Acórdão do Supremo Tribunal de Justiça

Processo: 9240720.5T8LSB.L1.S1
Nº Convencional: 7.ª SECÇÃO
Relator: MANUEL CAPELO
Descritores: ATIVIDADE BANCÁRIA
BANCO
INTERNET
RESPONSABILIDADE CONTRATUAL
DEPÓSITO BANCÁRIO
CONTA BANCÁRIA
HOMEBANKING
PHISHING
DOLO
CULPA DO LESADO
PRESSUPOSTOS
DEVER DE DILIGÊNCIA
CULPA
NEGLIGÊNCIA GROSSEIRA
TELEMÓVEL
CORREIO ELETRÓNICO
Data do Acordão: 12-12-2023
Votação: UNANIMIDADE
Texto Integral: S
Privacidade: 1
Meio Processual: REVISTA
Decisão: NEGADA A REVISTA
Sumário :

I - As perdas resultantes de operações de pagamento não realizadas e não autorizadas pelo utilizador/titular do serviço homebanking, mas por terceiros, nos termos do art. 796 nº1 do CCivil e do art. 115 do DL 91/2018 correm por conta do banco, exceto se forem devidas a atuação fraudulenta daquele ou a atuação grosseira do mesmo por incumprimento deliberado das obrigações que lhe estavam impostas, devendo o prestador do serviço demonstrar a existência de fraude, de dolo ou de negligência grosseira.

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

III - A negligência grosseira, merecedora de reprovação pelo mais elementar senso comum por configurar uma falta indesculpável na omissão dos deveres a que se está obrigado, não se verifica quando a lesada, com a atenção que lhe era exigida e de que era capaz nas circunstâncias do caso, não se pôde opor aos artifícios de complexidade eletrónica que lhe foram colocados por terceiros que se fizeram passar com aparente credibilidade pelos serviços do banco, solicitando a resolução de um problema que efetivamente, em momento anterior e por duas vezes, o banco informara dever ser resolvido.

IV - Tal negligência grosseira é de afastar se o acesso ao link, que foi fornecido na “sms” e que se apresentava como enviada pelo banco, com os elementos aí fornecidos pela lesada, não permitia, só por si, qualquer operação de movimento da conta, que careceria de confirmação por “SMS Code” a que os terceiros só vieram a aceder no dia seguinte e através de segundas vias do cartão do telemóvel da lesada sem que esta se tivesse apercebido de estar a fornecer ou ter fornecido quaisquer elementos necessários a essa obtenção.

Decisão Texto Integral:

Acordam no Supremo Tribunal de Justiça

Relatório

AA e BB instauraram ação declarativa comum contra Caixa Económica Montepio Geral SA e NOS – Comunicações, SA, pedindo a condenação solidária das rés a pagar-lhes:

- € 38.784,00 acrescida de juros de mora desde a data do conhecimento dos factos até à data do pagamento;

- € 10.000,00, a título de danos não patrimoniais, acrescida de juros de mora, desde a data da citação até integral pagamento.

Alegaram que em 11/03/2019 a A. recebeu uma sms que acreditou ser enviado pela 1ª R. referindo que o seu acesso à NET24 estava inativo e que teria de aceder ao site ali mencionado com designação Montepio e com hiperligação direta e alterar o seu Código PIN de modo a voltar a ter acesso à NET24 e ao seu cartão matriz, tendo assim procedido.

Referem que no dia 12/03/2019, foram realizadas 20 operações bancárias/pagamentos no valor total de 38.784 € no espaço de 20 minutos, que não foram autorizadas pelos AA e cujo destinatário desconhecem. As operações foram efetuadas através da utilização dos dados pessoais da 2ª A: número de cliente, código PIN e com coordenadas aleatórias do seu cartão matriz, validadas com código de autorização enviado por sms para o telemóvel associado à conta, por terceiros que obtiveram a segunda via do cartão SIM junto da 2ª R.

Concluem que competia às RR assegurar a segurança da utilização dos seus serviços aos seus clientes através de barreiras técnicas que impeçam estes esquemas fraudulentos, pedindo o valor dos montantes indevidamente retirados da conta e ainda pela angústia e revolta, tendo desistido de planos familiares que haviam traçado para as poupanças dos últimos 20 anos, danos morais no valor peticionado.

Os Réus, citados pessoal e regularmente, apresentaram contestação, pugnando pela improcedência, arguindo a 1ª ré a atitude negligente da A. no acesso aos seus dados por terceiros, com a consequente ausência de responsabilidade da ré.

Foi elaborado o despacho saneador, fixado o objeto do litígio e selecionados os temas de prova e foi realizada a audiência de julgamento, tendo sido proferida sentença que julgou a ação parcialmente procedente e condenou o Réu Caixa Económica Montepio Geral a reembolsar os Autores da quantia de € 38.784,00 euros, acrescida de juros de mora, à taxa de 4%, acrescidos de 10 pontos percentuais vencidos desde 14/03/2019 até à presente data e vincendos até integral pagamento. Mais condenou o Réu Caixa Económica Montepio Geral a pagar aos Autores uma indemnização por danos não patrimoniais no valor de 3.000 €, para a Autora e 1.000,00 € para o Autor.

Absolveu o Réu Caixa Económica Montepio Geral do mais peticionado e absolveu o Réu Nos Comunicações, SA do pedido.

Inconformada a 1ª ré Caixa Económica Montepio Geral interpôs recurso de apelação que foi julgado confirmando a decisão recorrida com um voto de vencido quanto à condenação da ré Montepio.

Desta decisão interpõe a mesma ré Montepio Geral SA recurso de revista concluindo que:

A) A R. não se conforma nem aceita a sua condenação, sequer parcial, nem a consequente responsabilidade por custas, confirmada, com voto de vencida, no acórdão recorrido.

B) Nada obsta à admissibilidade da revista nos termos gerais, mas a mesma seria ainda, e em qualquer caso, admissível a título excecional (artigo 672.º do CPC), na medida em que o Acórdão agora proferido mostra-se proferido contra o que vem decidido, relativamente a situação factual idêntica, em vários outros acórdãos, já transitados em julgado, proferidos no domínio da mesma legislação e sobre a mesma questão fundamental de direito, designadamente nos acórdãos cuja cópia se junta à presente revista (Acórdão do Tribunal da Relação de Lisboa de 12/07/2018 no Proc. n.º 2256/17.0T8LSB.L1-7; Acórdão do Tribunal da Relação de Évora de 12/04/2018, Proc. 9002/16.4T8STB.E1; Acórdão do Tribunal da Relação de Guimarães de 09/06/2020 no Proc. n.º 51/18.9T8PRG.G1; Acórdão do Tribunal da Relação do Porto de 14/07/2020 no Proc. n.º 22158/17.0T8PRT.P1; Acórdão do Tribunal da Relação de Lisboa de 01/10/2020 no Proc. n.º 19530/17.9T8LSB.L-8; Acórdão do Tribunal da Relação de Lisboa de 13/10/2022 no Proc. n.º 344/21.8T8AGH.L1-2.

C) Não foi apenas a R., agora Recorrente, a chamada, pelos AA. como “responsável face à relação contratual que estabeleceu com os AA. e as normas supra referidas.”, tendo também sido chamada à responsabilidade na presente ação a 2ª Ré, junto de quem, de forma violadora das obrigações reciprocamente assumidas por A. e 2ª R., foi obtido o último passo de autenticação perante a R. Recorrente, pelo

que seria por demais relevante apurar a peticionada responsabilidade da 2ª R.

D) Para a qualificação da atuação da A. como grosseiramente negligente nada releva o eventual comportamento de um terceiro, ou terceiros envolvidos em toda a operação e encadeamento de atos necessários para o efeito, na medida em que a ocorrência e configuração daquele ato de negligência grosseira não é eliminada ou alterada por este comportamento subsequente.

E) O acesso ilícito à conta dos AA. e o desvio patrimonial foi, como é sempre, praticado por um terceiro.

F) A decisão recorrida centra-se numa forma de comunicação do Banco com os seus clientes para excluir a responsabilidade da A. no seguimento da hiperligação numa mensagem SMS fraudulenta, com o argumento de que também o Banco contacta a cliente dessa forma. Porém, nunca os Bancos – e a Recorrente – excluíram as comunicações por SMS, antes alertam repetidamente para o conteúdo de mensagens recebidas por SMS ou correio eletrónico, cujo teor ou forma evidenciem o seu intuito fraudulento.

G) A atuação pretérita concreta da Autora não releva – nos termos legais e conforme jurisprudência abundante – para apurar a gravidade do seu comportamento negligente, pois esta é medida, não em função das características particulares de cada indivíduo, mas pelas características do cidadão médio colocado na mesma posição e com a medida de um "bom pai de família". Ademais, "a autora identificou-se com a profissão de professora, pelo que não é pessoa de parca instrução".

H) A interpretação restritiva do "aviso" contido no cartão matriz, de que se reportará apenas às operações a ser feitas com este, não encontra nos factos provados qualquer reflexo, e aliás contraria a prova documental constante dos autos (cfr. Ponto 88.), bem como as normas legais e disposições contratuais que estabelecem a obrigação de guardar segredo dos dados de acesso ao sistema.

I) NUNCA significa não, em tempo nenhum, nenhuma vez, jamais, em nenhuma circunstância, em nenhum momento no tempo passado, presente ou futuro, em tempo algum, em circunstâncias nenhumas, de modo nenhum, vez nenhuma.

J) A A. incumpriu o contrato de homebanking e contrariou todas as regras e informações de segurança veiculadas aquando da celebração do contrato de adesão ao serviço – de que a mesma declarou ter tomado conhecimento –, os avisos de segurança disponíveis no seu cartão matriz, bem como os constantes no próprio sistema de homebanking, que disparam quando o cliente a ele acede.

K) Foi a atuação grosseiramente negligente da Autora, no dia

11/03/2019, que permitiu e levou a que os autores do ato fraudulento, no dia seguinte, 12/03/2019, pelas 14h 50 min, tivessem junto da 2ª R. obtido indevidamente uma segunda via do cartão de serviço telefónico, pelo que o acesso ilícito às contas dos AA. foi proporcionado pelo fornecimento indevido de dados do cartão matriz, que determinou que um terceiro se tenha apropriado de todas as credenciais para a realização de operações, via homebanking.

L) A movimentação das contas de forma fraudulenta deveu-se a culpa da A.: a A. incumpriu, de forma grave e grosseira, os seus deveres contratuais, formalizados no contrato de homebanking. Não está afastada, mas antes claramente demonstrada, a negligência grave da A. ("um caso flagrante" na qualificação do "voto de vencida") preenchendo assim o estatuído no artigo 72.º, n.º 3 do Decreto-Lei n.º 317/2009, de 30/10.

M) Foi por causa imputável à negligência grosseira da A. e à subsequente atuação indevida, quiçá ilícita, de um funcionário da 2ª R., que se reuniram as condições para que um terceiro se apresentasse perante a R. Recorrente como se fosse a própria A., munido de todos os quatro passos de autenticação e segurança de acesso ao serviço de homebanking.

N) A R. cumpriu com todas as suas obrigações contratuais e o seu sistema não revelou qualquer falha técnica nem de segurança.

Cumpriu também com todos os deveres legais, designadamente de informação e alerta dos seus clientes e usuários, quando acedem à própria página inicial do sistema, para as situações correntes de utilização fraudulenta do serviço.

O) A R. estava obrigada, nos termos da lei, a colocar à disposição daquele que se apresentava como sendo a cliente, munido de todas as credenciais secretas de acesso ao sistema de homebanking, os fundos que esta lhe entregara no âmbito do contrato de depósito bancário.

P) A subsequente intervenção de terceiro – da 2ª R., e/ou do autor do ato fraudulento – não tem a virtualidade ou efeito de eliminar a primordial negligência grosseira da A. e de fazer retornar a responsabilidade à R. Recorrente, depois de aquela negligência a ter já excluído por completo.

Q) Haveria, por outro lado, de apurar-se a responsabilidade da 2ª R., "Demonstrado o ilícito contratual, a culpa e o dano provocado à Autora pelo uso ilegítimo do seu telemóvel que tal atuação da 2ª Ré permitiu (pelo menos, em termos naturalísticos)" (cfr. decisão proferida em 1ª instância).

R) A R. Recorrente ilidiu a presunção de culpa prevista no artigo 799.º do Código Civil, pelo que mostra-se excluída, sem qualquer margem para dissídio, a sua responsabilidade, nos termos legais, por

qualquer intromissão fraudulenta na conta do cliente.

S) Estando ilidida a presunção de culpa por parte da R., deve ser absolvida de todos os pedidos contra si formulados, incluindo da indemnização por danos morais a qualquer dos AA. e juros legais, pois não é merecedora de qualquer censura a sua atuação.

T) Agindo com negligência grave/grosseira, a A., e consequentemente os AA., titulares da conta de depósitos de onde foram removidos os valores, podem e devem ser responsabilizados pelas perdas decorrentes das operações de pagamento não autorizadas a que se referem os autos.

U) A Recorrente salienta ainda, e invoca em favor da tese que aqui defende, que inevitavelmente determinará que seja dado provimento à presente revista, todo o conteúdo unanimemente concordante de toda a extensa jurisprudência superior e doutrina, designadamente todas as decisões acima referidas a propósito da admissibilidade de uma revista extraordinária, bem como Acórdão de 19/09/2006 do Tribunal da Relação de Lisboa; Acórdão de 23/10/2012 do Tribunal da Relação de Guimarães Proc. n.º 305/09.5TBCBT.G1) Acórdão de 25/11/2013 do Tribunal da Relação de Guimarães, Proc. n.º 2869/11.4TBGMR.G1) Acórdão de 18/12/2013 do Supremo Tribunal de Justiça, Proc. 6479/09.8TBBRG.G1.S1) Acórdão de 25/06/2015 do Tribunal da Relação de Évora (Proc. n.º 3052/11.4TBSTR.E1) Acórdão do Tribunal da Relação de Lisboa (Proc. nº. 164/11.8TBSRT.L1-6) E, desde logo, o próprio conteúdo da douta fundamentação sumária do voto de vencida da Veneranda Juiz Relatora Anabela Calafate no acórdão recorrido.

V) Igualmente se entende (como a Veneranda Juiz Relatora Anabela Calafate no acórdão recorrido) que a omissão, pelos AA., do escrito referido no ponto 92 da matéria de facto, que a A. dirigiu à Recorrente, e a alegação contida nos artigos 98 e 99 da PI conjugados com a prova do contrário expressa naquele manuscrito da A. (que esta aceitou e confirmou nas suas declarações em audiência final), consubstancia até, litigância de má-fé, que não pode nesta sede deixar de ser sancionada.

W) Pelo que, repondo a conformidade com o Direito e a Justiça, deve, finalmente, a presente Revista ser julgada totalmente procedente, absolvendo-se a R. Recorrente de todos os pedidos e custas – como aliás pugnou a Veneranda relatora vencida no acórdão recorrido – ponderando ainda a responsabilidade da 2ª R. no cometimento do ato lesivo do património dos AA..

X) A decisão recorrida mostra-se assim violadora das seguintes disposições legais: Artigos 570º, 796, n.º 1, e 799º do Código Civil Artigos 67º a 72º do Decreto-Lei n.º 317/2009, de 30 de outubro, que transpôs para a ordem jurídica interna a Diretiva n.º 2007/64/CE, do

Parlamento Europeu e do Conselho, de 13 de novembro, relativa aos serviços de pagamento no mercado interno Artigos 103.º a 122.º, em particular o artigo 115.º, do Decreto-Lei n.º 91/2018, de 12 de novembro artigo 542.º, n.º 2, alínea b) do Código de Processo Civil

Conclui pedindo a revogação do acórdão recorrido e a improcedência da ação.

Não houve contra alegações

Cumpre decidir

… …

Fundamentação

Está provada a seguinte matéria de facto:

1. Em 01/07/2003, os aqui Autores, abriram, em conjunto, uma conta bancária solidária de depósitos à ordem, junto do Réu Banco, Caixa Económica Montepio Geral S.A., mais precisamente junto do balcão C.... .. .., figurando o Autor Marido, como 1.º titular da mesma e a Autora Mulher, como 2.ª titular daquela.

2. À referida conta, foi atribuído o n.º ... .-2,

3. E o IBAN: PT50 .... 4.

4. Os Autores aderiram ao serviço disponibilizado pelo Réu Banco, designado “homebanking NET24”

5. Tendo sido fornecidas, à aqui Autora, as chaves de acesso, que permitiam a utilização do serviço via internet, mais precisamente, um número de cliente, um código PIN/password e um cartão matriz para validar as operações bancárias on-line.

6. Tal serviço disponibilizado pelo Réu Banco permitiria à Autora, através de computador, tablet ou telefone com acesso à internet, 24 (vinte e quatro) horas por dia, (trezentos e sessenta e cinco) dias por ano, proceder a um conjunto de operações bancárias “on-line”, relativamente à conta de que era cotitular, nomeadamente, transferências bancárias e pagamentos de serviços.

7. A Autora raramente utilizou o referido serviço.

8. Todas as utilizações foram para consulta do saldo da conta à ordem.

9. E através do seu computador pessoal.

10. Para poder proceder a operações bancárias, através daquela plataforma informática, era necessária a introdução do número de cliente, do código PIN e a indicação de duas coordenadas aleatórias do Cartão Matriz, seguindo-se o envio de um “SMS” (“Short

Message Service") de confirmação, para o telemóvel associado à conta, o número do telemóvel da Autora, à data, o n.º .....14, com a indicação de um código único para a concreta operação visada, a introduzir na plataforma para finalizar a operação;

11. A Autora encontra-se registada como titular de um cartão telefónico móvel da aqui 2.ª Ré, com o n.º .....14, pelo menos desde 1995, constando do aludido registo o seu nome completo, o número de identificação fiscal e morada.

12. Em 11/03/2019, pelas 10h, a Autora recebeu um "SMS" ("Short Message Service"), no seu telemóvel (.....14), remetido alegadamente pelo Réu Banco, referindo que o seu acesso à NET24 se encontrava inativo e que teria de aceder ao site do Banco ali mencionado, com designação MONTEPIO e com hiperligação direta e alterar o seu Código PIN de modo a voltar a ter acesso à NET24 e ao cartão matriz.

13. Em data anterior àquela e pelo menos por duas vezes, a Autora já havia sido contactada pelo Réu Banco no sentido de reativar o seu acesso ao homebanking, por não ter aquela logrado utilizá-lo por longo período,

14. Pelo que, não estranhou a receção do referido "SMS" ("Short Message Service").

15. A Autora clicou na referida hiperligação e acedeu ao referido site graficamente igual ao que sempre conheceu como sendo do Banco Réu.

16. Verificou que o seu acesso ao serviço de Homebanking estava inativo.

17. Pelo que, acreditando na veracidade da mensagem escrita recebida, a Autora seguiu os passos ali referidos para reativar o referido acesso, designadamente, introduzindo o seu número de cliente e Código PIN.

18. Após ter concretizado todos os passos ali solicitados, a Autora verificou que já conseguia ter novamente acesso à plataforma, onde verificou o seu saldo e movimentos.

19. Em 12/03/2019, por volta das 14h50 min, a Autora verificou que o seu telemóvel estava sem rede.

20. Como se encontrava no seu local de trabalho, a Autora contactou a sua filha, ainda menor, pela aplicação whatsapp e pediu-lhe que avisasse o irmão que, em caso de necessidade, a deveriam contactar para o telefone fixo do trabalho.

21. Nesse mesmo dia, pelas 17h30 min., quando saiu do seu local de trabalho, a Autora deslocou-se à loja da 2.ª Ré, em ..., para ver o que

se passava com o cartão.

22. Após o manuseamento do telemóvel e a constatação de ausência de rede, a funcionária da 2.ª Ré, CC, referiu tratar-se de uma anomalia do cartão.

23. Aconselhando a Autora a adquirir uma 2ª via do cartão, de modo a resolver o problema.

24. A Autora adquiriu de imediato, na referida loja, uma 2.ª via do cartão,

25. Tendo apresentado o seu cartão de cidadão.

26. Assinado a fatura n.º GT163/....17, de 12/03/2019,

27. E liquidado a quantia de € 7,50 (sete euros e cinquenta cêntimos).

28. Cerca de dez minutos depois de substituir o cartão, a Autora já tinha rede no telemóvel.

29. Em 14/03/2019, pelas 9h15 min., o Autor recebeu um contacto telefónico efetuado pelos serviços do Réu Banco,

30. Questionando-o, no sentido de conhecer se este, em 12/03/2019, havia realizado movimentos a débito na identificada conta bancária, através do serviço de "homebanking".

31. O Autor respondeu, de imediato, negativamente.

32. Perante tal resposta, a funcionária do Banco Réu solicitou a presença de um dos Autores, no balcão do ....

33. A Autora saiu do seu local de trabalho e dirigiu-se ao referido balcão.

34. Ali chegada, foi informada que no referido dia 12/03/2019, haviam sido realizados, no espaço de 20 (vinte) minutos, 20 (vinte) transações bancárias de pagamento de serviços.

35. Cada uma no valor de € 1.939,20 (mil, novecentos e trinta e nove euros e vinte cêntimos),

36. No total de € 38.784,00 (trinta e oito mil, setecentos e oitenta e quatro euros), conforme infra se discrimina:

- 12/03/2019, PAG SERV. ....70, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....62, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....49, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....47, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....43, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....39, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....35, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....32, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....77, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....27, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....24, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....18, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....64, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....63, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....62, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....60, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....57, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....56, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....06, no valor de € 1.939,20

- 12/03/2019, PAG SERV. ....04, no valor de € 1.939,20

37. Para se lograr concretizar as referidas 20 (vinte) transações bancárias, havia sido utilizado todo o valor à ordem àquela data, cerca de € 6.244,79 (seis mil, duzentos e quarenta e quatro euros e setenta e nove cêntimos)

38. Valor utilizado para a concretização dos 3 (três) primeiros pagamentos.

39. Tendo sido posteriormente transferido todo o valor, alocado na conta poupança dos Autores, a prazo, no total de € 60.065,88 (sessenta mil e sessenta e cinco euros e oitenta e oito cêntimos), para a conta à ordem, de onde foram realizados mais 17 (dezassete) pagamentos,

40. Ficando o saldo de apenas € 27.411,56 (vinte e sete mil, quatrocentos e onze euros e cinquenta e seis cêntimos).

41. Os Autores apresentaram de imediato queixa-crime, junto da esquadra da PSP da ...,

42. A que foi atribuído o número de processo 194/19.1... e a correr termos pela 7.ªSecção do DIAP de ....

43. Os Autores dirigiram-se, posteriormente, à loja da 2ª Ré, sita em ... e contaram o sucedido.

44. Tendo a funcionária constatado que, no dia 12/03/2019, tinham sido pedidas duas segundas vias de cartões associados ao número de telemóvel da Autora,

45. Uma segunda via do cartão, pelas 15h 32 min., no balcão do Retail Park ...,

46. Alegadamente a pedido do cliente,

47. Sem assinatura nem apresentação de cartão do cidadão ou qualquer outro documento,

48. Operação registada pela funcionária DD,

49. E a outra segunda via, pelas 17h 55min., pela Autora, naquela mesma loja de ....

50. Em 15/03/2019, pelas 11h 30 min. a Autora foi contactada telefonicamente pelo balcão do Réu Banco, que a informou que, no dia 13/03/2019 alguém tinha tentado fazer um carregamento de telemóvel, com um número desconhecido dos Autores, o qual foi negado.

51. Em 30/03/2019, a Autora recebeu nova "SMS" ("Short Message Service") do Montepio 24, com o mesmo teor, conforme Doc.n.º4 que se junta e dá por integralmente reproduzido e articulado para os devidos e legais efeitos.

52. Tendo telefonado de imediato para o balcão do Réu Banco.

53. E apresentado aditamento à queixa-crime apresentada junto da PSP, com cópia da referida comunicação escrita recebida.

54. Em 01/04/2019, pelas 10h15 min., a Autora recebeu nova "SMS" ("Short Message Service") do Montepio 24 a dizer que o seu PIN estava desativado, conforme Doc. n.º5 que se junta e dá por integralmente reproduzido e articulado para os devidos e legais efeitos.

55. Em 18/07/2019, a Autora recebeu nova "SMS" ("Short Message Service"), do Montepio 24, referindo que o seu telemóvel não estava registado no SMS CODE.

56. Tendo o utilizador e PIN sido descativados por razões de segurança.

57. E pedindo que acedesse ao site com igual hiperligação direta.

58. Tais movimentações a débito na conta bancária dos Autores não foram por estes autorizadas ou de algum modo consentidas.

59. As operações foram efetuadas através da utilização do número de cliente da Autora, código PIN e coordenadas aleatórias do seu cartão

matriz,

60. Validadas com código de autorização, enviado por "SMS" ("Short Message Service") para o telemóvel associado à conta, com o nº 14,

61. Por terceiros que lograram pedir e obter a segunda via do referido cartão junto da 2ªRé,

62. Sem apresentar qualquer elemento identificativo para o efeito.

63. Para proceder à solicitação de segunda via de cartão SIM, numa das lojas da 2.ª Ré, é necessário que o titular da respetiva conta se apresente com o seu documento de identificação, ou o PIN ou PUK do cartão.

64. É igualmente possível proceder a essa solicitação através de terceiro com procuração ou documento assinado pelo titular, devidamente reconhecido por um advogado ou solicitador.

65. As referidas regras foram criadas como garantia de segurança dos serviços e da rede da Operadora e de inviolabilidade das comunicações eletrónicas dos seus clientes.

66. A situação causou profunda revolta e desgosto aos Autores,

67. Tendo sido um elemento de conflito entre o casal, desde aí,

68. Que levou a diversas discussões no seio familiar,

69. A noites sem dormir por parte de ambos os Autores,

70. A profunda vergonha da Autora,

71. Que nunca mais logrou ter um sono reparador,

72. Que se sentiu enganada e diminuída perante os demais,

73. Tendo vergonha de contar a situação às suas Colegas e amigas,

74. O que levou a que esta se fechasse, isolasse e evitasse convívios familiares ou com amigos.

75. A Autora passou, ainda, a sentir extrema frustração e angústia,

76. O que trouxe maior dificuldade na gestão do seu dia-a-dia familiar e até profissional.

77. A situação levou a que os Autores tivessem que desistir dos planos familiares que já haviam traçado de realizarem uma viagem de sonho, os quatro em família e alterar os planos de estudo dos filhos, especialmente a mais velha, que ia entrar na faculdade.

78. A 2ª Ré devolveu à Autora o valor de 7,5 euros pago pela 2ª via do cartão.

79. Os AA. aderiram ao serviço de homebanking do Banco Montepio, designado por Net 24 em 15/06/2010,

80. Tendo aderido à solução "15 em 1 – SERVIÇO MÁXIMO" apenas em 14/12/2018.

81. O número de utilizador (a)) é um número de identificação atribuído e entregue no momento da adesão ao serviço.

82. A password (b)), composta por seis dígitos, constitui um código PIN multicanal, e é atribuída e entregue ao cliente presencialmente, no balcão, no momento da adesão (pelo que foi atribuída à A. em 15/06/2010).

83. Após o primeiro login, a password tem de ser obrigatoriamente alterada por uma da autoria e do exclusivo conhecimento do cliente, sem intervenção da R., pelo que não é possível determinar a respetiva data de alteração.

84. Permitem estas duas credenciais (a) e b) em conjunto) apenas a realização de operações e consultas que não comportem alterações de património.

85. Por sua vez, o cartão matriz (c)) é um cartão de coordenadas com 72 posições, cada uma com 3 dígitos, que nunca se repetem, para validação de operações passíveis de alterar o património detido pelos clientes, junto do Banco Montepio, aqui R..

86. O respetivo processo de produção é externo à R. e não envolve qualquer atuação humana, uma vez que as coordenadas são geradas por computador,

87. Sendo o cartão remetido via CTT para o endereço do cliente em estado de préactivo, e apenas é passível de ser ativado mediante a validação de códigos de acesso ao Net24 (número de utilizador e password) adstrito ao cartão expedido.

88. Contém o cartão matriz, na mesma face em que constam todas as 72 posições de 3 dígitos cada, a seguinte advertência: "ATENÇÃO: Nunca indique mais do que 2 dígitos deste Cartão Matriz",

89. E apenas o legítimo possuidor do cartão matriz consegue validar uma operação passível de alterar o património, uma vez que é o único que conhece todas as coordenadas.

90. Por fim, o sistema SMS CODE consiste em associar o número de telemóvel do cliente ao homebanking por forma a que, no momento de realizar uma operação de que resultem alterações patrimoniais, o sistema envie um código via SMS para o seu telemóvel.

91. Assim, para a realização de uma operação com alterações patrimoniais, o utilizador teria de efetuar o login na página da internet

da R., identificar o respetivo número de utilizador, colocar a sua password, selecionar e ordenar a operação, inserir duas coordenadas aleatórias do seu cartão matriz e recorrer ao seu telemóvel para obter o código, aleatório e associado apenas àquela operação em concreto, entretanto remetido.

92. A Autora emitiu e subscreveu uma declaração manuscrita, datada de 14/03/2019, que enviou ao Réu Montepio, com o seguinte teor: "(…) no dia 11/3/2019, por volta das 10h recebi um sms no meu telemóvel (.....14) vindo do montepio (tudo levava a crer ser verdadeiro), em como o meu acesso ao net24 estava inativo e que teria de aceder ao site e dar um novo código e o acesso ao cartão matriz. Verifiquei que de facto não conseguia aceder ao net24, por isso achei credível o sms, e segui os passos, que foram apenas dar o meu código e foto do cartão matriz para o acesso ficar ativo (…)".

93. Sempre que se efetua um acesso ao sítio da R., na mesma página onde insere o código PIN, encontra-se destacada e em formato de fácil leitura e apreensão, informação diversa e bastante explícita sobre medidas de segurança por aquela adotadas, e medidas de segurança/ precauções que deverão ser tomadas pelos utilizadores, contendo inúmeros alertas de segurança com exemplos de tentativas de fraude sobre os diferentes métodos de captação maliciosa de credenciais, perpetrada por piratas informáticos. (cfr. Documento n.º 3, que se junta e aqui se dá por integralmente reproduzido para todos os efeitos legais)

94. Igualmente no sítio da R. se emite um Aviso de Segurança, com as referidas mensagens,

95. Bem como são apresentados exemplos de páginas fraudulentas e de e-mail e SMS de Phishing, por forma a alertar os utilizadores para eventuais fraudes, onde designadamente consta, entre muitos outros alertas: Cuidados com mensagens de correio eletrónico, SMS e outras formas de contacto:

- Suspeite de qualquer e-mail, chamada telefónica ou SMS, que peça uma "ação imediata" ou crie um sentido de urgência ou risco grave. Em caso de dúvida contacte o seu banco

- Suspeite de e-mails supostamente do seu Banco, mas que inicia o seu texto com cumprimentos como "Querido Cliente" ou qualquer outra saudação diferente das que o seu banco habitualmente utiliza nas suas comunicações

- Suspeite dos erros gramaticais ou de escrita nas mensagens que recebe através de qualquer canal habitual de comunicação

- Posicione o cursor do rato sobre links de mensagens de email suspeitas. Isso mostrará o verdadeiro endereço para onde será direcionado se o selecionar. Se o destino do link for diferente do

escrito na mensagem ou contenha um nome ou código de país diferente da entidade emissora, pode ser uma indicação de fraude

- Não clique nos links de mensagens ou SMS s suspeitos.

96. O estado "inativo" refere-se ao estado do canal resultante da decisão do Cliente de não pretender utilizar o canal, na medida em que, com exceção do Phone24, o Cliente pode ativar ou inativar os restantes canais sempre que pretender. A gestão deste estado é efetuada pelo Cliente no primeiro acesso ao Montepio24 ou, a qualquer momento, através do Net24 – Menu Gestão Multicanal e do Serviço Phone24.

97. O estado "revogado" de acesso ao Serviço M24 resulta de três inserções incorretas de códigos de acesso (pin / cartão matriz) ou decorrido 1 ano desde a data de ativação / último acesso, estando o processo de reativação disponível mediante contacto com o Phone24 (entretanto é possível a atribuição de novo pin mediante o processo de atualização de dados online).

98. Poderão ser enviadas mensagens a alertar para a necessidade de alteração de pin por questões de segurança, bem como para a adoção de boas práticas que, em conjunto, garantam condições de segurança na internet, como a enviada à A. em 27/04/2020.

99. Os movimentos indicados, apenas foram possíveis porque, em cada um deles e sem erros:

a) Foi introduzido o número de utilizador;

b) Foi introduzida a password / PIN – importando referir que a sua introdução se faz em teclado virtual, escolhido de forma aleatória, aparecendo os números sempre em local distinto, não permitindo a identificação do código, criado pelo cliente (cfr. Documento n.º 3);

c) Foram introduzidas duas coordenadas do cartão matriz, que são sempre solicitadas de forma aleatória, pelo sistema e nunca repetidas.

d) Foi introduzido o código único enviado para o telemóvel associado ao serviço, com 6 dígitos, gerado de forma aleatória e para a operação em concreto que, no momento, o utilizador se encontra a processar.

100. Para que os clientes da R. possam usar o serviço de homebanking é necessário, além do processo de contratação do serviço, que o utilizador associe o seu número de telemóvel, mediante a confirmação da identidade do cliente e a inserção de um código de 6 dígitos enviado para o telemóvel declarado, para efeitos de ativação do serviço.

101. Prevê o clausulado da Proposta de Adesão ao Serviço Montepio24, rubricado e subscrito pela Cliente aqui A. em 2015-05-04:

• Alínea b) do ponto 1 - Credenciais de Autenticação – Elementos ou formas de identificação e/ou assinatura, de carácter pessoal e intransmissível disponibilizados pelo Montepio no âmbito do Serviço Montepio24.

• Ponto 4.2. O Cliente compromete-se igualmente, a guardar sob segredo as suas Credenciais de Autenticação (…)

• Ponto 5.3. A responsabilidade do Cliente por todas as operações irregulares efetuadas utilizando as Credenciais de Autenticação, ou através da utilização abusiva das mesmas, motivadas por perda, extravio, roubo, falsificação, cessa no momento em que seja efetuada a comunicação acima referida, salvo se forem devidas a dolo e/ou negligência grosseira do Cliente".

102. Os computadores da R. não foram alvo de qualquer quebra de segurança informática, não tendo o sítio institucional do Montepio sido alvo de intrusão, ou qualquer outra violação.

… …

O objeto do recurso é delimitado pelas conclusões da Recorrente, não podendo este Tribunal conhecer de matérias nelas não incluídas, a não ser que sejam de conhecimento oficioso, conforme prevenido nos arts. 635º n.º 4 e 639º n.º 1, ex vi, art.º 679º, todos do Código de Processo Civil.

O conhecimento das questões a resolver na presente Revista consiste em saber se o comportamento da autora configura (ou não) uma negligência grosseira que afaste a responsabilidade pelo risco da recorrente, relativamente às perdas sofridas pelos recorridos com transações bancárias de pagamento de serviços, por terceiros não autorizados, através do serviço *homebanking* a que tais terceiros acederam fraudulentamente.

… …

Como delimitação elementar, na ação os autores pretendem obter das rés os valores que lhes forma retirados da sua conta bancária e o correspondente a todos os incómodos e sofrimento que dizem terem sofrido.

Quanto à responsabilidade NOS – Comunicações S.A. foi decidida a improcedência dos pedidos contra ela deduzidos e a decisão recorrida manteve essa absolvição pelos mesmos fundamentos sem que quanto a esta matéria tivesse havido qualquer voto de vencido. Tal situação determina que, quanto a esse segmento da decisão referente à absolvição do pedido da ré NOS – Comunicações SA, nada há que conhecer ou decidir uma vez que a recorrente Montepio, não interpôs recurso de revista excecional quanto a este segmento, limitando-se a arrogar que se a decisão proferida contra si não fosse admitida como

revista normal teria de o ser como revista excecional – não envolvendo nesta excecionalidade a decisão de improcedência do pedido contra a ré Nos – Comunicações SA.

Apreciando o objeto do recurso e que se limita à verificação da responsabilidade da recorrente observamos que a única questão suscitada é a de saber se a recorrida BB agiu com negligência grosseira que afaste a responsabilidade da ré Montepio.

A recorrente acolhe sem oposição o que a sentença e a decisão recorrida elaboram quanto ao quadro normativo em que se inscrevem os factos apurados. Que entre Autores e ela se estabeleceu uma relação contratual por via da abertura das contas bancárias mencionadas e adesão da Autora ao sistema de homebanking disponibilizado por aquele Réu e designado por "Net24", configurando esse negócio um contrato de depósito pelo qual uma das partes entrega à outra uma coisa, móvel ou imóvel, para que a guarde e restitua quando for exigida. E dizendo-se irregular o depósito que tem por objeto coisas fungíveis sendo-lhe aplicáveis com as devidas adaptações, as normas relativas ao contrato de mútuo – arts. 1205 e 1206 do CCivil -, o depósito bancário replica aqueles termos definidores tendo por objeto a entrega de dinheiro que origina a abertura de uma conta onde se vão registando as entregas feitas pelo cliente, ao abrigo do contrato inicialmente celebrado, bem como de todos os levantamentos das quantias nele depositadas.

No travejamento jurídico que preside a esta atividade desencadeada pelo contrato de deposito bancário o art. 407 do C. Comercial estabelece que "os depósitos feitos em bancos se regem pelos respetivos estatutos no que não estiver prevenido nas normas legais aplicáveis"; o art. 363 disciplina que "as operações de banco regular-se-ão pelas disposições especiais respetivas aos contratos que representarem ou em que afinal se resolverem." E o art. 1144 do CCivil que "As coisas mutuadas tornam-se propriedade do mutuário pelo facto da entrega". E no domínio da responsabilidade o art. 796 nº 1 do CCivil dispõe que " Nos contratos que importem a transferência do domínio sobre certa coisa ou que constituam ou transfiram um direito real sobre ela, o perecimento ou deterioração da coisa por causa não imputável ao alienante corre por conta do adquirente".

É esta a enunciação que as instâncias realizaram, sem que a recorrente se lhe oponha, concluindo que o Banco é o responsável pela guarda dos valores que lhe foram confiados pelo cliente e está obrigado à sua restituição com os seus frutos (art. 1142 e 1187 al c) do CC), correndo por conta dele, Banco, o risco relativo à subtração do dinheiro que lhe foi entregue pelos depositantes.

Acompanhando ainda o itinerário percorrido pela decisão recorrida, estando demonstrado que foram subtraídas quantias das contas bancárias dos Autores, através de operações efetuadas

fraudulentamente por terceiros com utilização do serviço de *homebanking* disponibilizado pelo Banco Réu, é com incidência no modo concreto como ocorreu essa subtração que deverá formar-se o juízo de responsabilidade ou irresponsabilidade da recorrente.

Conforme se refere no ac. do STJ de 18-12-2013 no proc. 6479/09.8TBBRG.G1.S1 que se tornou objeto de comentário e citação em todos os casos em que a matéria tem sido debatida: *"O progresso tecnológico dos últimos anos, veio revolucionar todo o comércio jurídico, nomeadamente a nível das relações bancárias, pois começamos com a emissão de cartões, de crédito e de débito, sendo que com estes se podem realizar uma infinidade de operações utilizando-se para o efeito os terminais de caixa automática, vulgo ATM e podemos agora, através dos sistemas de homebanking, aceder a uma variedade de operações bancárias, on line, utilizando para o efeito um computador pessoal.*

Para o efeito os bancos fornecem aos seus clientes senhas de acesso pessoais, bem como cartões matriz constituídos por uma infinidade de composições numéricas, que normalmente são solicitadas no final de cada operação efetuada por meios telemáticos e por forma a autenticá-la, já que esse cartão matriz deverá apenas ser do conhecimento do cliente, único a poder utiliza-lo, não lhe sendo permitido fornecer nenhum dos dados nele insertos a terceiros, uma vez que, quer o protocolo da página bancária, quer o tráfego de toda a informação nela processada, o que inclui as sobreditas senhas de acesso, são encriptadas, tornando quase impossível um terceiro obter ou alterar a informação depois de enviada.". E, acrescentamos nós, esse progresso tecnológico, conforme os tempos o revelaram, revelou-se em simultâneo produtor de maior comodidade para os clientes uma vez que passaram a poder realizar as suas operações sem terem de se deslocar às agências bancárias, mas também, e até essencialmente, revelou-se favorável às instituições bancárias que puderam reduzir (significativamente) os seus custos de atendimento quer com instalações quer com pessoal. A implementação e expansão destes meios eletrónicos, numa consideração geral considerados como fiáveis, reclama constantemente mecanismos de segurança por as plataformas onde se situam estarem sujeitas a ataques tendo por finalidade o acesso à conta bancária do cliente, contra a vontade deste, para realizar a subtração dos fundos que nela se encontrem.

O *homebanking* como um serviço prestado pelo Banco através do qual dá ao cliente a possibilidade de efetuar operações bancárias via Internet, nomeadamente, consultas, pagamentos, subscrição de produtos financeiros e transferências impõe que o banco assegure, em todas as atividades que exerce, elevados níveis de competência técnica, garantindo que a sua organização empresarial funcione com os meios humanos e materiais adequados a assegurar condições apropriadas de qualidade e eficiência (art. 73º do RGICSF aprovado

pelo DL 298/92 de 31/12, na redação do texto consolidado publicado em anexo ao DL 126/2008 de 21/7). Assim, sendo o *homebanking* um serviço prestado ao cliente pelo Banco, é este que tem de diligenciar para que seja seguro e nele possa o cliente confiar ou , como se refere no acórdão citado "*os riscos pela utilização normal do sistema correm por conta do prestador de serviços, isto é, sobre o Banco, o que não deixa de ser uma obrigação perfeitamente normal já que é o Banco que vai retirar os maiores benefícios económicos do seu bom funcionamento*. Por seu lado, o cliente deverá utilizar esse serviço seguindo as regras de segurança que lhe tenham sido comunicadas pelo Banco e aquelas que, segundo um padrão de normalidade, o comum utilizador da Internet sabe que devem ser observadas, nomeadamente, a não divulgação dos códigos de acesso. Com efeito, com a proliferação deste tipo de contratos surgiu a necessidade de regulamentar tal atividade, o que, entre nós, se consagrou através do DL 317/2009, de 30 de outubro (transpondo Diretiva Comunitária), diploma que foi revogado e substituído pelo DL 91/2018, de 12/11, de acordo com o qual se estipulam obrigações quer para o utilizador dos serviços de pagamento quer para o seu prestador. Com importância para o utilizador, este deve observar a obrigação de utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização; comunicar, atempadamente, a perda, roubo ou apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento, impondo-se-lhe que tome todas as medidas razoáveis, para preservar a eficácia dos dispositivos de segurança personalizados do instrumento de pagamento.

Conforme dispunha o art. 68 daquele primeiro diploma que corresponde ao agora estatuído no art. 111 do DL 91/218, 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 previstas no art. 113 nº3 que sob epígrafe *Prova de autenticação e execução da operação de pagamento* dispõe que *"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."* acrescentando o nº 4 que *"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."

Quanto à responsabilidade decorrente de operações de pagamento não autorizadas - nos termos que se encontravam disciplinados nos arts. 71 e 72 do anterior diploma e agora encontram consagração nos arts. 114 e 115 do DL 91/218 – ela é de imputar ao prestador do serviço se vier a comprovar-se que a mesma não foi autorizada e não se verificar o incumprimento de nenhuma das obrigações que são impostas ao utilizador em caso de perda, roubo, apropriação abusiva de instrumento de pagamento ou quebra da confidencialidade dos dispositivos de segurança personalizados, respetivamente.

No caso em decisão está demonstrado que o Banco recorrente comunicou à Autora, quer através do documento de adesão ao sistema de homebanking, quer na própria página de acesso facultada através da internet as regras de utilização e os cuidados a ter para a utilização do homebanking, tendo-se ainda provado, os procedimentos que a Autora teria de seguir para efetuar as operações de transferências e de pagamentos. Porém, o acesso à conta bancária da Autora foi realizado por terceiros, cuja identidade não foi apurada, os quais, através do sistema informático e da utilização de dados pertencentes apenas à Autora, sem autorização desta, lograram retirar da mesma a quantia de 38.784,00 euros.

Do que ficou apurado o processo de acesso por terceiros à conta da autora foi realizado numa sequência de atos que se iniciaram com uma "sms" recebida no telemóvel desta como enviada pelo banco réu referindo que o acesso à NET24 se encontrava inativo e que teria de aceder ao site do Banco ali mencionado com hiperligação direta e alterar o seu Código PIN de modo a voltar a ter acesso à NET24 e ao cartão matriz. Através da hiperligação fornecida na "sms" a autora acedeu a um site graficamente igual ao que sempre conheceu como sendo do Banco Réu e verificou nele que o seu acesso ao serviço de homebanking estava inativo. E foi na convicção de estar a reativar o acesso perdido que a autora seguiu os passos ali referidos, introduzindo o seu número de cliente e Código PIN.

Estes factos ocorreram em 11/03/2019 e após ter concretizado todos os passos ali solicitados, a autora verificou que conseguia ter novamente acesso à plataforma, onde verificou o seu saldo e movimentos.

No dia seguinte, isto é, em 12/03/2019, por volta das 14h50 h, a autora verificou que o seu telemóvel estava sem rede e tendo obtido junto da operadora a informação de que se tratava de uma anomalia do cartão adquiriu uma 2ª via do mesmo passando de novo a ter rede. Nesta sequência cronológica, no dia 14/03/2019 a autora recebeu a informação do banco no sentido de terem sido realizados no dia 12/3/2019 através do serviço de "homebanking", no espaço de 20 (vinte) minutos, 20 (vinte) transações bancárias de pagamento de

serviços cada uma no valor de € 1.939,20 (mil, novecentos e trinta e nove euros e vinte cêntimos).

Sabendo-se que as operações foram efetuadas através da utilização do número de cliente da Autora, código PIN e coordenadas aleatórias do seu cartão matriz e validadas com código de autorização, enviado por "SMS" ("Short Message Service") para o telemóvel associado à conta é possível configurar o procedimento de terceiros em dois momentos diferentes. O primeiro no dia 1/3/2019 em que obtêm através do logro em que fazem cair a autora o número de cliente e o código PIN de acesso ao homebanking e, um segundo, no dia 12 /3/2019 em que obtiveram uma segunda via do cartão de telemóvel da autora.

Sendo estes os factos relevantes no que respeita ao procedimento dos terceiros, devem tomar-se em consideração aqueles outros em que se revela que a autora raramente utilizou o serviço de homebanking e todas as utilizações foram para consulta do saldo da conta à ordem; em data anterior a 11/3/2019 pelo menos por duas vezes, já havia sido contactada pelo Réu Banco no sentido de reativar o seu acesso ao homebanking, por não ter aquela logrado utilizá-lo por longo período.

Por outro lado, importa que ficou provada atender a que no número 92 dos provados consta que "a autora emitiu e subscreveu uma declaração manuscrita, datada de 14/03/2019, que enviou ao Réu Montepio, com o seguinte teor: "(…) no dia 11/3/2019, por volta das 10h recebi um sms no meu telemóvel (.....14) vindo do montepio (tudo levava a crer ser verdadeiro), em como o meu acesso ao net24 estava inativo e que teria de aceder ao site e dar um novo código e o acesso ao cartão matriz. Verifiquei que de facto não conseguia aceder ao net24, por isso achei credível o sms, e segui os passos, que foram apenas dar o meu código e foto do cartão matriz para o acesso ficar ativo (…)". Em vez de se julgar provado que quando a autora acedeu ao site através da hiperligação que constava da "sms", para lá do número de utilizador e do PIN, forneceu também os números do seu cartão matriz, fez-se apenas constar que se julgava provado que a autora emitiu de uma declaração por si assinada e dirigida ao banco réu na qual constava a confirmação de ter facultado os números do seu cartão matriz. No entanto, a forma como se expressa este elemento não impede que se tenha por confessado pela autora que facultou os números do cartão matriz - vd. arts. 355 nº1 e 4 e 358 nº2 do CCivil.

É com o enquadramento normativo e fáctico acabado de expor que deve afrontar-se a questão a decidir e que se traduz em saber se o comportamento da autora configura uma negligência grosseira ou grave uma vez que, como dizemos anteriormente, só esta retira à recorrente a responsabilidade de repor as quantias subtraídas.

As instâncias foram concordantes em entender que o padrão de uma negligência grave/grosseira não se verificava e, em oposição, a

recorrente blasonando de fundado no voto de vencido da decisão recorrida sustenta que o caso em presença é paradigmático desse tipo de negligência, uma vez que foi a autora quem forneceu todos os elementos pessoais e de segurança que habilitaram terceiros a aceder à sua conta e a retirar dela os fundos.

No acórdão do STJ citado entendeu-se que *com a prova aí obtida* não tinha havido do lesado *"qualquer comportamento indiciador de quebra de segurança no acesso ao site (...) que tivesse proporcionado a um terceiro as coordenadas para a realização das operações bancárias via homebanking."* E considerou-se, em explicação, que havia ocorrido que o lesado havia entrado *"no que pensou ser a página do Réu para efetuar as suas operações, foram-lhe pedidas coordenadas, ao que aquela acedeu, sem se dar conta que estava afinal numa página «clonada»"*

No confronto das duas modalidades mais frequentes de obtenção doe elementos pessoais de acesso ao homebanking e utilização da conta a partir dessa plataforma o "*phishing*" pressupõe a tentativa de adquirir aqueles dados através do envio de e-mails com uma pretensa proveniência da entidade bancária do recetor, por exemplo, a pedir determinados elementos confidenciais (número de conta, número de contrato, número de cartão de contribuinte ou qualquer outra informação pessoal), por forma a que este, ao abri-los e ao fornecer as informações solicitadas e/ou ao clicar em links para outras páginas ou imagens, ou ao descarregar eventuais arquivos ali contidos, poderá estar a proporcionar o furto de informações bancárias e a sua utilização subsequente". Por sua vez o "*pharming"* consiste em suplantar o sistema de resolução dos nomes de domínio para conduzir o usuário a uma pagina Web falsa, clonada da página real, baseando-se o processo, sumariamente, 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, que leva o usuário a pensar que está a aceder a um determinado site – por exemplo o do seu banco – e está a entrar no IP de uma página Web falsa, sendo que ao indicar as suas chaves de acesso, estas serão depois utilizadas pelos hackers, para acederem à verdadeira página da instituição bancária e aí poderem efetuar as operações que entenderem.

Foi depois de se ter entendido que o caso que conhecia tratava de uma modalidade de *pharming* que no acórdão do STJ citado se decidiu a inexistência de negligência grave porque, afinal, os elementos pessoais estavam a ser facultados na convicção de se estar no site do Banco por se ter acedido a ele para realizar uma utilização, da forma que é usual tendo sido no decurso dessa utilização que tinha ocorrido um desvio, concluindo-se que os elementos efetivamente fornecidos não o tinham sido "voluntariamente" – entendimento que se repete em alguns outros casos como o contante do ac. RL de

29-9-2022 no proc. 15455 /20. 9T8LSB.L1-6 que segue o do STJ citado.

Em análise, não cremos que a negligência grosseira correspondente à falta grave e indesculpável, consistente na omissão dos deveres a que se está adstrito que só uma pessoa especialmente desleixada, descuidada e incauta deixaria de observar, só possa estar associada aos casos em que o procedimento se configure como *pharming*, acolhendo antes como critério definidor o de verificar se o lesado forneceu ou não as credenciais de segurança a terceiros voluntariamente. E será (só) na apreciação da voluntariedade do comportamento da autora quando confrontada com o padrão do homem médio nas condições concretas do caso que poderemos determinar se existiu negligência grosseira.

Quer nas situações de *pharming* quer nas de *phishing* ou, pelo menos, quer nas situações descritas na jurisprudência citada quer no caso dos autos, o lesado quando fornece os elementos pessoais de segurança encontra-se num site que pela sua configuração gráfica lhe fornece a convicção de se estar no site do Banco. E não nos parece decisivo, na análise da negligência, que a circunstância de se ter acedido a esse site (que não é o do Banco mas parece ser) porque foram digitados os números da conta de utilizador e do pin (e posteriormente os do cartão matriz para realizar operações) ou se venha a aceder a ele porque se recebeu uma "sms" com a identificação do banco a alertar para uma situação que importa resolver no aceso ao homebanking, seja estruturalmente diferente. Em ambos os casos é quando se está no site que tem toda a configuração do domínio do Banco que se realizam as operações através das quais são fornecidos os elementos.

Rememorando, a autora que raramente utilizou o serviço homebanking e apenas o fez para consulta do saldo da conta à ordem e para nenhuma outra finalidade, na sequência de ter sido anteriormente contactada por duas vezes pelo banco réu no sentido de reativar o seu acesso ao homebanking, por não ter utilizado por longo período, recebe no seu telemóvel uma "sms" identificada como sendo daquele banco referindo que o acesso se encontrava inativo e que teria de aceder ao site do Banco constante de uma hiperligação direta e alterar o seu Código PIN de modo a voltar a ter acesso ao serviço e ao cartão matriz.

Esta cronologia faz concluir que quando a "sms" é recebida pela autora, esta comunicação insere-se numa repetição de advertências anteriores do banco advertindo para uma mesma situação, o homebanking encontra-se inativo e ser necessário reativá-lo. É com base na credibilidade decorrente da insistência anterior e desta decorrer urgência em resolver um mesmo problema (o da ativação do homebanking) que a autora acede de imediato ao site que julga ser do Banco através da hiperligação fornecida na mensagem, obtendo no

decurso dessa utilização a confirmação de que o seu serviço (que estava inativo) tinha sido restabelecido. Tudo isto ocorre em 11/3/2019 e, pelos restantes factos apurados, verificamos que esta situação, através da qual os elementos pessoais de segurança da autora passam a estar em poder de terceiros, não permite ainda a realização de operações, designadamente transferências e pagamentos, porque para estas seria necessário o acesso ao telemóvel da autora no qual, em caso dessas operações, receberia do banco o "SMS Code" como quarto nível de segurança. Esta a razão porque, tendo a obtenção dos elementos pessoais de segurança sido obtida por terceiros em 11/3/2019, não é nesse dia que as operações de movimentação da conta se realizam, mas sim e apenas no dia seguinte, em 12/3/2019, quando esses mesmos terceiros conseguem ter em seu poder, através de segunda via, o cartão telefónico do telemóvel da autora. Aparentemente sem qualquer relação entre si, a sms recebida pela autora no dia 11/3/2019 e a verificação do seu telemóvel se encontrar sem rede, apenas ocorrida no dia seguinte, vem a ter explicação quando se apura que esses terceiros apenas conseguem obter (duas) segundas vias do cartão da autora nesse dia 12/03/2019.

A complexidade dos procedimentos descritos na obtenção de todos os elementos que habilitassem à realização dos movimentos através do homebanking e a maneira como eles se distribuem no tempo (em dois dias diferentes) é relevante para concluir que o comportamento da autora naquela circunstância concreta podendo ser considerado como menos prognóstico ou diligente, num sentido em que seria possível atribuir-lhe uma omissão de previsão, suspeita e cuidado objetivamente esperados ou, sobretudo, uma ação equivocada por falta de mais completo discernimento técnico, entendemos que não pode ser configurado como negligência groseira que tem na base e fundamento o poder ser o comportamento da autora reprovado pelo mais elementar senso comum. Que assim é resulta, desde logo, de ter sido precisamente um sentido de dever, imbricado em advertência anterior do banco (de que o homebanking estava inativo) que motivou a autora a aceder ao site fornecido na "sms" para resolver um problema que concretamente existia. Tratando-se ou não de uma coincidência a situação da "sms" recebida reportar à mesma advertência do banco, a verdade é que existe um contexto que isenta de *grosseria* o comportamento da recorrida, comportamento que ela estava convencida de ser diligente. Por outro aspeto, a qualificação da negligência extrai-se da análise do comportamento, não do resultado, não se opondo tampouco à ausência de culpa do banco recorrente. A simples verificação de os elementos de segurança necessários ao acesso ao serviço de homebanking terem sido fornecidos a terceiros pela autora não autoriza a configurar a negligência como grave, quando não teríamos de concluir que todos os acessos a esses serviços só podem ocorrer (mesmo na situação de *pharming*) se for o

detentor desses dados a fornecê-los. A diferença está em que esse fornecimento só adquire censurabilidade que isenta a regra da responsabilidade do banco, se se revestir de características, de um modo e de uma voluntariedade que coloque o fornecedor num registo flagrante de gravidade e reprovação por deliberada e avulsa desconsideração dos deveres a que estava obrigado.

Tendo facultado os elementos que facultou, só porque estava convicta de que os estava a revelar para acesso ao próprio banco recorrente, não se afigura que tal atitude possa ser qualificada como negligência grave, concluindo-se que nas circunstâncias do caso, qualquer pessoa, medianamente sagaz e cuidadosa, poderia ser induzida em erro e ser levada a ter exatamente o mesmo comportamento. A situação concreta que a sms recebida a convocava a resolver havia sido advertida pelo banco; a diligência de ativação do serviço por parte da autora não a iria conduzir a qualquer operação ativa de movimento da conta (da sua parte) e muito menos poderia prever que o seu comportamento autorizasse a utilização por terceiros porque, do que realizava, em sentido objetivo tal utilização só poderia ocorrer se tivesse sido fornecido o seu próprio cartão de telemóvel através do qual se acionava o "SMS CODE" e isso ela nunca admitiu que viesse a fazer ou que viesse a ocorrer. Nunca em momento algum se apercebeu que tivesse permitido o acesso ao seu telemóvel e, em verdade, o modo como esse acesso foi realizado não se encontra explicado, sabendo-se apenas que depois de ter acedido à hiperligação constante da sms a autora, no dia seguinte, ficou sem rede no telemóvel e segundo instruções da operadora, para solucionar o problema, obteve uma segunda via do cartão sendo que nesse mesmo dia *os terceiros* obtiveram igualmente duas segundas vias do mesmo cartão.

Julgamos que pela própria natureza das coisas, quem usa as credenciais de segurança na convicção de que está a fazer para realizar uma operação de reativação do serviço inativo, não o faz por descuido ou falta de cautela ou de senso tão elementares que afastem o risco do Banco e, a si e só a si possa ser imputada a responsabilidade de os dados terem passado para as mãos de terceiros. Tais práticas fraudulentas e em concreto a realizada ocorrem porque o seu grau de credibilidade e sofisticação conseguem atingir um grande número de pessoas minimamente avisadas e diligentes e não apenas as extremamente descuidadas ou incautas, que configuram as que têm uma total e gritante falta de atenção perante circunstâncias em que seria evidente em termos de senso comum, um outro comportamento - veja-se neste mesmo sentido e com esta formulação o acórdão de 14-12-2016 no proc. 1063/12.1TVLSB.L1.S1

Este entendimento afasta-se, portanto, daquele que identifica automaticamente a negligência grosseira com a demonstração de os

elementos pessoais de segurança terem saído do utilizador para o domínio de terceiros por atividade realizada por aquele (acesso a um site ou a uma hiperligação). Aliás, no caso dos autos a alusão a que a autora teria omitido (na petição inicial) o fornecimento dos dados do cartão matriz, quando a própria autora na comunicação que realizou ao banco refere expressamente os elementos que forneceu e que como assim foram julgados como provados, não releva para a apreciação da gravidade da negligência que reporta ao momento em que os dados pessoais foram fornecidos e não à comunicação que posteriormente é feita ao banco. Da mesma forma, não é admissível a ponderação de qualquer referência à profissão da autora que eventualmente tenha sido mencionada na audiência de julgamento e não tenha ficado a constar dos factos provados, como a recorrente alude aproveitando neste particular o que se escreve no voto de vencido. Ter ficado provado que os computadores do Banco não foram alvo de qualquer quebra de segurança informática, não tendo sido o seu sítio institucional alvo de intrusão ou qualquer outra violação e que no clausulado da Proposta de Adesão ao Serviço Montepio24 constavam todas as condições de utilização do mesmo, não isenta da responsabilidade o banco recorrente porque esta responsabilidade não resulta da verificação de qualquer culpa sua, mas sim de um comportamento da recorrida que pudesse ser julgado fraudulento ou grosseiro. O risco que corre por conta do recorrente, tendo por fundamento o art. 796 nº1 do CCivil apenas poderia ser afastado se tivesse ficado demonstrada a culpa da autora e neste caso, *culpa da autora* teria de corresponder a *culpa grosseira* por, nos termos da Diretiva transporta, a isenção de responsabilidade do banco apenas ocorrer em caso atuação fraudulenta ou negligência grosseira.

Em resumo, de acordo com o que decidiram as instâncias, confirma-se que a "atuação da Autora é alheia relativamente a todos os elos do modus operandi que permitiu a retirada de fundos das suas contas bancárias, ficando afastada a (sua) negligência grave a saída de fundos, concretizada por terceiros, sendo externa ao sistema concreto disponibilizado pela ré, advém igualmente na utilização de SMS e código gerado, e quanto a este não há dúvidas que tal acesso não foi proporcionado pelo fornecimento indevido de dados do cartão matriz" sendo que a entrega de cópia deste não configura igual negligência grave, quer pela forma como o serviço era utilizado pela mesma, quer pela ausência de prova da forma como a própria ré solicitava a reativação do serviço, resultando provado que a iniciativa desta era igual à ocorrida fraudulentamente."

Termos em que se deve negar provimento ao recurso.

… …

Síntese conclusiva

- As perdas resultantes de operações de pagamento não realizadas e

não autorizadas pelo utilizador/titular do serviço homebanking, mas por terceiros, nos termos do art. 796 nº1 do CCivil e do art. 115 do DL 91/2018 correm por conta do banco, exceto se forem devidas a atuação fraudulenta daquele ou a atuação grosseira do mesmo por incumprimento deliberado das obrigações que lhe estavam impostas, devendo o prestador do serviço demonstrar a existência de fraude, de dolo ou de negligência grosseira.

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

- A negligência grosseira, merecedora de reprovação pelo mais elementar senso comum por configurar uma falta indesculpável na omissão dos deveres a que se está obrigado, não se verifica quando a lesada, com a atenção que lhe era exigida e de que era capaz nas circunstâncias do caso, não se pôde opor aos artifícios de complexidade eletrónica que lhe foram colocados por terceiros que se fizeram passar com aparente credibilidade pelos serviços do banco, solicitando a resolução de um problema que efetivamente, em momento anterior e por duas vezes, o banco informara dever ser resolvido.

- Tal negligência grosseira é de afastar se o acesso ao link, que foi fornecido na “sms” e que se apresentava como enviada pelo banco, com os elementos aí fornecidos pela lesada, não permitia, só por si, qualquer operação de movimento da conta, que careceria de confirmação por “SMS Code” a que os terceiros só vieram a aceder no dia seguinte e através de segundas vias do cartão do telemóvel da lesada sem que esta se tivesse apercebido de estar a fornecer ou ter fornecido quaisquer elementos necessários a essa obtenção.

… …

Decisão

Pelo exposto, acordam os juízes que compõem este Tribunal, em julgar improcedente a revista e, em consequência, confirmar a decisão recorrida.

Custas pela recorrente.

Lisboa, 12 de dezembro de 2023

Relator: Cons. Manuel Capelo

1ª Adjunta: Srª. Juíza Conselheira Maria dos Prazeres Pizarro Beleza

2ª adjunto : Sr. Juiz Conselheiro Lino Ribeiro