude e a impossibilidade de a ré obstar aos mesmos.
A testemunha E… acentuou que a concretização da transacção apenas foi possível porque a autora forneceu as suas credenciais de acesso à conta de homebanking, incluindo a password, sem a qual os burlões não conseguiriam aceder à conta e dar seguimento aos passos seguintes da fraude e a qual não é acessível por qualquer outra forma, em face da forma de encriptação utilizada.
O seu depoimento, resultante do conhecimento adquirido no exercício de funções na área de segurança e prevenção de fraude na banca online como técnico de informática, mostrou-se coerente, objectivo e elucidativo, pelo que convenceu o Tribunal.
Assim, as declarações da autora, que negou ter cedido a sua password, não sendo corroboradas por qualquer outro meio, e sendo claramente infirmadas pelas explicações fornecidas pela testemunha, foram insuficientes, nesta parte, para convencer o

Tribunal, motivo pelo qual foi considerado como provada a divulgação da password no facto nº 7 e como não provado o facto n.º1».
Por seu turno, a recorrente pretende que não se pode considerar provado que a A. tenha clicado no *link* por estar confiante, face ao número utilizado, nem que a página a que acedeu fosse graficamente igual à da R., devendo considerar-se provado que o grafismo dessa página divergia do da sua. Alega que, por um lado, dizer que a A. estava confiante, face ao número de telefone utilizado, é um juízo conclusivo que contém a solução do pleito. E, por outro lado, das declarações da A. não resulta que a página fraudulenta que se apresentou fosse graficamente igual à da R., já que os elementos de identificação pedidos eram diversos.
Não assiste razão à recorrente.
Em primeiro lugar, porque a A., nas suas declarações de parte, disse que estava a trabalhar e recebeu um SMS da Caixa Geral de Depósitos (sendo certo que do facto provado n.º5 já consta que o número aparecia identificado como pertencente à R.). Daqui se infere que confiou que aquele SMS tinha sido, efectivamente, remetido pela R.. Ora, tal afirmação não contém qualquer juízo conclusivo.
Efectivamente, como refere o Prof. Alberto dos Reis (*in Código de Processo Civil Anotado*, vol III, 4ª ed., págs. 206-207) «é questão de facto tudo o que tende a apurar quaisquer ocorrências da vida real, quaisquer eventos materiais e concretos, quaisquer mudanças operadas no mundo exterior» e «é questão de direito tudo o que respeita à interpretação e aplicação da lei». Ou seja, há matéria de direito «sempre que, para se chegar a uma solução, se torna necessário recorrer a uma disposição legal» e «há matéria de facto quando o apuramento das realidades se faz todo à margem da aplicação directa da lei, isto é, quando se trata de averiguar factos cuja existência ou não existência não depende da interpretação a dar a nenhuma norma jurídica». «Reduzido o problema à sua simplicidade, a fórmula é esta: a) é questão de facto determinar o que aconteceu; b) é questão de direito determinar o que quer a lei, ou seja a lei substantiva, ou seja a lei de processo».
Face a estes ensinamentos, facilmente verificamos que determinar se a A. confiou, ou não, em que poderia clicar no *link*, por o número de telefone pertencer à R., é uma questão de facto, porque visa apurar o que efectivamente aconteceu na realidade, não implicando qualquer juízo de direito, ou seja, o recurso a uma qualquer norma legal. Questão diversa - essa sim, contendo um juízo jurídico -, mas sobre a qual não se pronuncia o ponto 7 dos factos provados, é a de saber se essa confiança era, ou não, justificada.
Além disso, a A. afirmou que, depois de clicar no *link*, abriu

«uma página da Caixa Geral de Depósitos, aparentemente[3]». Referiu, ainda, que o «layout» era muito similar ao da R. - as cores, os logotipos. Ora, se a aparência (ou seja, o aspecto exterior apresentado[4]) era a de que a página era da R., é forçoso que o grafismo fosse idêntico em ambas as páginas, caso contrário, a aparência seria diversa. Por outro lado, não foi produzida qualquer prova que tenha contrariado, nessa parte, as declarações da A., sendo certo que não vemos razões para não lhes conferir credibilidade (aliás, se o grafismo fosse diverso, certamente que a A. se teria apercebido de imediato de que estava perante uma página falsa). Claro que a testemunha E… (funcionário da R. na área de segurança, informação e prevenção de fraude) disse que as páginas não são semelhantes, mas apenas porque as informações pedidas são diversas. Ora, a circunstância, de eventualmente, terem sido pedidos dados diferentes daqueles que costumavam ser pedidos na página da R. não significa que a apresentação gráfica desses pedidos (e dos outros elementos) não fosse a mesma, já que o grafismo se reporta à forma (à aparência) e não ao conteúdo. Note-se, ainda, que o facto provado n.º7 se refere à primeira página que abriu após a A. ter clicado no link (e essa a testemunha E… disse que é igual) e não às páginas abertas subsequentemente.

Portanto, deve manter-se a redacção do ponto 7 dos factos provados, nessa medida improcedendo a impugnação da decisão de facto.

Em relação à alínea B) supra, pretende a recorrente que os factos constantes do ponto 9 da sentença [«Aquela conversa iniciou-se com os procedimentos normais de autenticação perante a ré o que, associado ao facto de a chamada telefónica provir de número identificado como pertencente à CGD, não levantou qualquer suspeita de que a chamada pudesse não provir da ré»] não podem considerar-se provados.

A seu ver, estes factos contêm em si mesmos um juízo de direito (na parte em que se refere que «não levantou qualquer suspeita de que a chamada pudesse não provir da R.») e, de acordo com a descrição feita pela A., não ocorreram procedimentos de autenticação.

Compulsadas as declarações de parte da A., efectivamente a mesma não mencionou a existência de quaisquer «procedimentos normais de autenticação» (expressão que, aliás, é vaga, desconhecendo-se quais são esses concretos procedimentos). A A. limitou-se a dizer que recebeu uma chamada, de alguém que se identificou como funcionário da Caixa Geral de Depósitos, e que pretendia evitar que entrassem na sua conta. Conversaram, no decurso da conversa a A. foi ao computador e confirmou que o número que fez a chamada pertencia à R., após o que foi recebendo mensagens da R., com códigos, os quais a A. foi

fornecendo à interlocutora, que lhe afirmara que tais códigos visavam evitar uma transferência fraudulenta. Nem a A., nem as testemunhas ouvidas mencionaram que tenham sido efectuados procedimentos de autenticação no início da conversa (o que, quanto às testemunhas, é natural, dado que nenhuma assistiu ao telefonema).
Deste modo, não tendo sido confirmada por nenhuma das provas produzidas, deve ser eliminada do ponto 9 dos factos provados a alusão à existência dos «procedimentos normais de autenticação».
Já quanto à circunstância de a A. não ter desconfiado de que a chamada pudesse não provir da R., atentas as suas declarações de parte, é forçoso considerá-la provada (a A. foi mesmo confirmar se o número de telefone pertencia à R.), sendo certo que, conforme já referimos supra, a inexistência de suspeitas da parte da A. é uma questão de facto (dado que se reporta a uma realidade, não implicando o recurso a qualquer norma legal).
Questão diversa - e, essa sim, jurídica, mas que não é aflorada no ponto 9 da matéria de facto - é saber se a A. devia, ou não, ter suspeitado de que o telefonema não provinha da R..
Procede, assim, parcialmente, a impugnação da decisão de facto, passando o ponto 9 a ter a seguinte redacção:
«Aquela conversa iniciou-se e, pelo facto de a chamada telefónica provir de número identificado como pertencente à CGD, não levantou à A. qualquer suspeita de que a chamada pudesse não provir da ré».
Quanto à alínea C) supra, o acrescento pretendido pela recorrente é um mero preciosismo, sendo espúrio, porque já está subentendido. Com efeito, se se refere que a A. recebeu códigos para autorização da operação, à semelhança dos procedimentos usualmente seguidos pela R., já se sabe que aqueles procedimentos usuais se referem à autorização de operações.
Nada há, assim, a alterar no ponto 11 dos factos provados.
Finalmente, quanto à matéria mencionada na alínea D) supra, o tribunal recorrido justificou a sua fixação da seguinte forma:
«Os factos n.ºs 34 a 38 resultaram do depoimento da testemunha G…, que confirmou a realização de alertas frequentes pela ré quanto a situações de fraude, nomeadamente através de janelas de pop up que abrem quanto se entra no site. Referiu ainda que na altura dos factos havia um alerta específico para este tipo de fraude.
Tais alertas são também confirmados pelos documentos n.ºs 7 a 10 juntos com a contestação.
Destes elementos não é, contudo, possível identificar com segurança a data em que os avisos foram inseridos na página de homebanking da ré (a sua inserção não é atestada pela mera indicação de uma data no próprio documento), nem se os mesmos foram remetidos por alguma forma à autora, nem que sejam igualmente publicados na App».

Ora, em primeiro lugar, diga-se que, tendo-se dado credibilidade ao teor do documento 10 da contestação, cujo conteúdo foi confirmado pelo depoimento da testemunha G… [o qual, sendo funcionário da R. desde 2001 (exercendo funções na área de análise de fraudes desde 2006), explanou os factos (de que tinha conhecimento directo) de modo claro e coerente], não vemos qualquer razão para não se conferir credibilidade à data da publicação aposta nesse documento, sendo certo que não existem quaisquer indícios (nem foi produzida qualquer prova nesse sentido) de que a aposição dessa data tenha sido manipulada.
Justifica-se, assim, acrescentar ao ponto 38 dos factos provados que a publicação aí referida ocorreu em 10/7/2022.
Já não se justifica - ao contrário do que pretende a recorrente - reproduzir o conteúdo de todo o documento n.º10 da contestação. É que os documentos não são factos, mas sim meios de prova dos factos que tiverem sido alegados (e que houve a oportunidade de a outra parte contraditar). Ora, no art. 118.º da contestação, a R. alegou que publicou determinados avisos, que são, precisamente, os que constam do ponto 38 da sentença, pelo que não há que acrescentar a publicação de outros avisos não alegados naquela peça processual (nem em qualquer outro articulado).
Procede, pois, de forma meramente parcial a impugnação da decisão de facto quanto ao ponto 38 da matéria provada, a qual passará a ter a seguinte redacção:
«Em 10/7/2022, a ré publicou no seu site institucional acessível ao público, na área relativa à segurança um anúncio que alertava para este tipo de fraude, com os seguintes avisos:
- Não aceda à CGD através de links em mensagens de email, SMS, endereços gravados nos "Favoritos" ou no "Histórico", nem através de anúncios ou outros resultados de pesquisas internet.
- Digite sempre o endereço https://www.cgd.pt no seu browser, e confirme o certificado digital da CGD. Proteja-se online e preserve as suas credenciais e os seus dados pessoais.
- Suspeite sempre de links e ficheiros em mensagens eletrónicas. Um email, um SMS ou uma notificação nas redes sociais, cuja origem lhe pareça familiar, pode ter propósitos fraudulentos!
- Suspeite da origem e do teor de mensagens e chamadas não solicitadas, e nunca forneça dados confidenciais e bancários em resposta às mesmas. Se adequado, contacte diretamente a entidade em causa através de um meio de contacto confiável.
- Para sua proteção, não aceda a links enviados por SMS ou e-mail.
- Suspeite sempre de mensagens que lhe peçam qualquer ação ou interação urgente.
- Não responda, não clique nos links nem abra anexos dessas mensagens.
- A Caixa não envia emails, sms ou notificações nas redes sociais a solicitar dados de segurança ou outra informação confidencial

- A CGD não simula a execução de transações nem simula procedimentos de sincronização.
- Desconfie de solicitações inusitadas da CGD.
- Nunca valide a adesão a serviços ou operações bancárias que não solicitou, nem forneça incautamente, num qualquer esquema fraudulento quaisquer dados de validação que lhe sejam eventualmente dirigidos por SMS ou por outra via».

Do mérito da decisão recorrida:
Os presentes autos reportam-se às consequências que a A. pretende fazer extrair do invocado incumprimento, por parte da R., de determinado contrato de utilização de *homebanking*, associado a conta de depósito à ordem de que era titular.
A este respeito, provou-se, antes de mais, que, a A. era titular, junto da R., de conta bancária à ordem, com o n.º…, da agência de Condeixa-a-Nova.
«O contrato de abertura de conta[5] consiste num acordo estabelecido entre uma entidade bancária e um cliente "através do qual se constitui, disciplina e baliza a respectiva relação jurídica bancária". Assim, este contrato constitui o ponto de partida[6] para o complexo contratual que compõe a relação bancária e opera como "fio condutor e integrador dos diferentes negócios concretos que as partes venham a celebrar." A abertura de conta caracteriza-se por se tratar de um contrato atípico embora correspondendo, hoje em dia, a um tipo social cuja disciplina jurídica assenta nas cláusulas contratuais gerais e nos usos bancários. (…) Tendo em vista o início de uma relação contratual duradoura como é a relação bancária, através da abertura de conta, o banco pretende definir e determinar as suas bases gerais, deixando em aberto a celebração de ulteriores contratos bancários. Por essa razão, o seu clausulado inclui regras que extravasam o contrato singular, fazendo referência a "produtos comercializados" pela entidade bancária e que dependem da vontade do cliente, apontando, desta forma, para o intuito de iniciar uma relação mais complexa. Contudo, isto não significa que da abertura de conta derivam deveres de contratar no futuro, apesar de se poder identificar deveres de disponibilidade para negociar e mesmo de negociação. (…) A relação contratual bancária criada entre o banco e o cliente apenas irá alcançar densidade económica e negocial através da celebração futura de vários contratos bancários especiais e renovar-se-á sucessivamente através da movimentação da conta. Estes contratos bancários referidos são, por exemplo, o contrato de depósito, de abertura de crédito, de emissão de cartão e de *home banking*, e inserem-se no conteúdo contratual complexo do contrato de abertura de conta, qualificando-se como convenções acessórias embora mantendo a sua autonomia[7]».

É assim que a relação contratual emergente do contrato de abertura de conta, que tradicionalmente se desenrolava apenas mediante sucessivos depósitos e levantamentos de dinheiro, tem-se vindo a complexificar, dando origem a uma rede negocial que constitui a relação bancária, onde se inserem outras figuras contratuais, associadas ao contrato de abertura de conta e com o mesmo interligadas, constituindo uma união de contratos. Tal complexo negocial tem por base «o convénio principal e (…) vai ter a sua existência e razão de ser no mesmo, continuando o banco a ter a obrigação de guardar o dinheiro depositado, restituindo-o quando e se lhe for solicitado; sobre os depositantes [e sobre o depositário], poderão acrescer outros deveres, consoante as obrigações que forem assumindo (…) por via» de outras relações «negociais encetadas e às quais podem ter acesso por serem titulares daquele contrato de conta bancária[8]».
No caso dos autos, provou-se que, além do contrato de abertura de conta, foram também celebrados entre A. e R. contratos de depósito bancário, de utilização de cartão de débito e de utilização de serviços de *home banking* (cfr. pontos 2, 3, 28 e 29 da matéria de facto).
Contrato de depósito bancário é aquele em que uma pessoa entrega algo de seu a uma instituição bancária, na medida da confiança que o comportamento e a solvabilidade dessa instituição lhe transmitam, para que o guarde ou movimente, mas lhe restitua em valor, nos termos desse mesmo contrato. É o chamado depósito irregular, a que se reportam os arts. 1205.º e 1206.º do Código Civil, já que o objecto material desse contrato é uma coisa fungível, como dinheiro corrente[9]. E, como depósito irregular que é, nele estrutura-se a obrigação de restituir o capital depositado, por parte do depositário, logo que lhe seja exigido [cfr. art. 1.º n.º1 a) e n.º2 do DL 430/91 de 2-11].
Contrato de utilização de cartão de débito é aquele em que por uma instituição bancária é emitido e entregue ao cliente um cartão que permite, através de terminais electrónicos, aceder directa e imediatamente à conta bancária do titular, operando a mobilização das suas disponibilidades monetárias, quer pelo levantamento de numerário, quer pelo pagamento directo das aquisições de bens ou serviços, sem que seja necessário recorrer a qualquer outro meio[10].
Contrato de *home banking* ou de banca electrónica é aquele em que a instituição bancária «confere ao cliente a possibilidade de efectuar consultas de saldos e de realizar operações bancárias, *maxime* pagamentos e transferências, relativamente às contas de que seja titular e que possa movimentar livremente, utilizando para o efeito o telefone (serviço telefónico) ou a internet (serviço *online*)[11]».
Conforme resulta do art. 2.º i) do DL 91/2018 de 12-1[12] (Regime

Jurídico dos Serviços de Pagamento e da Moeda Electrónica[13]), os contratos de utilização de cartão de débito e de *home banking* constituem contratos-quadro em relação às sucessivas operações de transferência electrónica de fundos ordenadas através do cartão / através da internet. «Assim, cada vez que o cliente emite uma ordem de pagamento a favor de terceiro através do sistema informático posto à disposição pelo banco, é celebrado um novo contrato de execução» do contrato-quadro. «Esta figura contratual potencia uma multiplicidade de contratos subsequentes, simplificados, na sua conclusão e execução, através do recurso a meios electrónicos. Estes contratos de execução resultam de tantos acordos de vontade quantos os contratos celebrados, não se cingindo a simples actos de execução de um contrato anterior[14]», embora sejam por ele enformados.

Isto posto, temos que, como resulta da matéria provada, no dia 22 de Novembro de 2022, foi feito, na conta bancária aberta pela A. junto da R., um pagamento de € 4.950,00, não tendo tal pagamento sido realizado, nem autorizados, pela A., mas antes levados a cabo por terceiros não identificados, através de uma aplicação móvel que instalaram depois de terem obtido os dados de autenticação da A. (número de contrato, palavra-passe, número e nome do cartão bancário, coordenadas do cartão-matriz e códigos fornecidos por SMS), o que conseguiram quando a A. acedeu a uma página falsa de *home banking*, convencida de que se tratava da página oficial da R., ali introduzindo alguns daqueles dados e, posteriormente, quando a A. forneceu os restantes dados àqueles terceiros, mediante telefonema que deles recebeu, convencida de que se tratava de telefonema com origem na própria R..

Tendo a A. reclamado, junto da R., a restituição de tal quantia, esta não a efectuou, por ter considerado que os danos resultaram de comportamento culposo da própria A..

Vejamos.

Nos termos do art. 103.º n.º1 a 5 do RJSPME, «uma operação de pagamento ou um conjunto de operações de pagamento só se consideram autorizados se o ordenante consentir na sua execução», sendo certo que «o consentimento deve ser dado previamente à execução da operação», «na forma acordada entre o ordenante e o respetivo prestador do serviço de pagamento». Na falta desse consentimento, «considera-se que a operação de pagamento não foi autorizada».

Por outro lado, prevê o art. 104.º, do mesmo diploma, que, caso o ordenante aceda em linha à sua conta de pagamento, inicie uma operação de pagamento electrónico, ou realize uma acção, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou de outros abusos, o prestador de serviço de pagamento deverá aplicar a autenticação forte do cliente,

devendo adoptar medidas de segurança suficientes para proteger a confidencialidade e a integridade das credenciais de segurança personalizadas do utilizador. As normas técnicas de regulamentação daquela autenticação forte são elaboradas pela EBA, em colaboração com o BCE, nos termos do art. 98.º n.º1 da Directiva (UE) 2015/2366, do Parlamento Europeu e do Conselho, de 25 de novembro de 2015[15].

Para além destes requisitos – necessidade de autorização do ordenante e autenticação forte –, e considerados os riscos de utilização de meios de pagamento electrónicos, o RJSPME estabelece especiais obrigações do utilizador dos serviços e do respectivo prestador, repartindo depois tais riscos entre ambos. Com efeito, «no uso electrónico do instrumento de pagamento, encontramo-nos no âmbito de sistemas informáticos que permitem concretizar as operações de pagamento, mas comportam naturalmente riscos. A segurança do sistema estará dependente da actuação diligente de todos os seus utilizadores e intervenientes. Assim, há-de fazer-se uma repartição dos prejuízos entre as partes, tendo em consideração a actuação de cada uma delas no cumprimento dos deveres que lhe são impostos[16]».

É assim que, de acordo com o art. 110.º, daquele diploma:

«1 - O utilizador de serviços de pagamento com direito a utilizar um instrumento de pagamento deve:

a) Utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, as quais têm de ser objectivas, não discriminatórias e proporcionais; e

b) Comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento ou à entidade designada por este último, a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento.

2 - Para efeitos da alínea a) do número anterior, o utilizador de serviços de pagamento deve tomar todas as medidas razoáveis, em especial logo que receber um instrumento de pagamento, para preservar a segurança das suas credenciais de segurança personalizadas.

Por outro lado, prevê o art. 111.º n.º1 a), também do RJSPME, que «o prestador de serviços de pagamento que emite um instrumento de pagamento deve assegurar que as credenciais de segurança personalizadas do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento, sem prejuízo das obrigações do utilizador do serviço de pagamento estabelecidas no artigo anterior».

Caso ocorra uma operação de pagamento não autorizada, que dê origem a uma reclamação, nomeadamente ao abrigo dos arts.

130.º e 131.º, refere o art. 112.º n.º1, do mesmo diploma, que «o utilizador do serviço de pagamento obtém do prestador de serviços de pagamento a rectificação» dessa operação, «se comunicar a operação ao prestador de serviços de pagamento logo que dela tenha conhecimento e sem atraso injustificado, e dentro de um prazo nunca superior a 13 meses a contar da data do débito».

Quanto à prova da existência, ou não, de autorização ou de autenticação, rege o art. 113.º do RJSPME, que estabelece que, caso o utilizador negue ter autorizado a operação executada, incumbe ao prestador do serviço fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afectada por avaria técnica ou qualquer outra deficiência do serviço prestado. No entanto, a utilização do instrumento de pagamento registada pelo prestador de serviços não é necessariamente suficiente, por si só, para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira, uma ou mais das obrigações previstas no art. 110.º. Nessas situações, o prestador de serviços deve apresentar elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento (cfr. n.ºs 3 e 4 do art. 113.º). É que, «em face do carácter diabólico que assumiria a demonstração por parte do utilizador de serviços de pagamento de um facto negativo – a não prestação de consentimento em dada operação de pagamento – a lei inverte o ónus da prova, em caso de operação de pagamento não autorizada. Esta inversão é ainda justificada pelo facto de os prestadores de serviços de pagamento estarem vinculados a observar um grau de competência técnica acrescido, que se reflecte na utilização de sistemas informáticos sofisticados e robustos e de técnicas de registo detalhadas, que lhes permitem obter elementos sobre a operação de pagamento reclamada[17]».

Em caso de operação de pagamento não autorizada, e respeitado o disposto no art. 112.º, refere o art. 114.º, também do RJSPME, que o prestador de serviços deverá reembolsar imediatamente o ordenante do montante dessa operação, após ter tido conhecimento da mesma, a não ser que tenha motivos razoáveis para suspeitar de actuação fraudulenta do ordenante e desde que comunique esses motivos, por escrito, às autoridades judiciárias. Pelo contrário, conforme resulta do art. 115.º, do mesmo diploma, será o ordenante a suportar todas as perdas resultantes de operações de pagamento não autorizadas se aquelas forem devidas a actuação fraudulenta ou ao incumprimento deliberado de uma ou mais das obrigações previstas no artigo 110.º. Havendo negligência grosseira do ordenante, este suporta as perdas

resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento. Porém, se o prestador de serviços não exigir a autenticação forte do ordenante, este não deve suportar quaisquer perdas relativas a operação de pagamento não autorizada, salvo se tiver agido fraudulentamente.
Transportando este regime para o caso *sub judice*, temos que se provou que a operação de pagamento de € 4.950,00 realizada em 22/11/2022 na conta da A. não foi autorizada, confirmada ou consentida por este.
Assim, caberia à R., em princípio, reembolsar a A. da quantia movimentada, nos termos do art. 114.º do RJSPME.
No entanto, alegou a R. que a operação em causa foi realizada por terceiros, que conseguiram aceder aos meios de pagamento electrónicos da A. por via de comportamento culposo desta, ao incumprir as obrigações previstas no artigo 110.º do RJSPME, o que excluiria a responsabilidade da R., em conformidade com o disposto no citado art. 115.º, do mesmo diploma.
A este propósito, provou-se que a A. introduziu em página de internet falsa [embora pensando que era verdadeira] parte das suas credenciais de acesso ao *home banking* e que, de seguida, forneceu as restantes credenciais de acesso por via telefónica [pensando tratar-se de chamada da R.] - número de contrato, palavra-passe, número e nome do cartão bancário, coordenadas do cartão-matriz e códigos fornecidos por SMS -, assim as dando a conhecer a terceiros.
Não obstante tal poder configurar uma violação de uma das regras inerentes à utilização dos serviços de pagamento electrónico (não cessão, a terceiros, dos dados de acesso), seria ainda necessário que se provasse que a mesma adveio de negligência grosseira da A..
O tribunal recorrido entendeu que não, com o seguinte raciocínio:
«É certo que o texto das SMS indicava a operação que estava a ser autorizada, e que a autora assumiu ter apenas atentado no texto da última mensagem, o qual estranhou e a fez inclusive questionar o procedimento, acabando, contudo, por ser convencida da sua fidedignidade. Porém, em face da surpresa causada pela situação, da urgência transmitida no telefonema, e de toda a construção do esquema fraudulento, nomeadamente em face da confiança transmitida pelo facto de a informação provir de número de telefone correspondente ao da CGD, crê-se que qualquer homem médio acreditaria estar efectivamente a ser contactado pelo seu banco e necessitar de actuar do modo descrito para evitar a transferência iminente. Tal circunstancialismo leva-nos à conclusão de que ainda que se possa verificar alguma falta de diligência da autora, a mesma não

configura uma negligência grosseira, a qual deve, assim, ser afastada. Veja-se ainda que os factos remontam já a 2022, há mais de dois anos, momento em que este tipo de fraude não era amplamente divulgado. Finalmente, diga-se que, tendo ficado demonstrado que a ré realiza diversos alertas aos seus clientes relativos a este e outro tipo de fraudes na utilização dos serviços online, desconhece-se desde que datas são realizados tais alertas e concretamente o alerta referente a esta específica fraude, afigurando-se ainda que os alertas são realizados apenas através do site e não também através da APP, plataforma que a autora costumava utilizar. Acredita-se, pois, que uma pessoa medianamente diligente colocada nas mesmas circunstâncias da autora, actuaria da mesma forma».

Vejamos.

Tendo em conta que, conforme resulta do art. 1.º n.º1 do RJSPME, o DL 91/2018 de 12-11 transpôs para a ordem interna portuguesa a Directiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de Novembro de 2015, os considerandos desta Directiva são preciosos auxiliares na interpretação dos conceitos legais. Assim, é de assinalar que, de acordo com o respectivo considerando n.º 72, «para avaliar a eventual negligência ou negligência grosseira cometida pelo utilizador dos serviços de pagamento, deverão ser tidas em conta todas as circunstâncias. Os elementos de prova e o grau da alegada negligência deverão ser avaliados nos termos do direito nacional. Todavia, embora o conceito de negligência implique uma violação do dever de diligência, a negligência grosseira deverá significar mais do que mera negligência, envolvendo uma conduta que revela um grau significativo de imprudência; por exemplo, conservar as credenciais utilizadas para autorizar uma operação de pagamento juntamente com o instrumento de pagamento, num formato que seja aberto e facilmente detectável por terceiros. As modalidades e condições contratuais relativas ao fornecimento e à utilização de um instrumento de pagamento que tenham por efeito agravar o ónus da prova que recai sobre o consumidor ou atenuar o ónus da prova que recai sobre o emitente deverão ser consideradas nulas e sem efeito. Além disso, em situações específicas e, nomeadamente quando o instrumento de pagamento não estiver presente no ponto de venda, como sucede no caso de pagamentos em linha, é adequado que o prestador de serviços de pagamento seja obrigado a apresentar provas da alegada negligência, uma vez que o ordenante apenas dispõe de meios muito limitados para o efeito em tais casos».

Em consonância com aquele considerando, e como se refere no Ac. RL de 19/12/2024[18], «o conceito de negligência grosseira é aferido nos termos aplicáveis à responsabilidade civil (art.º 487.º, n.º 2 do CC), "que remete para a comparação entre o

comportamento concretamente adoptado pelo agente e o que seria observado nas mesmas circunstâncias de facto por um utilizador do serviço de pagamento normalmente informado, diligente e cuidadoso, pois este é o padrão referencial ou parâmetro de aferição a considerar para apurar do grau de reprovação ou censura de que é merecedor a conduta do utilizador (o grau de reprovação ou de censura será tanto maior quanto mais ampla for a possibilidade de a pessoa ter agido de outro modo), donde resulta que a culpa grosseira ocorrerá quando a omissão do dever de cuidado em que a negligência se traduz revelar que o comportamento observado se afastou do (contraria o) grau de diligência minimamente exigível e da observância de deveres de cuidado (resultantes da relação jurídica) ostensivamente evidentes, patentes e manifestos, traduzindo desconsideração do proceder expectável a qualquer comum utilizador do serviço de pagamento minimamente cuidadoso, apresentando-se como altamente reprovável à luz do mais elementar senso comum, revelando desconformidade com todos os padrões de referência. À míngua de outro critério legal, o padrão de conduta exigível ao utilizador do serviço, *rectius*, o padrão com que se mede o grau de diligência exigível é o prescrito no artigo 487.º, n.º 2, do CC. Deste modo, a culpa (juízo de censura ético) será apurada por referência ao modelo de uma pessoa-tipo, um sujeito ideal, o tipo de homem médio ou normal, medianamente sagaz, prudentemente avisado e cuidadoso (fazendo reportar estas qualidades ao do utilizador do serviço em causa) que utiliza tais serviços. (…) A negligência grosseira será de afirmar, destarte, quando o grau de reprovação ultrapassar a mera censura que merece a simples imprudência, irreflexão ou o impulso leviano, alcançando um mais alto grau de desleixo e incúria, decorrendo da inobservância das mais elementares regras de cuidado e da não adopção do esforço e diligência minimamente exigíveis, nas circunstâncias concretas, correspondendo ao erro imperdoável, à desatenção inexplicável e à incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas pouco diligentes – comportamento que de todo seria adotado pela generalidade dos utilizadores do serviço de pagamento colocados perante as concretas circunstâncias que se apresentaram ao agente, pois que a diligência e cuidados exigíveis no caso os levariam a abster-se de o adotar e/ou prosseguir”».

Na apreciação do grau de culpa do utilizador não se pode olvidar que o fim pretendido pelo RJSPME com a distribuição do risco inerente ao uso de meios de pagamento electrónico é o de proteger o utilizador que, consabidamente, é a parte mais fraca na relação, face à diversidade de meios, designadamente informáticos, ao dispor da entidade bancária para prevenir e detectar fraudes. É o que resulta, desde logo, do preâmbulo do

DL 91/2018 de 12-11, onde se refere que o diploma tem como objectivos fundamentais «preocupações relacionadas com a protecção e segurança dos consumidores na utilização desses serviços de pagamento (…) preservando a escolha do consumidor em melhores condições de segurança, eficácia e eficiência de custos. A segurança dos pagamentos electrónicos afigura-se como um aspecto fundamental para assegurar a protecção dos utilizadores e a promoção adequada do desenvolvimento do comércio electrónico em condições concorrenciais».
No caso dos autos, não podemos concordar com a ponderação efectuada em 1.ª instância.
É verdade que a A., ao receber um SMS de um número que era pertença da R., tinha fundadas razões para crer que se tratava de um SMS com origem na própria R., tanto mais que o link fornecido vinha com a menção de que um dispositivo desconhecido tinha acedido à sua conta, pelo que, para um utilizador médio, poderia, perfeitamente, tratar-se de uma página própria para resolução do problema em causa. Note-se, aliás, que, se se provou que a R., quatro meses antes dos factos, fez publicar no seu *site* uma informação segundo a qual os seus clientes não deveriam aceder a *links* que lhes chegassem por SMS, nenhuma garantia existe de que a A. tenha acedido a esse *site*, nem nada permite concluir que tenha obrigação de o fazer. Muito menos se pode considerar que a circunstância de a A. ter digitado, no sítio «falso», como ali foi solicitado, o número do seu contrato com a CGD, a palavra-passe e o número e nome do cartão de débito, constitua qualquer desatenção indesculpável. É que se provou que a A. estava convencida de tratar-se de página da R., já que a página a que acedeu após clicar no *link* tinha uma configuração idêntica à da R. e, portanto, não lhe era exigível ter-se apercebido de que estava perante uma página falsa: não existia qualquer circunstância que pudesse ter alertado a A. para a falta de fidedignidade da página.
Porém, o mesmo já não podemos dizer do comportamento da A. perante o telefonema que recebeu. É certo que, também nesse caso, a chamada foi feita a partir de número identificado como pertencente à R., não tendo a A., no momento em que atendeu a chamada, razões para desconfiar de que o seu interlocutor nada tinha a ver com a CGD, até porque a conversa continuava a dizer respeito a alegadas operações para evitar que alguém pudesse efectuar uma transacção no valor de € 4.950,00 a partir da conta da A.. Igualmente não nos parece que o fornecimento dos códigos recebidos por SMS para autorização de «associação de dispositivo ao contrato» e de consulta dos dados de segurança do cartão de débito possa ser considerado uma desatenção indesculpável, dado que um homem médio poderia, ainda assim, pensar tratar-se de procedimentos necessários a evitar a invocada «fraude». Mas o que não pode, de forma nenhuma, deixar de ser

atentatório do grau de diligência minimamente exigível é fornecer um código indicado num SMS que expressamente refere que visa concretizar uma operação de pagamento no valor de € 4.950,00. Tendo lido a mensagem e tendo verificado que a mesma dizia o contrário daquilo que queria evitar (a mensagem dizia autorizar um pagamento e não impedi-lo), é totalmente incompreensível, do ponto de vista de uma pessoa minimamente informada, perspicaz, cuidadosa e diligente, ainda assim fornecer esse código. Merece, pois, este comportamento da A. um especial juízo de censura, já que contrariou frontalmente o mais elementar senso comum, integrando o conceito de negligência grosseira, supra explanado.
Assim, configurada que está a negligência grosseira da A., é a si mesma que cabe suportar as perdas resultantes do pagamento em causa, nos termos do art. 115.º, n.º4, do RJSPME, pelo que não compete à R. reembolsá-la de tal quantia.
E, não sendo obrigação da R. efectuar esse reembolso, também não lhe cabe indemnizar a A. de quaisquer danos não patrimoniais que a mesma possa ter sofrido, o que desde logo decorre da inexistência de qualquer facto ilícito imputável à R. (cfr. art. 483.º do Código Civil).
Não pode, assim, manter-se a decisão recorrida, procedendo o recurso.

DECISÃO
Pelo exposto, acorda-se em julgar procedente a apelação, revogando-se a decisão recorrida, a qual se substitui por outra que, julgando improcedente a acção, absolve a R. de todos os pedidos.
Custas, em ambas as instâncias, pela A. – art. 527.º do Código de Processo Civil.

Lisboa, 13-01-2026,
Alexandra de Castro Rocha
Luís Lameiras
Cristina Silva Maximiano

---

[1] A este respeito pode ver-se, com grande desenvolvimento, o Ac. RL de 17/10/2017, proc. 585/13, disponível em http://www.dgsi.pt, onde se refere, além do mais, que a verdade apurada no processo não é absoluta, antes se baseando em «duas regras fundamentais:
(i)-Entre as várias hipóteses de facto deve preferir-se e considerar-se como verdadeira aquela que conte com um grau de confirmação relativamente maior face às demais;
(ii)-Deve preferir-se aquela hipótese que seja "mais provável que não", ou seja, aquela hipótese que é mais provável que seja verdadeira do que seja falsa".
"Este critério da probabilidade lógica prevalecente (…) não se reporta à probabilidade como frequência estatística mas sim como grau de confirmação lógica que um enunciado obtém a partir das provas disponíveis. (…) O que o standard preconiza é que, quando sobre um facto existam provas contraditórias, o julgador deve sopesar as probabilidades das diferentes versões para eleger o enunciado que pareça ser relativamente "mais provável", tendo em conta os meios de prova disponíveis. Dito de outra forma, deve escolher-se a hipótese que receba apoio relativamente maior dos elementos de prova conjuntamente disponíveis. Todavia, pode acontecer que todas as versões dos factos tenham um nível baixo de apoio probatório e, nesse contexto, escolher a relativamente mais provável pode não ser suficiente para considerar essa versão como "verdadeira". Pelo que

para que um enunciado sobre os factos possa ser escolhido como a versão relativamente melhor é necessário que, além de ser mais provável que as demais versões, tal enunciado em si mesmo seja mais provável que a sua negação. Ou seja, é necessário que a versão positiva de um facto seja em si mesma mais provável que a versão negativa simétrica».

[2] A este respeito pode ver-se, ainda, o Ac. RC de 27/5/2014 (proc. 1024/12, disponível em http://www.dgsi.pt): «Não há lugar à reapreciação da matéria de facto quando o (s) facto (s) concreto (s) objecto da impugnação for insusceptível de, face às circunstância próprias do caso em apreciação, ter relevância jurídica, sob pena de se levar a cabo uma actividade processual que se sabe, de antemão, ser inconsequente».

[3] Sublinhado nosso.

[4] Cfr. definições constantes da Infopédia em https://www.infopedia.pt/dicionarios/lingua-portuguesa/apar%C3%AAncia e https://www.infopedia.pt/dicionarios/lingua-portuguesa/aparentemente

[5] Também denominado contrato de conta bancária.

[6] No dizer de Engrácia Antunes, o «contrato bancário primogénito» - cfr. *Direito dos Contratos Comerciais*, Almedina, pág. 483.

[7] Cfr. Maria Carolina dos Santos Gomes França Barreira, *Home Banking A Repartição dos Prejuízos Decorrentes de Fraude Informática*, Fevereiro de 2015, págs. 9-10, disponível em https://cij.up.pt/download-file/1342.

[8] Cfr. Ac. STJ de 18/12/2013, proc. 6479/09, disponível em http://www.dgsi.pt.

[9]Cfr. Ac. do STJ de 19/10/1993, *Sub Judice / Novos estilos*, 10, pág. 173.

[10] Cfr. Ac. do STJ de 23/11/1999, proc. 99A796, disponível em http://www.dgsi.pt.

[11] Cfr. Maria Carolina…Barreira, ob. cit., pág. 16.

[12] «Para efeitos do presente Regime Jurídico, entende-se por "contrato-quadro" um contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento».

[13] Doravante, RJSPME.

[14] Cfr. Maria Carolina…Barreira, ob. cit., págs. 15-16.

[15] Cfr., a este respeito, as informações divulgadas pelo Banco de Portugal, disponíveis nas hiperligações https://www.bportugal.pt/comunicado/eba-esclarece-o-mercado-sobre-os-elementos-de-autenticacao-forte-do-cliente e https://www.bportugal.pt/page/autenticacao-forte .

[16] Cfr. Raquel Sofia Ribeiro de Lima, *A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento electrónico na jurisprudência portuguesa*, *in Revista Electrónica de Direito*, Outubro de 2016, nº3, FDUP, pág. 36.

[17] Cfr. Patrícia Guerra, *A realização de operações de pagamento não autorizadas e a tutela do utilizador de serviços de pagamento em face do Regime Jurídico dos Serviços de Pagamento e da Moeda Electrónica*, *in Revista Electrónica de Direito*, Junho de 2016, nº2, pág. 26.

[18] Proc. n.º15407/23, disponível em https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/dca9485bc8c74c5c80258c140056afe2?OpenDocument