jurisprudência.pt

Tribunal da Relação de Coimbra
Processo nº 8/23.8T8SAT.C1

Relator: ANABELA MARQUES FERREIRA
Sessão: 25 Março 2025
Votação: UNANIMIDADE
Meio Processual: APELAÇÃO
Decisão: CONFIRMADA

AÇÃO INDEMNIZATÓRIA **SISTEMA HOMEBANKING**

PRESTADOR DO SERVIÇO DE PAGAMENTO **RESPONSABILIDADE**

UTILIZADOR DO SERVIÇO **NEGLIGÊNCIA GROSSEIRA**

Sumário

I – É o prestador do serviço de pagamento quem, em princípio, deve suportar os danos decorrentes da sua utilização, por ser quem tem a capacidade de assegurar o seu complexo funcionamento.
II – O que não acontece se o prestador do serviço provar que a operação foi devidamente autorizada, que não se ficou a dever a avaria técnica ou a outra deficiência do serviço e que houve negligência grosseira por parte do utilizador, sobre o qual recai o dever de cuidar da preservação dos dados confidenciais que lhe são fornecidos.
III – O utilizador do serviço de pagamento, ao informar terceiro dos dados da sua password e do código OTP, agiu com negligência grosseira, uma vez que o resultado era previsível para qualquer pessoa normalmente diligente, que se encontrasse na mesma situação.
(Sumário elaborado pela Relatora)

Texto Integral

Recorrente **AA**

Recorridos **Banco 1..., C.R.L.**

Juiz Desembargador Relator: Anabela Marques Ferreira

Juízes Desembargadores Adjuntos: Hugo Meireles

Luís Manuel Carvalho Ricardo

Sumário (da responsabilidade do Relator – artº 663º, nº 7, do Código de Processo Civil)

(…).

Acordam os juízes que nestes autos integram o coletivo da 3ª Secção Cível do Tribunal da Relação de Coimbra:

I – Relatório

Nos autos de ação de processo comum, que correram termos no Juízo de Competência Genérica de Sátão, a Autora AA demandou a Ré Banco 1…, C.R.L., pedindo a condenação da Ré:

1- A reconhecer e assumir a responsabilidade pelo ressarcimento de todos os danos sofridos pela Autora em consequência do ocorrido no dia 29 de março de 2022;

2- A pagar à Autora o montante de € 4.916,32 (quatro mil novecentos e dezasseis euros e trinta e dois cêntimos), a título de danos patrimoniais sofridos em consequência da falha de segurança do sistema de homebanking da Ré, acrescida de juros à taxa legal desde a propositura da ação até efetivo e integral pagamento;

3- A pagar à Autora € 2.000,00 (dois mil euros) a título de compensação por danos não patrimoniais sofridos.

Para tanto, alegou, que *a Autora é titular de conta bancária, na instituição bancária da ora Ré, tendo celebrado contrato de abertura de conta e, mais tarde, contrato de homebanking.*

No dia 29 de março de 2022, a Autora foi contactada telefonicamente por uma mulher que se identificou como sendo colaboradora da Ré em Lisboa. Após ter confirmado a identidade da Autora, a putativa colaboradora da Ré esclareceu ainda que aquele contacto se devia ao facto de o Banco ter recebido um alerta relativamente a uma operação pendente no valor de € 4.916,32 (quatro mil

novecentos e dezasseis euros e trinta e dois cêntimos), operação essa que estaria a ser realizada pela Autora, tendo questionado a Autora sobre se confirmava a operação ou se, pelo contrário, pretendia anular aquela operação.

A putativa colaboradora da Ré informou então a Autora que, para cancelar aquela operação, precisaria que a Autora lhe confirmasse os números referentes às 3.ª, 6.ª e 10.ª posições da sua password, o que a Autora fez. Após o que, a putativa colaboradora da Ré questionou a Autora sobre se tinha recebido no seu telemóvel a mensagem sms com o código de autorização, tendo informado a Autora de que tinha de receber a mensagem para fazer a anulação da operação.

Mais alegou que confirmou assim a receção da mensagem e, a pedido da putativa colaboradora da Ré, transmitiu-lhe o código de autorização da operação, estando convencida de que estava a anular a transferência do seu dinheiro para uma conta bancária de terceiro.

Terminada a chamada, a Autora consultou, no seu telemóvel, a sua conta bancária através da aplicação do Banco, tendo constatado que havia sido enganada e que tinha acabado de dar ordem e confirmar a operação bancária de transferência no montante de € 4.916,32.

Acrescentou ainda que de imediato contactou telefonicamente o Sr. BB colaborador da Ré e deslocou-se ao Balcão ..., tendo feito participação escrita do sucedido, havendo apurado que a conta para a qual tinha sido transferido a quantia era um balcão da Ré localizado na Amadora, em Lisboa e que já não era possível cancelar a operação de transferência, tendo procedido a queixa crime.

Deu conta que a Ré a informou que não se podia responsabilizar pela transferência realizada, pois a Autora havia facultado os números da sua password/cartão matriz, discordando a Autora pois alguém já tinha entrado na sua conta quando foi contactada telefonicamente pela putativa colaboradora da Ré, ou seja, a sua conta já tinha sido acedida por terceiros sem que tenha facultado o seu número de adesão, a sua chave multicanal ou o seu PIN, elementos necessários e prévios ao acesso à conta e ao serviço de homebanking prestado pela Ré.

De acordo com a Autora quando foi contactada telefonicamente pela putativa colaboradora da Ré, a instituição bancária já havia falhado, revelando-se insegura, por ter permitido o acesso à conta da Autora por alguém que não

deveria ter nem o número de adesão nem a chave multicanal, logo não assegurou que as credenciais de segurança personalizadas do instrumento de pagamento da Autora apenas fossem acessíveis a esta.

Concluiu assim estarem reunidos todos os requisitos legalmente previstos para ser a Ré condenada no pagamento do valor a reembolsar à Autora, no montante de € 4.916,32 a que acrescem juros vencidos e, outrossim, juros vincendos até efetivo e integral pagamento e em indemnização pelos danos não patrimoniais sofridos pela Autora no montante de € 2.000,00 (mil euros).

A Ré contestou, *alegando, em síntese, que, esta ação surge na sequência de uma "fraude informática" de que a Autora foi alvo, concretizada através de uma chamada telefónica, realizada por terceiro desconhecido, que logrou que a Autora transferisse, através do CA Online - homebanking do Banco 1..., o montante total de € 4.916,32 (quatro mil novecentos e dezasseis euros e trinta e dois cêntimos).*

Mais arguiu, que foram celebrados entre a Autora e a Ré os seguintes contratos:

i. Contrato de Depósito, subjacente à conta de depósito à ordem nº...91;

ii. Contrato de Adesão ao Sistema Multicanal, aplicável à conta de depósito à ordem nº. ...91.

Aduzindo que a pessoa que praticou a referida "fraude informática" detinha alguns dados pessoais e intransmissíveis da Autora, ignorando a Ré como foram obtidos, e convenceu a Autora a partilhar telefonicamente os detalhes dos seus dados de utilização do CA Online em expressa violação das regras de acesso e utilização e de segurança do mesmo.

O terceiro encaminhou a Autora não só a partilhar os três dígitos aleatórios da password pedidos aquando da realização de uma operação, como também, o código "OTP" de autorização, que consiste numa palavra-passe de utilização única e que é apenas válida durante um período muito reduzido de tempo, ambos necessários para a concretização da transferência ordenada.

Argumenta ainda que o sistema de homebanking implementado pela Ré cumpre com todos os preceitos legais e normativos, o que é comprovado pelas auditorias regulares efetuadas ao sistema, que não detetaram qualquer falha de segurança e não sofreu qualquer ingerência fraudulenta, informática ou outra, que tenha exposto os dados dos Clientes a terceiros, o que é suportado

pelo facto de não ter realizado qualquer comunicação dando conta desse evento ao Banco de Portugal, o que se lhe impunha, caso tivesse acontecido.

Os danos que a Autora reclama são, antes, imputáveis à atuação manifestamente negligente da mesma, que incumpriu as regras de acesso e de utilização do sistema multicanal, (i) seguindo instruções de uma chamada telefónica, bem sabendo, ou devendo saber, que o sistema multicanal da Ré não é operado desse modo, (ii) comunicando a um terceiro os dados pessoais e intransmissíveis de acesso e utilização do sistema multicanal, pois que aquando do primeiro acesso ao sistema multicanal, o Cliente tinha de alterar, obrigatoriamente, a chave multicanal atribuída no momento da ativação do serviço, sendo que a Ré só conhece o número de adesão dos Clientes, não conhece nem tem como conhecer a chave multicanal, dado que a validação dessa chave é feita com base numa chave encriptada a partir da chave multicanal definida pelo Cliente aquando do primeiro acesso ao sistema multicanal, pelo que somente o Cliente, no caso a Autora, conhece efetivamente a mesma associada ao seu número de adesão.

Mais alega que à data da prática da fraude relatada nos autos, o Banco 1… aplicava a autenticação forte no acesso ao serviço de 90 em 90 dias e aquando da realização de cada operação e que cabe ao Cliente o especial dever de não revelar, nem por qualquer forma tornar acessível ao conhecimento de terceiros, os seus elementos de identificação e os códigos de acesso, seja o número de adesão, seja o código multicanal, seja a password, sejam as OTP do login ao serviço ou de autorização de operações, elementos que são pessoais e intransmissíveis, aliás informação que é disponibilizada através de documento com Recomendações de Segurança nos Canais Digitais e através de pop-ups de alerta que aparecem sempre aquando de cada acesso ao Ca Online, após a introdução do número de adesão e antes da introdução da chave multicanal, que têm de ser expressamente fechados pelo utilizador para este poder concretizar o acesso ao serviço.

E, pese embora da mensagem OTP de autorização recebida pela Autora por SMS às 13h51 de 29 de março de 2022, resulte inequivocamente a conta bancária da qual é debitado o valor, a conta bancária em que será creditado o valor e o valor que está a ser transferido, ainda assim a receção de tal mensagem não foi suficiente para que a Autora ficasse alertada e adotasse uma postura distinta, em violação das regras de acesso e de utilização do sistema multicanal, sem cuidar sequer de ler a mensagem de texto que recebeu e ignorando todas as instruções constantes dos pop ups divulgados no

CA Online e dos SMS de alerta que recebeu, assim como as suas obrigações contratuais.

Alega, por fim, que os danos sofridos pela Autora são imputáveis à mesma, na medida em que atuou, no mínimo, com incúria/negligência grave e grosseira, desconsiderando as regras de acesso e utilização do sistema e os avisos que foram sendo feitos pela Ré e nunca de uma falha do sistema da Ré, não tendo esta como cancelar ou reverter a transferência realizada, porquanto a mesma constitui uma transferência intrabancária, isto é, entre contas bancárias abertas no mesmo Banco, que são sempre concretizadas de imediato.

Conclui que não se verifica, pois, qualquer fundamento jurídico válido para responsabilizar a Ré pelos danos sofridos pela Autora e igualmente pelos danos morais peticionados.

Foi dispensada a audiência prévia e proferido despacho saneador, no qual foi identificado o objeto do litígio e enunciados os temas da prova.

Foi realizada audiência de julgamento e proferida sentença, julgando a ação totalmente improcedente.

A Recorrente AA interpôs recurso da sentença, concluindo, nas suas alegações, que:

(…).

A Recorrida Banco 1…, C.R.L. respondeu ao recurso, concluindo, nas suas contra-alegações, que:

(…).

II – Objeto do processo

Colhidos os vistos legais, prestados contributos e sugestões pelos Exmos. Juízes Desembargadores Adjuntos e realizada conferência, cumpre decidir.

Da conjugação do disposto nos artºs 635º, nºs 3 e 4, 637º, nº 1 e 639º, todos do Código de Processo Civil, resulta que são as conclusões do recurso que delimitam os termos do recurso (sem prejuízo das questões de conhecimento oficioso - artº 608º, nº 2, *ex vi* artº 663º, nº2, ambos do mesmo diploma legal),

não vinculando, porém, o Tribunal *ad quem* às soluções jurídicas preconizadas pelas partes (artº 5º, º 3, do Código de Processo Civil). Assim:

Questões a decidir:

1) Da alteração da decisão relativa à matéria de facto

2) Da falha de segurança do sistema bancário

III – Fundamentação

A) De facto

Factos julgados provados na sentença recorrida:

1. A Autora é titular da conta bancária n.º ...91, na instituição bancária da Ré, tendo sido celebrado entre as partes, a 23 de novembro de 2010, um

contrato de abertura da conta de depósito à ordem n.º ...91.

2. Mais tarde, as partes inscreveram um novo contrato destinado a permitir a consulta e movimentação de conta através da internet – contrato de homebanking/de Adesão ao Sistema Multicanal, aplicável à conta de depósito à ordem nº. ...91 a 26 de setembro de 2018.

3. Tal adesão permitiu à Autora consultar e movimentar a conta de depósito à ordem n.º...91, através da internet – acedendo ao CA Online – ou através de dispositivos móveis– acedendo ao CA Mobile.

4. Isto porque o sistema multicanal de cariz facultativo, conferiu ao Titular, no caso à Autora a possibilidade de "efectuar um conjunto de operações bancárias, designadamente, de consulta e/ou movimentação, relativamente a contas de depósito de que seja titular único ou co-titular em regime de solidariedade e que possa livremente movimentar através de canais telemáticos: internet (Online Particulares), serviço telefónico (Linha Directa), dispositivos móveis (CA Mobile), ou outras formas de acesso que venham a ser disponibilizadas pelo Banco 1…".

5. E deve ser realizado através do endereço www.Banco1....pt, quando se pretende aceder ao "CA Online Particulares" (doravante somente "CA Online") ou da Aplicação CA Mobile.

6. Para o acesso ao sistema multicanal, é atribuído ao Cliente um número de adesão, que consiste num código numérico de oito posições, gerado pelo sistema após ser efetuado, com sucesso, um Pedido de Adesão ao sistema multicanal.

7. Para concretizar o acesso, é também necessária a chave multicanal, que consiste num código numérico de 8 posições que permite, em conjunto com o número de adesão, identificar inequivocamente o Cliente para o acesso à realização de Consultas no CA Online Particulares e na Linha Direta.

8. Como medida de segurança, aquando do primeiro acesso ao sistema multicanal, a Cliente teve de alterar, obrigatoriamente, a chave multicanal atribuída no momento da ativação do serviço.

9. Incumbe-se a Cliente ainda de proceder, regularmente, à alteração da chave multicanal.

10. Desde 26 de setembro de 2018, a Autora é utilizadora frequente deste serviço, inclusive por referência aos meses de fevereiro a março de 2022, usando com maior frequência o CA Mobile.

11. No que se refere à informação detida pela Ré, esta apenas conhecia o número de adesão da Cliente, uma vez que a Ré não conhece nem tem como conhecer a chave multicanal, dado que a validação da chave multicanal é feita com base numa chave encriptada a partir da chave multicanal definida pela Cliente aquando do primeiro acesso ao sistema multicanal.

12. O PIN corresponde a um código numérico de quatro posições, definido pela Cliente no momento de adesão ao CA Mobile e que permite, em conjunto com o número de adesão, identificar inequivocamente a Cliente para o acesso ao serviço CA Mobile, bem como realizar consultas.

13. A password corresponde a um código numérico composto por entre 8 a 12 dígitos, dos quais apenas três são solicitados de forma aleatória, aquando da consulta de informação considerada sensível, do acesso a documentos digitais e da realização de transações de cariz financeiro.

14. Quando o acesso ao sistema multicanal é feito através do CA Mobile, a password é ainda utilizada como código de validação de transações.

15. No período que mediou a celebração do Contrato de Depósito entre a Autora e a Ré e a data da alegada burla, o teor das Condições Gerais do mesmo foi alterado, acompanhando a evolução legislativa.

16. Tais alterações foram comunicadas à Autora, conforme as Condições Gerais assinadas pela Autora a 31 de julho de 2019.

17. No dia 29 de março de 2022, pelas 13:40 horas, a Autora foi contactada telefonicamente por uma mulher, cujo nome a Autora não se recorda, e que, par além do mais, se identificou como sendo colaboradora da Ré na Caixa Central em Lisboa.

18. A putativa colaboradora da Ré identificou-se dizendo o seu nome e informando a Autora de que estava a ligar da parte da Ré, enquanto sua colaboradora/funcionária, tendo esta indagado sobre a identidade da Autora, perguntando-lhe especificamente se estava a falar com a Sra. AA.

19. Após ter confirmado a identidade da Autora, a putativa colaboradora da Ré esclareceu ainda que aquele contacto se devia ao facto de o Banco ter recebido um alerta relativamente a uma operação pendente no valor de € 4.916,32 (quatro mil novecentos e dezasseis euros e trinta e dois cêntimos), operação essa que estaria a ser realizada pela Autora.

20. A putativa colaboradora da Ré justificou ainda o contacto à Autora alegando que não era usual a Autora realizar transferências daqueles montantes, pelo que o contacto telefónico tinha como objetivo obter a confirmação da Autora de que estava efetivamente a fazer a transferência daquele montante, tendo questionado a Autora sobre se confirmava a operação ou se, pelo contrário, pretendia anular aquela operação.

21. A Autora surpreendida com o telefonema, disse à putativa colaboradora que não estava a realizar nenhuma operação bancária e que não confirmava nenhuma transferência.

22. A putativa colaboradora da Ré questionou a Autora sobre se pretendia anular imediatamente e através daquele telefonema a operação bancária (alegadamente) em curso, ou se enviava um e-mail para a Autora com os procedimentos necessários para a anulação da operação.

23. Confrontada com a hipótese de imediatamente anular a operação bancária que supostamente se encontrava em curso, a Autora solicitou que a putativa colaboradora da Ré cancelasse de imediato a operação.

24. A putativa colaboradora da Ré informou então a Autora que, para cancelar aquela operação, precisaria que a Autora lhe confirmasse os números referentes às 3.ª, 6.ª e 10.ª posições da sua password.

25. Neste conspecto a Autora transmitiu à putativa colaboradora da Ré a informação relativa aos números da sua password solicitada.

26. Após o que, a putativa colaboradora da Ré questionou a Autora sobre se tinha recebido no seu telemóvel a mensagem (sms) com o OTP- código de autorização, tendo informado a Autora de que tinha de receber a mensagem para fazer a anulação da operação.

27. A Autora recebeu no seu telemóvel uma mensagem sms naquele dia 29/03 pelas 13.51h com os seguintes dizeres: «Transf. Contas CA Conta Debitar: ...91 IBAN CREDITAR: ...81 Montante:4916.32 Cod. Aut.:...72.

28. A Autora confirmou assim a receção da mensagem e, a pedido da putativa colaboradora da Ré, transmitiu-lhe o código de autorização da operação, tendo estranhado nesta altura que a mensagem recebida fosse para confirmar e não cancelar a operação, dizendo-lhe a burlona que era o que iria suceder se não cancelasse a operação.

29. Após ter obtido as informações pedidas e supostamente tendentes à anulação da transferência, a putativa colaboradora da Ré agradeceu e confirmou a anulação da transferência, tendo de seguida questionado a Autora se havia mais alguma questão em que pudesse ajudar.

30. Através de um discurso encadeado, o terceiro encaminhou a Autora não só a partilhar os três dígitos aleatórios da password pedidos aquando da realização de uma operação, como também, o código "OTP" de autorização, sigla que abrevia a expressão "one time password", que consiste numa palavra-passe de utilização única e que é apenas válida durante um período muito reduzido de tempo (doravante "OTP"), ambos necessários para a concretização da transferência ordenada.

31. A Autora questionou a putativa colaboradora da Ré sobre quais seriam os procedimentos seguintes do Banco, nomeadamente se iria ser tomada alguma providência sobre a identificação de quem estava a tentar fazer a

transferência, ao que a putativa colaboradora respondeu afirmativamente, comprometendo-se em nome da Ré a facultar à Autora toda a informação que viesse a ser apurada, num futuro contacto, após o que concluíram a chamada telefónica.

32. Terminada a chamada, e supostamente anulada a operação bancária de transferência do seu dinheiro, a Autora consultou, no seu telemóvel, a sua conta bancária através da aplicação do Banco, tendo constatado que havia sido enganada e que, ao contrário do que foi levada a crer, tinha acabado de dar ordem e confirmar a operação bancária de transferência do montante de € 4.916,32 (quatro mil novecentos e dezasseis euros e trinta e dois cêntimos), através do CA Online, serviço disponibilizado pelo sistema multicanal.

33. De imediato contactou telefonicamente o Sr. BB, colaborador/funcionário da Ré que trabalha no balcão da Ré localizado no ..., com quem a Autora costuma tratar dos assuntos relativos à sua conta bancária, e explicou-lhe o que havia sucedido, tendo este avisado a Autora que teria sido vítima de burla e que se dirigisse ao balcão da Ré no ....

34. Após a Autora deslocou-se até ao balcão da Ré no ..., onde falou presencialmente com o Sr. BB e com a Sra. CC, também colaboradora/funcionária da Ré que trabalha no balcão da Ré localizado no ....

35. Tais colaboradores/funcionários da Ré já se encontravam a verificar a situação da Autora, na sequência do seu telefonema, tendo apurado que a transferência do dinheiro da Autora havia sido feita para a conta bancária n.º ...81 da Banco 1..., titulada por DD.

36. Neste seguimento, a Autora fez junto do balcão da Ré no ... a competente participação oral do sucedido, tendo a mesma sido enviada por e-mail pelo Sr. BB a EE, FF, GG, CC, HH e II:

"Boa tarde

Hoje dia 29-03-2022 pela 13.43 horas a nossa cliente AA cliente n.º ...48 Foi contactada por alguém do sexo feminino que se identificou como colaboradora do Banco 1... em Lisboa, a informar que tinha uma transferência pendente no valor de 4.916,32€, e se tinha sido a cliente a fazer a transferência. A AA respondeu que não, que não tinha sido ela a efetuar a transação, então a suposta colaboradora perguntou se queria anular a transferência, ao que a AA respondeu que sim, entretanto perguntou se queria que lhe enviasse um e-mail, ou anular a transação já! A cliente pediu para anular de imediato a

transação e a suposta colaboradora começou a pedir os dados á relativamente á Password (terceiro o sexto e o décimo dígito), entretanto perguntou se recebeu uma mensagem e pediu o código da mesma o qual a AA facultou! A suposta colaboradora despediu-se e perguntou se precisava de mais alguma coisa, e que durante as próximos 24 horas iria receber um email ou ser contactada pelo Banco 1… para saber a identificação da pessoa que lhe supostamente tinha feita a transferência."

37. Feita a participação, e tendo sido apurado que a conta bancária para onde fora transferido o dinheiro da Autora, sendo conta do mesmo banco, a Autora indagou se era possível bloquear a conta do titular para onde havia sido transferido o dinheiro da Autora.

38. A autora foi aconselhada pelos funcionários do balcão de … a ir apresentar queixa-crime, o que fez.

39. No balcão da Ré no …, a Autora foi informada pelos funcionários/ colaboradores de que o acesso à sua conta bancária através da aplicação e do site do Banco, ou seja, o seu contrato relativo aos serviços de homebanking, tinha sido imediatamente cancelado, no seguimento do telefonema da Autora.

40. Uma semana depois do sucedido, deslocou-se novamente ao balcão da Ré no …, pediu para falar com o gerente, Sr. HH e novamente expôs todo o sucedido no dia 29/03/2022.

41. Nessa altura foi informada por um dos colaboradores da Ré de que do montante que havia sido transferido da sua conta – € 4.916,32 (quatro mil novecentos e dezasseis euros e trinta e dois cêntimos) – € 3.916,32 tinham sido utilizados numa compra na Fnac em Lisboa e haviam sido feito dois levantamentos no valor de € 500,00, tendo a conta de destino ficado sem qualquer valor.

42. O gerente do balcão da Ré no …, Sr. HH, esclareceu a Autora que o Banco não se podia responsabilizar pela transferência realizada, pois a Autora havia facultado os números da sua password/cartão matriz, tendo esta respondid que não havia cedido facultado o número de adesão ou a chave multicanal referente à sua conta bancária.

43. Ao que o Sr. HH respondeu, esclarecendo que se tratava de uma situação de "phishing".

44. O CA Online exige a introdução do número de adesão e da chave multicanal para o acesso ao serviço, bem como a introdução de três dígitos

aleatórios da password para a realização de toda e qualquer operação de pagamento.

45. Até 14 de setembro de 2019 apenas eram exigidas três posições aleatórias da password para a realização de transações de cariz financeiro.

46. A Cliente, querendo, poderia, contudo, aderir voluntariamente ao Sistema de Autenticação Forte ("SAF") - autenticação baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a confidencialidade dos dados de autenticação".

47. A Autora aderiu ao SAF, voluntariamente, no dia 31 de julho de 2019 às 11:20:17, passando a exigir-se para a realização de transações financeiras através do CA Online, para além das três posições aleatórias da password, a OTP de autorização enviada por SMS para o telemóvel do titular associado ao sistema multicanal.

48. Mesmo que não o tivesse feito, a verdade é que, a partir de 14 de setembro 2019, passou a exigir-se sempre a introdução de três posições aleatórias da password e a OTP de autorização para a autorização de cada operação, pelo que deixou, de ser voluntária a adesão ao SAF, na medida em que passou a ser obrigatória a autenticação forte para a realização de toda e qualquer operação de pagamento.

49. A partir de 14 de setembro de 2019, o acesso ao CA Online passou a exigir, a cada 90 dias, a introdução de uma OTP de acesso ou de login, para além dos sempre necessários o número de adesão e a chave multicanal.

50. À data dos factos – março de 2022 – o acesso ao CA Online era efetuado através da introdução do número de adesão, da chave multicanal e, a cada 90 dias, de uma OTP de login enviada por SMS para o número de telemóvel associado à adesão do sistema multicanal. No ínterim dos referidos 90 dias, o acesso ao CA Online era efetuado apenas através da introdução do número de adesão e da chave multicanal;

51. A partir de outubro de 2022, a Autora apercebeu-se de um reforço de autenticação no LOGIN ao serviço de homebanking da Ré, quando se acede ao serviço online através do site da instituição bancária, sendo enviado por sms um código numérico com seis dígitos, o qual tem de ser introduzido para

permitir acesso à conta e aos serviços, sendo que porém essa alteração se iniciou em abril de 2022.

52. O acima descrito mecanismo de autenticação reforçado não existia à data – março de 2022 – em que ocorreram os factos que deram origem à queixa crime identificada e ao presente processo.

53. A partir de abril de 2022 passou a exigir a introdução da OTP do acesso/ login em todos os acessos ao CA Online.

54. À data da realização da burla, nos termos do Contrato celebrado entre a Autora e a Ré, a OTP só era solicitada aos clientes do CA Online, nos seguintes casos:

i) Acesso ao CA Online de 90 em 90 dias;

ii) Transferências;

iii) Pagamento de serviços;

iv) Carregamento de Telemóveis;

v) Definição de um limite de Movimentação Diário no CA Online.

55. Tal alteração deveu-se não a qualquer reconhecimento de falibilidade e insegurança do CA Online, mas antes ao aumento exponencial de fraudes informáticas de que os clientes de sistemas de homebanking passaram a ser alvo e ao intuito de reforçar o estado de alerta dos mesmos aquando do acesso a tais sistemas.

56. O acesso à conta bancária da Autora pela burlona foi feito através do CA Online.

57. Existem obrigações decorrentes da assinatura do contrato de homebanking para a instituição de crédito e para a cliente/Autora.

58. Cabia à instituição de crédito responsável pelo serviço no caso a Caixa Agrícola manter, sob rigorosa confidencialidade, os códigos de acesso e a informação constante nos mesmos, realizando as operações ordenadas pelos Clientes apenas quando possa assegurar, através de um sistema de autenticação forte, o sentido da ordem da Cliente.

59. Cabia à Cliente o especial dever de não revelar, nem por qualquer forma tornar acessível ao conhecimento de terceiros, os seus elementos de

identificação e os códigos de acesso, seja o número de adesão, seja o código multicanal, seja a password, sejam as OTP do login ao serviço ou de autorização de operações, elementos que são pessoais e intransmissíveis.

60. A Autora seguiu após a burla as instruções do Sr. HH, tendentes à resolução da situação, e enviou um e-mail a solicitar esclarecimentos no dia 11 de abril de 2022.

61. O e-mail da Autora viria a ter resposta no dia 18 de abril de 2022, do balcão de ....

62. Inconformada com a resposta que obteve, a Autora novamente enviou um e-mail, no dia 02 de maio de 2022.

63. A pessoa que praticou a referida "fraude informática" detinha alguns dados pessoais e intransmissíveis da Autora, ignorando a Ré como foram obtidos, e convenceu a Autora a partilhar telefonicamente os detalhes dos seus dados de utilização do CA Online.

64. A Ré sistematicamente alerta os seus Clientes para situações de burla e fraudes, desde logo, aquando da subscrição do sistema multicanal, foi disponibilizado um documento com Recomendações de Segurança nos Canais Digitais á Autora.

65. A 09 e a 25 de fevereiro de 2022, foram lançados novos pop-ups de alerta na página de acesso / login ao CA Online, que aparecem sempre aquando de cada acesso ao Ca Online, após a introdução do número de adesão e antes da introdução da chave multicanal, que têm de ser expressamente fechados pelo utilizador para este poder concretizar o acesso ao serviço que advertiam para novas tentativas de phishing, destacando os dados que não são pedidos pela Ré, e frisando os elementos que os autores deste tipo de práticas solicitavam, reiterando os cuidados que os utilizadores do CA Online devem ter.

66. Entre o dia seguinte à publicação do 1.º pop-up acima identificado e o dia anterior ao da chamada efetuada pela terceira mal-intencionada – período de 46 dias -iniciou sessão no sistema multicanal, pelo menos, 58 vezes.

67. A 25 de março de 2022, quatro dias antes da ocorrência da burla, a Autora acedeu ao CA Online, tendo necessariamente visualizado o Pop Up com o teor "O Banco 1... ALERTA não forneça os seus dados pessoais ou códigos de acesso por telefone".

68. A 21 de janeiro de 2022 e a 25 de fevereiro de 2022, a Ré foi também remetendo por SMS alertas dando conta das tentativas de phishing que estavam a ser perpetradas, conforme cópia das mensagens que ora se junta e aqui se dá por integralmente reproduzida para todos os legais e devidos efeitos.

69. A mensagem remetida a 25 de fevereiro de 2022 foi recebida pela Autora às 18:54:06 e refere "Alertamos para possíveis tentativas de fraude ou burla. Não aceda a links e nunca forneca por telefone os seus codigos de acesso aos canais se for contactado."

70. O Banco de Portugal lançou uma campanha, designada "#ficaadica: Fraude financeira digital: também caía nesta?". Na página do Banco de Portugal pode ler-se: "Recebe um e-mail ou uma mensagem do seu banco ou outro prestador de serviços de pagamento ou de uma entidade com a qual contratou um serviço. Dizem que a sua conta pode estar comprometida ou bloqueada e pedem que faça login para recuperar o acesso. Clica no link e insere as suas credenciais ou transmite-as por telefone, sem pensar duas vezes? É provável que esteja perante uma forma comum de phishing, isto é, um ataque destinado a captar os seus dados pessoais. E há outras técnicas fraudulentas, aparentemente inofensivas igualmente eficazes, que são usadas por pessoas que, em qualquer parte do mundo, se podem apropriar dos seus dados. Muitas vezes os piratas informáticos utilizam informação que obtêm nas redes sociais e utilizam a manipulação psicológica para ganhar a confiança da vítima e, assim, obter informações confidenciais."

71. A chamada rececionada pela Autora foi efetuada através de um número móvel.

72. O Banco 1… dispõe de um serviço telefónico, a Linha Direta, este serviço é utilizado para os Clientes contactarem o Banco 1… e não o contrário consiste num "serviço telefónico, informativo ou transaccional, que permite o atendimento automático (IVR) ou personalizado e que se destina a possibilitar aos Titulares aderentes do Sistema Multicanal a realização de consultas e/ou operações financeiras; também permite o contacto dos Clientes em geral para obtenção de informações, esclarecimentos ou para apresentar sugestões, pedidos e reclamações, através do número de telefone 808 20 60 60 (custo da chamada local)".

73. Existem diferentes formas de o terceiro burlão poder ter acesso a informação de dados pessoais dos burlados, designadamente, através de redes

de wi-fi públicas sem recurso a uma VPN adequada (uma "Virtual Private Network" – rede privada virtual, que providencia uma conexão encriptada e, desse modo, segura), através da instalação de malware ou spyware nos seus dispositivos informáticos ou eletrónicos (computador ou telemóvel), entre outras formas ilícitas de acesso a dados pessoais, tais como a subscrição in loco ou online com vista a obter determinados descontos ou antecipação de promoções de marcas, ou a participação em determinados concursos online para ganhar determinados produtos ou ainda a associação do email e do número de telefone a redes sociais, facilmente expõem pessoas à divulgação destes dados, sem que os mesmos se apercebam.

74. A Ré foi sujeita a auditorias regulares que não detetaram qualquer falha de segurança ao serviço prestado por si e não sofreu aquela qualquer ingerência fraudulenta, informática ou outra, tal como avaria técnica ou deficiência do CA Online que tenha exposto os dados dos Clientes e desta cliente em particular a terceiros, pelo facto de não ter realizado qualquer comunicação dando conta desse evento ao Banco de Portugal, o que se lhe impunha, caso tivesse acontecido.

75. A Ré, reportou a situação às áreas técnicas e às autoridades competentes.

76. A Ré diligenciou no sentido de ser contactado o beneficiário da transferência bancária em causa, de forma que este justificasse a sua origem e finalidade, bem como utilização da conta em questão, tendo o mesmo informado desconhecer tal transferência bancária.

77. A Ré não podia reverter a transferência que foi ordenada e devidamente autorizada pela Autora, em estrita observância de todos os procedimentos instaurados e que estão em consonância com as normas legais vigentes.

78. A Ré não tinha como cancelar ou reverter a transferência realizada, porquanto a mesma constitui uma transferência intrabancária, isto é, entre contas bancárias abertas no mesmo Banco, que são sempre concretizadas de imediato e uma vez ordenada uma ordem de pagamento, a mesma é irrevogável.

79. A situação em causa trouxe à Autora angústia, tristeza, revolta, e um grande sentimento de injustiça, tendo passado a andar nervosa e a não dormir.

Factos julgados não provados na sentença recorrida:

a) Feita a participação, e tendo sido apurado que a conta bancária para onde fora transferido o dinheiro da Autora estava relacionada com o balcão da Ré

localizado na Amadora, em Lisboa, a Autora indagou sobre a possibilidade de contactar o balcão da Ré na Amadora, uma vez que a pessoa que recebeu o dinheiro tinha morada naquela localidade, por forma a solicitar o cancelamento da operação e evitar que o dinheiro fosse utilizado, ao que lhe foi respondido que tal não era possível sem uma justificação.

b) Desde a alegada burla a Autora apenas tem acesso à sua conta bancária no multibanco ou num balcão da Ré.

c) O Sr. HH esclareceu a Autora que se tratava de uma situação de "phishing", não tendo dado mais nenhuma explicação, tendo ficado a Autora sem perceber o que era a situação de phishing.

d) Até hoje a Ré ainda não deu cabal esclarecimento sobre o sucedido, pois se Autora facultou os números da sua password (cartão matriz) e o código enviado por sms (otp), certo é que nunca a Autora revelou qual era o seu número de adesão, e nunca facultou a sua chave multicanal ou o seu PIN, elementos necessários e prévios ao acesso à conta e ao serviço de homebanking prestado pela Ré.

Da alteração da decisão relativa à matéria de facto

(…).

Da matéria de facto provada consolidada

A supratranscrita, que não se mostra necessário reproduzir aqui novamente.

B) De Direito

Da falha de segurança do sistema bancário

No caso em apreço, a Recorrente foi vítima de uma burla informática perpetrada por terceiro desconhecido que a contactou telefonicamente, identificando-se como colaboradora da Recorrida.

A referida pessoa conhecia a identificação da Recorrente, bem como o seu número de adesão e código multicanal, para acesso à página de homebaking da Autora no sistema da Ré.

Na posse destes dados, entrou nessa página e efetuou uma ordem de transferência no valor de € 4.916,32, após o que entrou em contacto com a Autora, a quem chamou pelo nome, solicitando os dados da sua password para confirmação da transferência, o que a Recorrente forneceu, bem como o OTP, código de autorização específico para aquela transação que foi recebido por sms de seguida, e que a Autora também forneceu.

A questão e apreço passa por analisar se, apesar de ter sido a Autora quem forneceu os dados da password e a OTP, ainda assim, a Ré deve ser responsabilizada pelos danos sofridos pela Autora.

Vejamos.

Nesta matéria, rege o disposto no Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME), aprovado pelo Dec.-Lei nº 91/2018, de 12 de Novembro (e posteriores alterações), o qual dispõe que:

Artigo 113.º

Prova de autenticação e execução da operação de pagamento

1 - Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada, incumbe ao respetivo prestador do serviço de pagamento fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento.

2 - Se a operação de pagamento tiver sido iniciada através de um prestador do serviço de iniciação do pagamento, recai sobre este último o ónus de provar que, no âmbito da sua esfera de competências, a operação de pagamento foi autenticada e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento por si prestado.

3 - Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, incluindo o prestador do serviço de iniciação do pagamento, se for caso disso, não é necessariamente suficiente, por si só, para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira, uma ou mais obrigações previstas no artigo 110.º

4 - Nas situações a que se refere o número anterior, o prestador de serviços de pagamento, incluindo, se for caso disso, o prestador do serviço de iniciação do pagamento, deve apresentar elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento.

Artigo 115.º

Responsabilidade do ordenante em caso de operação de pagamento não autorizada

1 - Em derrogação do disposto no artigo 114.º, o ordenante pode ser obrigado a suportar as perdas relativas às operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido, furtado, roubado ou da apropriação abusiva de um instrumento de pagamento dentro do limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, até ao máximo de (euro) 50.

2 - O disposto no n.º 1 do presente artigo não se aplica caso:

a) A perda, o furto, o roubo ou a apropriação abusiva de um instrumento de pagamento não pudesse ser detetada pelo ordenante antes da realização de um pagamento; ou

b) A perda tiver sido causada por atos ou omissões de um trabalhador, de um agente ou de uma sucursal do prestador de serviços de pagamento, ou de uma entidade à qual as suas atividades tenham sido subcontratadas.

3 - O ordenante suporta todas as perdas resultantes de operações de pagamento não autorizadas, se aquelas forem devidas a atuação fraudulenta ou ao incumprimento deliberado de uma ou mais das obrigações previstas no artigo 110.º, caso em que não são aplicáveis os limites referidos no n.º 1.

4 - Havendo negligência grosseira do ordenante, este suporta as perdas resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, ainda que superiores a (euro) 50.

5 - Se o prestador de serviços de pagamento do ordenante 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.

6 - Caso o beneficiário ou o seu prestador de serviços de pagamento não aceite a autenticação forte do cliente, reembolsa os prejuízos financeiros causados ao prestador de serviços de pagamento do ordenante.

7 - Após ter procedido à comunicação a que se refere a alínea b) do n.º 1 do artigo 110.º, o ordenante não deve suportar quaisquer consequências financeiras resultantes da utilização de um instrumento de pagamento perdido, furtado, roubado ou abusivamente apropriado, salvo em caso de atuação fraudulenta.

8 - Se o prestador de serviços de pagamento não fornecer meios apropriados que permitam a comunicação, a qualquer momento, da perda, furto, roubo ou da apropriação abusiva de um instrumento de pagamento, conforme requerido pela alínea c) do n.º 1 do artigo 111.º, o ordenante não fica obrigado a suportar as consequências financeiras resultantes da utilização

Daqui resulta que é o prestador do serviço de pagamento quem, em princípio, deve suportar os danos decorrentes da utilização do serviço de pagamento, por ser quem tem a capacidade de assegurar o seu complexo funcionamento[1].

O que não acontece se o prestador do serviço provar que a operação foi devidamente autorizada, que não se ficou a dever a avaria técnica ou a outra deficiência do serviço e que houve negligência grosseira por parte do utilizador, sobre o qual recai o dever de cuidar da preservação dos dados confidenciais que lhe são fornecidos[2].

No que toca à autorização da operação, verificamos que foram cumpridos todos os passos da mesma, nada tendo falhado, tendo sido utilizados os quatro passos necessários à autorização da transferência: número de adesão, código multicanal, password e OTP, estes últimos confessamente fornecidos pela Autora à pessoa que a contactou.

No que concerne à exigência de a operação indesejada não se ter ficado a dever a avaria técnica ou a outra deficiência do serviço, apurou-se que:

74. A Ré foi sujeita a auditorias regulares que não detetaram qualquer falha de segurança ao serviço prestado por si e não sofreu aquela qualquer ingerência fraudulenta, informática ou outra, tal como avaria técnica ou deficiência do CA Online que tenha exposto os dados dos Clientes e desta cliente em particular a terceiros, pelo facto de não ter realizado qualquer comunicação dando conta desse evento ao Banco de Portugal, o que se lhe impunha, caso tivesse acontecido.

Inexistindo avaria ou deficiência, importa ainda saber da responsabilidade da Ré quanto ao conhecimento parte de terceiro, do número de adesão e do código multicanal atribuídos à Autora aquando da contratação do serviço de homebanking.

Nesta matéria, apurou-se que:

6. Para o acesso ao sistema multicanal, é atribuído ao Cliente um número de adesão, que consiste num código numérico de oito posições, gerado pelo sistema após ser efetuado, com sucesso, um Pedido de Adesão ao sistema multicanal.

7. Para concretizar o acesso, é também necessária a chave multicanal, que consiste num código numérico de 8 posições que permite, em conjunto com o

número de adesão, identificar inequivocamente o Cliente para o acesso à realização de Consultas no CA Online Particulares e na Linha Direta.

11. No que se refere à informação detida pela Ré, esta apenas conhecia o número de adesão da Cliente, uma vez que a Ré não conhece nem tem como conhecer a chave multicanal, dado que a validação da chave multicanal é feita com base numa chave encriptada a partir da chave multicanal definida pela Cliente aquando do primeiro acesso ao sistema multicanal.

73. Existem diferentes formas de o terceiro burlão poder ter acesso a informação de dados pessoais dos burlados, designadamente, através de redes de wi-fi públicas sem recurso a uma VPN adequada (uma "Virtual Private Network" – rede privada virtual, que providencia uma conexão encriptada e, desse modo, segura), através da instalação de malware ou spyware nos seus dispositivos informáticos ou eletrónicos (computador ou telemóvel), entre outras formas ilícitas de acesso a dados pessoais, tais como a subscrição in loco ou online com vista a obter determinados descontos ou antecipação de promoções de marcas, ou a participação em determinados concursos online para ganhar determinados produtos ou ainda a associação do email e do número de telefone a redes sociais, facilmente expõem pessoas à divulgação destes dados, sem que os mesmos se apercebam.

A este propósito, ver acórdão deste Tribunal da Relação de Coimbra de 11 de Fevereiro de 2020, proferido no processo nº 8592/17.9T8CBR.C1, disponível em www.trc.pt, relativo a factos aos quais era aplicável a legislação em vigor, mas nesta parte inteiramente atual:

3.Entre esses contratos que se encontram associados à abertura de conta encontra-se o designado contrato de homebanking, que normalmente se concretiza através da possibilidade conferida pela entidade bancária aos seus clientes, mediante a aceitação de determinados condicionalismos, de utilizar toda uma panóplia de operações bancárias, on line, relativamente às contas de que sejam titulares, os quais têm vindo a obter um forte incremento e adesão pelas inegáveis vantagens que propicia às partes, quer aos clientes, permitindo-lhes um acesso mais rápido, continuado (sem limitação de horários) e cómodo (sem deslocações aos balcões) às suas contas e, desse modo, a realização das mais variadas operações, quer aos bancos, permitindo agilizar serviços e otimizar a gestão dos seus recursos humanos, com a inerente diminuição de custos.

4.Tratando-se de serviços prestados via internet, os mesmos são frequentemente alvo de ataques dos designados hackers, com objetivo de se apropriarem, de forma ilícita, dos fundos existentes nas contas bancárias.

5.De entre essas técnicas de fraude informática mais comuns, destacam-se o phishing que, grosso modo, consiste no envio "ao cliente" de mensagens de correio eletrónico, que provêm aparentemente do banco prestador do serviço, visando obter dados confidenciais que permitam o acesso ao serviço de pagamento eletrónico, e o pharming, que se consubstancia numa técnica mais sofisticada através da qual é corrompido o próprio nome de domínio de uma instituição financeira, redirecionando o utilizador para um site falso – mas em tudo similar ao verdadeiro – sempre que este digita no teclado a morada correta do seu banco, ou seja, através dessa técnica suplanta-se o sistema de resolução dos nomes de domínio para conduzir o usuário a uma pagina Web falsa, clonada da página real, ou melhor ainda, essa técnica baseia-se em alterar o IP numérico de uma direção no próprio navegador, através de programas que captam os códigos de pulsação do teclado, o que pode ser feito através da difusão de vírus via spam, e que leva o usuário a pensar que está a aceder a um determinado site – por exemplo o do seu banco –, quando na realidade está a entrar no IP de uma página Web falsa.

7.Negando o utilizador ter dado autorização para uma operação de pagamento que foi executado pela instituição bancária, é sobre esta que impende o ónus de prova de que a operação de pagamento não foi afetada por avaria técnica ou qualquer outra deficiência e/ou que esse pagamento só foi possível devido à atuação fraudulenta daquele ou ao incumprimento deliberado ou com negligência grave dos deveres/obrigações… (sublinhado nosso)

Assim, também aqui, nenhuma responsabilidade pode ser imputada à Ré, no que toca ao conhecimento, por terceiros, da identificação, número de adesão e código multicanal da Autora, os quais, se não foram de alguma forma fornecidos por esta, terão certamente sido obtidos por uma das formas ilícitas de acesso a dados informáticos supra descritas.

Finalmente, no que diz respeito à atuação com negligência grosseira por parte do utilizador, dispõe o artº 487º, nº 2, do Código Civil, que *A culpa é apreciada, na falta de outro critério legal, pela diligência de um bom pai de família, em face das circunstâncias de cada caso*[3].

Como nos diz Francisco Mendes Correia, “Responsabilidade e risco nas operações de pagamento não autorizadas” *in* “Revista da Faculdade de Direito da Universidade de Lisboa”, 2023, número 2, págs. 446 e 447.

Quanto à distinção entre negligência e negligência grosseira, como se referiu, o legislador europeu forneceu uma indicação, nos Considerandos da DSP 2, apelando, como critério diferenciador a um "grau significativo de imprudência" e concretizando num exemplo (a conservação de credenciais de segurança juntamente com o instrumento de pagamento, num formato que seja aberto e facilmente detetável por terceiros). Parece estar aqui em causa a intensidade do juízo de censura e não uma diferenciação estrutural, que envolva como elemento adicional a consciência da ilicitude. Por outro lado, um grau significativo não parece apontar para níveis máximos de imprudência, que provocassem repúdio ou escândalo, mas apenas para um grau mais intenso de censurabilidade. (sublinhado nosso)

No caso em apreço, apurou-se que:

44. O CA Online exige a introdução do número de adesão e da chave multicanal para o acesso ao serviço, bem como a introdução de três dígitos aleatórios da password para a realização de toda e qualquer operação de pagamento.

45. Até 14 de setembro de 2019 apenas eram exigidas três posições aleatórias da password para a realização de transações de cariz financeiro.

46. A Cliente, querendo, poderia, contudo, aderir voluntariamente ao Sistema de Autenticação Forte (“SAF”) - autenticação baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a confidencialidade dos dados de autenticação”.

47. A Autora aderiu ao SAF, voluntariamente, no dia 31 de julho de 2019 às 11:20:17, passando a exigir-se para a realização de transações financeiras através do CA Online, para além das três posições aleatórias da password, a OTP de autorização enviada por SMS para o telemóvel do titular associado ao sistema multicanal.

48. Mesmo que não o tivesse feito, a verdade é que, a partir de 14 de setembro 2019, passou a exigir-se sempre a introdução de três posições

aleatórias da password e a OTP de autorização para a autorização de cada operação, pelo que deixou, de ser voluntária a adesão ao SAF, na medida em que passou a ser obrigatória a autenticação forte para a realização de toda e qualquer operação de pagamento.

Ou seja, à data dos factos, nos termos do contrato celebrado entre a Autora e a Ré, eram necessários o número de adesão e a chave multicanal para o acesso ao serviço, três dígitos aleatórios da password para a realização de toda e qualquer operação de pagamento e a introdução da OTP para confirmação de ordens de transferência.

Mais se tendo apurado que:

8. Como medida de segurança, aquando do primeiro acesso ao sistema multicanal, a Cliente teve de alterar, obrigatoriamente, a chave multicanal atribuída no momento da ativação do serviço.

9. Incumbe-se a Cliente ainda de proceder, regularmente, à alteração da chave multicanal.

15. No período que mediou a celebração do Contrato de Depósito entre a Autora e a Ré e a data da alegada burla, o teor das Condições Gerais do mesmo foi alterado, acompanhando a evolução legislativa.

16. Tais alterações foram comunicadas à Autora, conforme as Condições Gerais assinadas pela Autora a 31 de julho de 2019.

28. A Autora (…), a pedido da putativa colaboradora da Ré, transmitiu-lhe o código de autorização da operação, tendo estranhado nesta altura que a mensagem recebida fosse para confirmar e não cancelar a operação, dizendo-lhe a burlona que era o que iria suceder se não cancelasse a operação.

30. Através de um discurso encadeado, o terceiro encaminhou a Autora não só a partilhar os três dígitos aleatórios da password pedidos aquando da realização de uma operação, como também, o código "OTP" de autorização, sigla que abrevia a expressão "one time password", que consiste numa palavra-passe de utilização única e que é apenas válida durante um período muito reduzido de tempo (doravante "OTP"), ambos necessários para a concretização da transferência ordenada.

58. Cabia à instituição de crédito responsável pelo serviço no caso a Caixa Agrícola manter, sob rigorosa confidencialidade, os códigos de acesso e a informação constante nos mesmos, realizando as operações ordenadas pelos

Clientes apenas quando possa assegurar, através de um sistema de autenticação forte, o sentido da ordem da Cliente.

59. Cabia à Cliente o especial dever de não revelar, nem por qualquer forma tornar acessível ao conhecimento de terceiros, os seus elementos de identificação e os códigos de acesso, seja o número de adesão, seja o código multicanal, seja a password, sejam as OTP do login ao serviço ou de autorização de operações, elementos que são pessoais e intransmissíveis.

63. A pessoa que praticou a referida "fraude informática" detinha alguns dados pessoais e intransmissíveis da Autora, ignorando a Ré como foram obtidos, e convenceu a Autora a partilhar telefonicamente os detalhes dos seus dados de utilização do CA Online.

64. A Ré sistematicamente alerta os seus Clientes para situações de burla e fraudes, desde logo, aquando da subscrição do sistema multicanal, foi disponibilizado um documento com Recomendações de Segurança nos Canais Digitais á Autora.

65. A 09 e a 25 de fevereiro de 2022, foram lançados novos pop-ups de alerta na página de acesso / login ao CA Online, que aparecem sempre aquando de cada acesso ao Ca Online, após a introdução do número de adesão e antes da introdução da chave multicanal, que têm de ser expressamente fechados pelo utilizador para este poder concretizar o acesso ao serviço que advertiam para novas tentativas de phishing, destacando os dados que não são pedidos pela Ré, e frisando os elementos que os autores deste tipo de práticas solicitavam, reiterando os cuidados que os utilizadores do CA Online devem ter.

67. A 25 de março de 2022, quatro dias antes da ocorrência da burla, a Autora acedeu ao CA Online, tendo necessariamente visualizado o Pop Up com o teor "O Banco 1… ALERTA não forneça os seus dados pessoais ou códigos de acesso por telefone".

68. A 21 de janeiro de 2022 e a 25 de fevereiro de 2022, a Ré foi também remetendo por SMS alertas dando conta das tentativas de phishing que estavam a ser perpetradas, conforme cópia das mensagens que ora se junta e aqui se dá por integralmente reproduzida para todos os legais e devidos efeitos.

69. A mensagem remetida a 25 de fevereiro de 2022 foi recebida pela Autora às 18:54:06 e refere "Alertamos para possíveis tentativas de fraude ou burla.

Não aceda a links e nunca forneça por telefone os seus códigos de acesso aos canais se for contactado."

Dispõe o artº 110º, do RJPSME, que:

Artigo 110.º

Obrigações do utilizador de serviços de pagamento associadas aos instrumentos de pagamento

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 objetivas, não discriminatórias e proporcionais;

(...)
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.

Ora, a Autora violou estas suas obrigações de utilizadora de serviços de pagamento, ao informar terceiro dos dados da sua password e do código OTP, o que fez de forma manifestamente negligente, uma vez que o resultado era previsível para qualquer pessoa normalmente diligente que se encontrasse na posição da Autora.

Como se diz no elenco de factos provados *Cabia à Cliente o especial dever de não revelar, nem por qualquer forma tornar acessível ao conhecimento de terceiros, os seus elementos de identificação e os códigos de acesso, seja o número de adesão, seja o código multicanal, seja a password, sejam as OTP do login ao serviço ou de autorização de operações, elementos que são pessoais e intransmissíveis.*

Na verdade, a Ré comunicou à Autora as suas obrigações, devendo estar consciente de que não poderia fornecer a terceiros os dados da sua password e código OTP, o que lhe era amiúde relembrado por aquela, nomeadamente na *A 25 de março de 2022, quatro dias antes da ocorrência da burla, a Autora acedeu ao CA Online, tendo necessariamente visualizado o Pop Up com o teor*

"O Banco 1… ALERTA não forneça os seus dados pessoais ou códigos de acesso por telefone".

Acresce que a própria mensagem que lhe forneceu o código OTP referia o objetivo de confirmar uma transferência, tendo a Autora *estranhado nesta altura que a mensagem recebida fosse para confirmar e não cancelar a operação,* mas, ainda assim, forneceu-o à sua interlocutora.

Assim, bem andou o Tribunal *a quo* ao julgar improcedente a presente ação, destacando-se a seguinte passagem da sentença recorrida, com a qual concordamos integralmente:

A pessoa que praticou a referida "fraude informática" detinha alguns dados pessoais e intransmissíveis da Autora, ignorando a Ré como foram obtidos, e convenceu a Autora a partilhar telefonicamente os detalhes dos seus dados de utilização do CA Online.

Em concreto, a Autora disponibilizou apesar de não se ter provado em concreto como, apesar de várias formas terem sido avançadas pela Ré, ao autor da fraude informática os elementos necessários para efetuar o acesso ao CA Online, pois alguém já estava na posse do n.º de adesão, chave multicanal e PIN e, bem assim, os elementos necessários para realizar uma transferência bancária no montante de € 4.916,32.

Entre as técnicas mais frequentemente utilizadas por terceiros para aceder, fraudulentamente, através do sistema, à conta do cliente utilizador do serviço de homebanking, contam-se: (i) o phishing, que consiste "o envio de mensagens de correio eletrónico, que provêm aparentemente do banco prestador do serviço, tentando obter dados confidenciais que permitam o acesso ao serviço de pagamento eletrónico; e (ii) o pharming, uma técnica mais sofisticada em que é «corrompido» o próprio nome de domínio de uma instituição financeira, redirecionando o utilizador para um site falso – em tudo similar ao verdadeiro – sempre que este digita no teclado a morada correta do seu banco".

O autor da fraude informática pode ter tido acesso aos dados da Autora por diferentes vias que não através da Ré ou da informação que esta detém sobre a Autora.

Através de um discurso encadeado, o terceiro encaminhou a Autora não só a partilhar os três dígitos aleatórios da password pedidos aquando da realização de uma operação, como também, o código "OTP" de autorização, sigla que

abrevia a expressão "one time password" que consiste numa palavra-passe de utilização única e que é apenas válida durante um período muito reduzido de tempo (doravante "OTP"), ambos necessários para a concretização da transferência ordenada.

O dinheiro foi, assim, movimentado em conformidade com as instruções dadas pela Autora, em observância das regras contratuais existentes e aceites pela própria, pois cabia à Cliente o especial dever de não revelar, nem por qualquer forma tornar acessível ao conhecimento de terceiros, os seus elementos de identificação e os códigos de acesso, seja o número de adesão, seja o código multicanal, seja a password, sejam as OTP do login ao serviço ou de autorização de operações, elementos que são pessoais e intransmissíveis (cfr. Cláusula 40.2 do Documento n.º 2 DA CONTESTAÇÃO Condições Gerais atualizadas do Contrato de Depósito Singular).

Logo a Autora ao contrário do que alega, não "cumpriu escrupulosamente as obrigações a que estava adstrita", por alegadamente "ter permitido o acesso à conta da Autora por alguém que não deveria ter nem o número de adesão nem a chave multicanal", sendo que se aqui poderá ter sido enganada sem se dar conta, coisa diferente é quando já transmite via telefone posições da password e código de OTP.

Ao nosso ver não existiu violação da Ré da obrigação plasmada na alínea a), do n.º 1 do artigo 111.º do DL 91/2018 de "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".

Na verdade a Ré conseguiu demonstrar que foi sujeita a auditorias regulares que não detetaram qualquer falha de segurança ao serviço prestado pela Ré e não sofreu aquela qualquer ingerência fraudulenta, informática ou outra, tal como avaria técnica ou deficiência do CA Online que tenha exposto os dados dos Clientes e desta em particular a terceiros, pelo facto de não ter realizado qualquer comunicação, dando conta desse evento ao Banco de Portugal, o que se lhe impunha, caso tivesse acontecido (...).

A ré comprovou que o CA Online, cumpre e observa todas as regras de operacionalidade impostas não só pela Entidade Bancária Europeia, designadamente, no que se refere aos métodos de autenticação, mas também as que resultam do Decreto-Lei n.º 91/2018, designadamente, o disposto no

artigo 104.º deste diploma, ao exigir o sistema de autenticação forte do Cliente para a realização de uma operação de pagamento eletrónico.

A Ré comprovou aliás como resultou da vária prova testemunhal que não existiu qualquer avaria técnica ou deficiência do CA Online, que impusesse à Ré reembolsar ou ressarcir a Autora por quaisquer danos sofridos.

Deste modo, cumpre julgar improcedente o presente recurso.

IV - Decisão

Nestes termos, acordam os Juízes Desembargadores da 3ª Secção deste Tribunal da Relação em julgar improcedente o recurso, mantendo a decisão recorrida.

Custas pela Apelante – artºs 527º, nºs 1 e 2, 607º, nº 6 e 663º, nº 2, todos do Código de Processo Civil.

Coimbra, 25 de Março de 2025

Com assinatura digital:

Anabela Marques Ferreira

Hugo Meireles

Luís Manuel Carvalho Ricardo

[1] Como se diz no acórdão do Supremo Tribunal de Justiça de 23 de Janeiro de 2024, proferido no processo nº 379/21.0T8FAR.E1.S1, disponível em www.dgsi.pt:

I - O contrato de "homebanking" celebrado entre a autora e banco réu é o acordo mediante qual o cliente adere a um serviço prestado pelo banco, que consiste na possibilidade de manter relações via internet, de forma a aceder a informações sobre produtos e serviços do banco; obter informações e realizar operações bancárias sobre contas de que a autora fosse titular e, realizar pagamentos, cobranças e operações de compra, venda, subscrição ou resgate sobre produtos ou serviços disponibilizados pelo banco.

II - Apenas o prestador do serviço de pagamento (banco) pode assegurar a operacionalidade do complexo sistema informático utilizado e a regularidade do seu funcionamento, garantindo, também, a confidencialidade dos dispositivos de segurança que permitem aceder ao instrumento de pagamento.

III - Por esta razão, recai sobre o banco prestador do serviço o risco das falhas e do deficiente fundamento do sistema impendendo ainda sobre o mesmo o ónus da prova de que a operação de pagamento não foi afetada por avaria técnica ou qualquer outra deficiência.

IV - Ao utilizador do serviço de pagamento - que deve dispor de um conjunto de dispositivos de segurança, como o código de acesso, cartão matriz, entre outros, que lhe vão permitir aceder a serviço, dada a sua função de autenticação e identificação - exige-se que tome as medidas razoáveis em ordem a preservar a eficácia desses dispositivos. (sublinhado nosso)
[2] Neste sentido, também, acórdão do Tribunal da Relação do Porto de 12 de Outubro de 2023, proferido no processo nº 728/21.8T8VFR.P1, disponível em www.dgsi.pt, onde se diz:
I - Da conjugação do art. 115.º, n.º 3 e n.º 4 com o art. 113.º, n.º 1, n.º 3 e n.º 4 do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, aprovado pelo Decreto-Lei n.º 91/2018, de 12 de novembro, resulta que o risco inerente à utilização e funcionamento dos serviços de pagamento recai sobre o prestador de serviços de pagamento.
II - Para se eximir da obrigação de reembolso prevista no n.º 1 do art. 114.º, cabe ao prestador de serviços o ónus de prova não só de que a operação de pagamento foi devidamente autenticada (art. 113.º, n.º 1), mas ainda que o utilizador dos serviços de pagamento (ordenante) atuou de forma fraudulenta ou incumpriu de forma deliberada uma ou mais das suas obrigações decorrentes do artigo 110.º, ou que atuou com negligência grosseira (art. 113.º, n.º 3 e n.º 4).
III - A qualificação como negligência grosseira da atuação do utilizador dos serviços de pagamento (ordenante) exige que se possa afirmar que, dentro das circunstâncias do caso concreto, agiu de forma perfeitamente incauta, constituindo o seu comportamento um erro grave, que a generalidade das pessoas minimamente diligentes não cometeria. (sublinhado nosso)

[3] Ensina Ana Prata, Dicionário Jurídico, 2ª edição, Almedina, págs. 394 e 395, que: *O conceito jurídico de negligência é assimilável ao de mera culpa, consubstanciando-se na omissão do dever de diligência, sendo a diligência exigível aquela que teria um bom pai de família em face das circunstâncias do*

caso (cfr. art. 487.º, n.º 2, C.C.). A negligência ou mera culpa refere-se (...) às situações em que o agente não prevê o resultado danoso, por imprevidência ou descuido, embora este resultado fosse previsível, se ele o houvesse ponderado e houvesse sido cauteloso.