jurisprudência.pt

Tribunal da Relação de Lisboa
Processo nº 9240/20.5T8LSB.L1-1

Relator: GABRIELA DE FÁTIMA MARQUES
Sessão: 13 Julho 2023
Número: RL
Votação: MAIORIA COM * VOT VENC
Meio Processual: APELAÇÃO
Decisão: IMPROCEDENTE

HOMEBANKING **SISTEMA DE PAGAMENTO BANCÁRIO**

CULPA GRAVE DO UTILIZADOR

Sumário

I. Tem sido entendido que age, censuravelmente, demonstrando negligência grave – cometendo erro imperdoável, desatenção inexplicável, incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes – e violação do seu dever de segurança e confidencialidade sobre os seus dispositivos, o utilizador que – embora sendo utilizador frequente do sistema de pagamento “homebanking” - não se limita a inserir as credenciais de segurança que habitualmente lhe são solicitadas pelo seu banco, mas disponibiliza as coordenadas do cartão matriz.
II. Porém, para aferir de tal culpa (grave e grosseira) haverá que considerar todas as nuances do caso concreto, pois ao prestador de serviços, para se eximir de responsabilidade, não basta que prove que o utilizador desse serviço introduziu no instrumento de pagamento os seus dados confidenciais para acesso ao mesmo, para que se conclua pela culpa do utilizador nas subsequentes operações fraudulentas de homebanking efectuadas por terceiro.
III. Tal culpa grave e grosseira fica desde logo afastada pela circunstância de não ter sido por iniciativa da cliente obtido o código de autenticação enviado por SMS, pois tendo a autora aderido a tal “autenticação forte”, esta falhou não por actuação directa da Autora, mas sim a intervenção de um terceiro, que de forma ilícita logrou obter a 2ª via do cartão do telefone afecto a tal operação de homebanking, permitindo assim, na conjugação com este, número de cliente e cartão matriz, efectuar as operações bancárias subsequentes.

IV. A par daquela circunstância haverá ainda que considerar como não-grave a actuação da Autora que, não obstante ter facultado cópia do cartão matriz, a sua utilização do sistema de homebanking, desde a adesão, limitava-se à consulta de saldos, serviço para o qual não era necessário a utilização do cartão, pelo que é normal que não atentasse nos procedimentos relativos à utilização do cartão-matriz e aos alertas com tal utilização relacionados.
V. A configuração da negligência grave fica ainda afastada pela circunstância de o próprio Banco já ter contactado a Autora para reactivação do serviço de Homebanking pela mesma forma como foi contactada fraudulentamente, competindo à ré provar que nessa reactivação por iniciativa da própria seriam muitos diferenciados os passos a seguir pela Autora.
(Sumário elaborado pela relatora)

Texto Integral

Acordam os Juízes na 6ª Secção Cível do Tribunal da Relação de Lisboa:

I. Relatório:
R… e S… instauraram acção declarativa comum contra M..., SA e N… – SA, pedindo a condenação solidária das rés a pagar-lhes os seguintes valores:
− €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.
Alegam, em síntese, que em 11/03/2019 a A. recebeu um sms que acreditou ser enviado pela 1ª R. referindo que o seu acesso à NET24 estava inactivo e que teria de aceder ao site ali mencionado com designação M… e com hiperligação directa e alterar o seu Código PIN de modo a voltar a ter acesso à NET24 e aos eu cartão matriz, tendo assim procedido. Refere 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 efectuadas 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 objecto do litígio e seleccionados os temas de prova e foi realizada a audiência de julgamento, tendo sido proferida sentença que julgou a acção parcialmente procedente e condenou o Réu M… 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 M… 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 M… do mais peticionado e absolveu o Réu N… S.A. do pedido.
Inconformada veio a 1ª ré M… recorrer, pugnando pela revogação da sentença e prolação de Acórdão que absolva a ré de tudo o peticionado, apresentando as seguintes conclusões:
««A) Vem o presente recurso interposto da douta sentença proferida nos autos em 21/11/2022, a qual julgou "a acção parcialmente procedente e, em consequência, condeno o Réu M… 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 condeno o Réu M… 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. Absolvo o Réu M… do mais peticionado. Absolvo o Réu N… S.A. do pedido. Custas por Autores e Réu M… na proporção de 20% para a primeira e 80% para o segundo – art.º 527º CPC."
B) A R. não se conforma nem aceita a sua condenação, sequer parcial, nem a consequente responsabilidade por custas.
C) Conforme resulta de todos os factos demonstrados nos autos, o R. cumpriu com todas as suas obrigações contratuais e o seu sistema não revelou qualquer falha técnica nem foi alvo de qualquer quebra de segurança informática, não tendo o sítio institucional do M… sido alvo de intrusão, ou qualquer outra violação de segurança.
D) Conforme resulta de todos os factos demonstrados nos autos, o R. cumpriu com todos os deveres, designadamente de informação e alerta dos seus clientes e usuários para as situações correntes de utilização fraudulenta do serviço, alertas de que a A. necessariamente teria tomado conhecimento em qualquer acesso ao serviço

E) “Provou-se ainda que o Banco cumpriu, de forma genérica o dever de prestar informações sobre o modo de utilização do sistema e divulgou conselhos para evitar acessos fraudulentos, publicando exemplos de como os autores de crimes informáticos agem nesta área”.
F) A partir do momento da adesão ao serviço de homebanking, a A passou a autorizar o R. Recorrente a realizar as operações ordenadas, através daquele meio electrónico, desde que introduzidas as necessárias credenciais de utilização e todas as ordens transmitidas mediante a sua correcta validação através do serviço de homebanking gozam de plenos efeitos jurídicos
G) A A., porém, incumpriu de forma grave e grosseira os seus deveres contratuais, formalizados no contrato de “homebanking”, facultando a terceiros dados pessoais e intransmissíveis de acesso à sua conta bancária através daquele meio de pagamento, clicando numa hiperligação recebida por SMS, dando o código e foto do cartão matriz.
H) O facto de a A. não ser uma utilizadora assídua dos serviços de homebanking, não tendo até aquela data utilizado os serviços de pagamento do Banco, não desculpa a menor atenção que dedicou às advertências de segurança e cuidados do R. Banco publicadas desde logo na página inicial do acesso ao serviço Net24 (portanto em página que a A. teria obrigatoriamente visualizado, sempre que acedesse ao serviço, mesmo que apenas para consulta do saldo da conta e sem pretender realizar operações de transferência patrimonial).
I) Essa menor experiência exigiria, pelo contrário, redobrados cuidados e atenção.
J) A falta de cuidado e/ou gravidade da negligência do cliente do serviço de homebanking não são, nos termos legais, avaliadas em função das características particulares de cada indivíduo, mas em abstracto, face ao cidadão comum colocado na mesma posição e com a medida de um “bom pai de família”,
K) É absolutamente irrelevante a apontada menor experiência da A. (veja-se, aliás, que a própria sentença recorrida refere “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”), que não constitui causa legal de desculpação.
L) O SMS recebido pela A. em 11/03/2019, pelas 10h, no seu telemóvel (…) – em cuja hiperligação a A. clicou desencadeando toda a situação dos autos –, que, conforme os AA. invocam, seria idêntico ao recebido pela A. em 18/07/2019, tendo ambos sido remetidos alegadamente pelo Réu Banco,

revelaria evidentes e sobejamente salientados sinais de origem e finalidade fraudulenta, contendo erros de português e linguagem “abrasileirada”.
M) Um outro incumprimento contratual imputável a terceiro e de nenhuma forma controlado pelo R. Recorrente entrecortou a cadeia de segurança no acesso ao serviço de homebanking prestado pelo R., desta feita de algum funcionário da 2ª R. que, violando as obrigações contratuais a que funcionalmente estava adstrito (desconhecendo-se se também por negligência ou em conluio com os autores do acto criminoso), permitiu a apropriação ilegítima de outro dos elementos pessoais e intransmissíveis da A. – o número de telefone associado ao contrato de homebanking.
N) “da descrição feita pela própria Autora do que ocorreu no dia 11/03/2019, sabemos ainda que no dia 12/03/2019 terceiros não identificados efectuaram 20 operações de pagamento de serviços, de idêntico valor, tendo para o efeito utilizado os fundos existentes na conta à ordem e mobilizado o restante montante existente na conta a prazo, através da utilização das credenciais de acesso da Autora ao sistema de homebanking, incluindo o código enviado por telemóvel”.
O) Conforme resulta dos factos provados, todos os quatro passos de autenticação para a realização de cada uma das ordens de transferência patrimonial que lesaram o património dos autores foram inseridos correctamente e sem erros,
P) Sendo os dois primeiros os inseridos pela A., na página de internet a que acedeu por hiperligação, e sendo os dois últimos os obtidos por envio da própria A. (foto do cartão matriz) e por entrega indevida da 2.ª R. (acesso ao número de telefone associado ao contrato),
Q) Eventos que, em conjunto e naturalisticamente, conduziram de forma decisiva à produção do resultado, com a actuação ilícita do(s) agente(s) que, utilizando os dados facultados pela A. (número de utilizador, código PIN e todas as 72 posições do cartão matriz) e pela 2.ª R. (serviço de telemóvel com o número contratado pela Autora), obtiveram acesso a todos os elementos de autenticação necessários para efectuar, com todas as credenciais de validação, operações à distância nas contas bancárias dos AA..
R) De todos os factos provados nos autos ressalta à evidência que foi por causa imputável à negligência grosseira da A. e também à actuação 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 passos de autenticação e segurança de acesso ao serviço de homebanking.
S) Estando o Recorrente obrigado, nos termos da lei, a colocar à disposição da cliente (ou daquele que como se ela fosse se apresentava, munido de todas as

credenciais de acesso) os fundos que entregara no âmbito do contrato de depósito bancário.
T) Mostra-se assim excluída, sem qualquer margem para dissídio, a responsabilidade da R. Recorrente, nos termos legais,
U) Diversamente, a Autora, 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 a que se referem os autos, por o comportamento da A. – que "não atendeu às advertências feitas pelo Banco" – se qualificar como manifesta negligência grosseira, sendo-lhes imputável, contrariamente ao que vem considerado na sentença recorrida, "uma culpa grave no sentido de desatenção e incúria indesculpável".
V) Ao utilizador dos serviços de pagamento cabe a guarda e o dever de "tomar todas as medidas razoáveis, em especial ao receber um instrumento de pagamento, para preservar a eficácia dos seus dispositivos de segurança personalizados", tendo o dever primordial de não facultar a terceiros os elementos de segurança que lhe são atribuídos, atendendo à sua função de autenticação das operações de pagamento.
W) "mesmo numa situação de pharming em que o utilizador não tenha responsabilidade na entrada na página falsa, terá responsabilidade se facultar mais elementos que aqueles que o banco lhe transmitiu que lhe pedirá: «Já será censurável o seu comportamento se fornece mais informação do que aquela que habitualmente lhe é pedida – se, nomeadamente, faculta todas as coordenadas do seu cartão-matriz, quando o banco anuncia que estas nunca são pedidas para uma mesma operação – ou se lhe são pedidos dados inusuais, como o número de telefone»" [Maria Raquel Guimarães (in «As operações fraudulentas de homebanking na jurisprudência recente: acórdão do Supremo Tribunal de Justiça de 18/12/2013, Proc. 6479/09», Cadernos de Direito Privado, n.º 49 (jan.-mar. 2015), pp. 9-33 (27)].
X) A A. teve uma conduta gravemente negligente, fornecendo, de forma deliberada, as credenciais de segurança a terceiros, com base nas quais os movimentos na conta tiveram / puderam ter lugar, preenchendo assim o estatuído no artigo 72º, nº 3, do DL 317/2009, de 30/10.
Y) Agindo com negligência grave/grosseira ou dolo, terá de ser o utilizador do serviço a arcar com as consequências nefastas que para si resultaram do desvio ilícito de fundos da sua conta, a ele, portanto, cabendo suportar os prejuízos que decorram de tais operações de pagamento por si não autorizadas.
Z) … "caso o cliente faculte a alguém qualquer dos três níveis de segurança (número de contrato, password e Cartão Matriz), [não cremos que] tal possa ser considerado um risco da actividade económica. Ou seja, a conduta

negligente grave da Autora não se pode consubstanciar como um risco inerente à actividade económica da Ré. A não se entender assim, teríamos o campo aberto à aceitação do desleixo, da incúria do utilizador do serviço, sem quaisquer consequências para o mesmo. O equilíbrio contratual – inerente ao sinalagma contratual – ficaria seriamente posto em causa, com aceitação duma postura leónica a todos os títulos inaceitável."
AA) Ao provar a culpa da A., como provou, na transmissão dos dados do cartão matriz a terceiros, e a culpa da 2.ª R. na transmissão do quarto elemento de validação, o R. Recorrente ilidiu a presunção de culpa prevista no artigo 799.º do C. Civil e logrou provar que a falta de cumprimento não procedeu de culpa sua, mas antes de culpa do seu cliente, ora A. Recorrida,
BB) A qual incumpriu o contrato de homebanking e contrariou todas as regras e informações de segurança veiculadas à A. aquando da celebração do contrato de adesão ao serviço, 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.
CC) O R. Recorrente cumpriu o ónus de provar a actuação gravemente negligente da A., na utilização do serviço de homebanking, concorrendo ainda a culpa da 2ª R., facultando a terceiro, que não o seu titular, uma segunda via do cartão telefónico.
DD) Seria inaceitável e todo incompreensível que se viesse a responsabilizar o Banco Réu numa situação em que – como ocorreu no presente caso – tenha cumprido integralmente os seus deveres legais e contratuais mas o seu cliente tenha fornecido ou permitido de forma deliberada o acesso, a terceiros, dos seus códigos pessoais de validação de acesso, que serviram para a realização de movimentos na sua conta por banda desses mesmos terceiros.
EE) Pelo que o R. Recorrente não é responsável pela movimentação fraudulenta das contas, devendo os clientes, AA. Recorridos, suportar as perdas resultantes de operações de pagamento efectuadas por terceiros, a quem, por actuação gravemente negligente, facultaram os códigos e chaves necessários a que tais ordens fossem identificadas como tendo sido dadas por si.
FF) Estando ilidida a presunção de culpa por parte da Ré, conforme inelutavelmente decorre da factualidade provada nos autos, não pode ser imputada qualquer responsabilidade ao banco R., que deve ser absolvido de todos os pedidos contra si formulados, incluindo da indemnização por danos morais a qualquer dos AA e juros legais, pois, se não há censura a fazer ao Banco Réu, evidentemente não há lugar a qualquer indemnização a arbitrar aos AA.,
GG) Não sendo o R., também, responsável por quaisquer custas processuais.

HH) Diversas situações factuais em tudo idênticas à que foi provada nos presentes autos têm vindo a merecer análise e tratamento jurisprudencial, em doutas decisões responsabilizadoras da actuação grosseiramente negligente do cliente bancário, decisões cuja fundamentação e sentido decisório o R. Recorrente invoca e de que nesta sede se socorre, pela sua prolixidade, erudição, sensatez e total aplicabilidade ao caso a que os presentes autos respeitam, nos exactos termos que resultam dos factos provados, designadamente as que se mostram plasmadas nos seguintes arestos:
Acórdão do Tribunal da Relação de Lisboa de 19/09/2006 (Relatora Maria Amélia Ribeiro)
Acórdão do Tribunal da Relação do Porto de 14/07/2020 (Processo 22158/17.0T8PRT.P1)
Acórdão do Supremo Tribunal de Justiça de 18/12/2013 (Ana Paula Boularot, Proc. 6479/09.8TBBRG.G1.S1)
Acórdão do Tribunal da Relação de Guimarães de 23/10/2012 (relator Filipe Caroço, Proc. nº 305/09.5TBCBT.G1),
Acórdão do Tribunal da Relação de Guimarães 25/11/2013 (Espinheira Baltar, Processo n.º 2869/11)
Acórdão do Tribunal da Relação de Lisboa no processo nº. 164/11.8TBSRT.L1-6
Acórdão do Tribunal da Relação de Guimarães de 23/10/2012 (Proc. nº 305/09.5TBCBT.G1)
Acórdão do Tribunal da Relação de Évora de 25/06/2015 processo número 3052/11.4TBSTR.E1
Acórdão do Tribunal da Relação de Guimarães, em 25/11/2013, proc. 2869/11.4TBGMR.G1
Acórdão do Tribunal da relação de Évora de 12/12/2013
Acórdão do Tribunal da Relação de Évora de 12/04/2018
Acórdão do Tribunal da Relação de Lisboa de 12/07/2018 no processo número 2256/17.0T8LSB.L1-7
Acórdão do Tribunal da Relação de Lisboa de 01/10/2020, PROC 19530/17.9T8LSB.L8
Acórdão do Tribunal da Relação de Guimarães de 09/06/2020, processo número 51/18.9T8PRG.G1
Acórdão do Tribunal da Relação de Lisboa de 13/10/2022, no processo número 344/21.8T8AGH.L1-2
II) A decisão recorrida mostra-se assim violadora, entre outras que V. Exas doutamente suprirão, 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.».
Não foram apresentadas contra alegações.
Admitido o recurso neste tribunal e colhidos os vistos, cumpre decidir.
*
Questão a decidir:
O objecto do recurso é definido pelas conclusões do recorrente (art.ºs 5.º, 635.º n.º3 e 639.º n.ºs 1 e 3, do CPC), para além do que é de conhecimento oficioso, e porque os recursos não visam criar decisões sobre matéria nova, ele é delimitado pelo conteúdo da decisão recorrida.
Importa assim, no caso concreto, saber:
-Se a 2ª A. agiu com negligência grosseira, facultando a terceiros dados pessoais e intransmissíveis de acesso à sua conta bancária através daquele meio de pagamento
- Se por isso, a apelante ilidiu a presunção de culpa prevista no artigo 799.º do C. Civil e provou que a culpa da sua cliente, devendo ser absolvida do pedido

*
II. Fundamentação:
No Tribunal recorrido foram considerados provados os seguintes Factos:
1. Em 01/07/2003, os aqui Autores, abriram, em conjunto, uma conta bancária solidária de depósitos à ordem, junto do Réu Banco, M... S.A., mais precisamente junto do balcão Casal Da Serra, 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 ...,
3. E o IBAN: PT50 ....
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, 365 (trezentos e sessenta e cinco) dias por ano, proceder a um conjunto de operações bancárias "on-line", relativamente à conta de que era co-titular, 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 ..., 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 ..., 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 (...), remetido alegadamente pelo Réu Banco, referindo que o seu acesso à NET24 se encontrava inactivo e que teria de aceder ao site do Banco ali mencionado, com designação M... e com hiperligação directa 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 reactivar o seu acesso ao homebanking, por não ter aquela logrado utilizá-lo por longo periodo,
14. Pelo que, não estranhou a recepção 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 inactivo.
17. Pelo que, acreditando na veracidade da mensagem escrita recebida, a Autora seguiu os passos ali referidos para reactivar 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 Alverca, 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, I..., 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 factura n.º GT163/262017, 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 efectuado 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 Forte da Casa.
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) transacções 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 descrimina:
- 12/03/2019, PAG SERV. 11893 535918270, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535919862, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535922449, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535922847, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535923643, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535943839, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535944635, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535945232, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535945977, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535946227, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535946824, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535948018, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535948564, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535948763, no valor de €1.939,20

- 12/03/2019, PAG SERV. 11893 535948962, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535949360, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535949957, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535950156, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535950406, no valor de €1.939,20
- 12/03/2019, PAG SERV. 11893 535950804, no valor de €1.939,20

37. Para se lograr concretizar as referidas 20 (vinte) transacções 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 Póvoa de Santa Iria,
42. A que foi atribuído o número de processo 194/19.1PEVFX e a correr termos pela 7.ªSecção do DIAP de Loures.
43. Os Autores dirigiram-se, posteriormente, à loja da 2ª Ré, sita em Alverca 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 do Barreiro,
46. Alegadamente a pedido do cliente,
47. Sem assinatura nem apresentação de cartão do cidadão ou qualquer outro documento,
48. Operação registada pela funcionária Dora Santos,
49. E a outra segunda via, pelas 17h 55min., pela Autora, naquela mesma loja de Alverca.
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 M... 24, com o mesmo teor, conforme Doc. n.º 4 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 M... 24 a dizer que o seu PIN estava desativado, conforme Doc. n.º 5 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 M... 24, referindo que o seu telemóvel não estava registado no SMS CODE.
56. Tendo o utilizador e PIN sido desactivados por razões de segurança.
57. E pedindo que acedesse ao site com igual hiperligação directa.
58. Tais movimentações a débito na conta bancária dos Autores não foram por estes autorizadas ou de algum modo consentidas.
59. As operações foram efectuadas 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 ...,
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 respectiva 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 electrónicas 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 M…, 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 M…, 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 pré-activo, 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 M..., com o seguinte teor: "*(...) no dia 11/3/2019, por volta das 10h recebi um sms no meu telemóvel (...) vindo do M... (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 efectua 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 adoptadas, 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 electrónico, 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 “inactivo” refere-se ao estado do canal resultante da decisão do Cliente de não pretender utilizar o canal, na medida em que, com excepção do Phone24, o Cliente pode activar ou inactivar os restantes canais sempre que pretender. A gestão deste estado é efectuada pelo Cliente no primeiro acesso ao M...24 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 activação / último acesso, estando o processo de reactivação disponível mediante contacto com o Phone24 (entretanto é possível a atribuição de novo pin mediante o processo de actualização 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 adopção 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 activação do serviço.
101. Prevê o clausulado da Proposta de Adesão ao Serviço M... 24, 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 M... no âmbito do Serviço M...24.
• 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 efectuadas utilizando as Credenciais de Autenticação, ou através da utilização abusiva das mesmas, motivadas por perda, extravio, roubo, falsificação, cessa no momento em que seja efectuada 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 M... sido alvo de intrusão, ou qualquer outra violação.
*
Foram considerados na sentença recorrida como não provados os seguintes factos:
1. A Autora utilizou o serviço de homebanking do Banco Réu cerca de 3 (três) vezes, no máximo, desde a sua adesão até à data dos factos;
2. À data dos factos, a 2.ª Ré já era conhecedora de centenas de situações idênticas aos presentes autos
3. À data dos factos, era tecnicamente possível à 2.ª Ré utilizar filtros que bloqueassem todos estes tipos de "SMS" ("Short Message Service").
*
III. O Direito:
A questão essencial a decidir prende-se com a verificação ou não por parte da Autora de actuação na utilização dos meios informáticos no acesso à sua conta bancária de forma negligentemente grosseira, com a consequente ausência de responsabilidade da ré instituição financeira.
Subscrevemos na íntegra a bem fundamentada decisão quanto à relação contratual estabelecida entre os AA. e réu Banco, quer quanto à abertura das contas bancárias mencionadas nos autos e adesão da Autora ao sistema de homebanking disponibilizado por aquele Réu e designado por "Net24, expondo-se de forma clara e precisa tal relação, sendo que relativamente ao busílis da questão expõe-se que:« *No caso concreto, encontra-se demonstrado que foram subtraídas quantias das contas bancárias dos Autores, através de operações efectuadas fraudulentamente por terceiros com utilização do serviço de homebanking disponibilizado pelo Banco Réu.*
O homebanking é um serviço prestado pelo Banco Réu através do qual dá ao cliente a possibilidade de efectuar operações bancárias via Internet, nomeadamente, pagamentos e transferências. Portanto, através desse serviço, o Banco transfere para o cliente a execução de actos que anteriormente estavam cometidos aos seus funcionários, dispensando-se a intervenção

destes. Tem vantagens para o cliente, ao permitir-lhe realizar operações bancárias, comodamente, em sua casa, nos horários que lhe são mais convenientes. Mas também traz vantagens ao Banco pois o cliente efectua operações bancárias sem intervenção do seu pessoal, com a inerente diminuição de custos de funcionamento. O Banco deve assegurar, em todas as actividades 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.º 73º do RGICSF aprovado pelo DL 298/92 de 31/12, na redacção 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. 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 actividade, o que, entre nós, se consagrou através do DL 317/2009, de 30 de Outubro (transpondo Directiva 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, de que assumem especial relevo, para a situação sub judice, o disposto nos seus artigos 67.º a 72.º, com paralelismo no disposto nos art.ºs 103º a 122º do capítulo autorização de operações de pagamento do diploma legal que actualmente rege as operações de pagamento efectuadas à distância. Designadamente, para o utilizador, assume especial importância 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 e impondo-se-lhe que tome todas as medidas razoáveis, para preservar a eficácia dos dispositivos de segurança personalizados do instrumento de pagamento.
Conforme o artigo 68.º, ao prestador de serviços impõe-se que assegure que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador. A ter, ainda, em conta, o disposto no artigo 70.º, n.º 2, de acordo com o qual, se um utilizador negar a regularidade de uma transferência executada, não é suficiente para provar que a mesma foi autorizada pelo ordenante, que este agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, alguma das obrigações

que sobre si impendem (actualmente - art.º 113º, nº 3 DL 91/2018 que tem a seguinte redacção: - "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" acrescentando o nº 4 da mesma disposição legal: - "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, a mesma, cf. artigos 71.º e 72.º, 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, respectivamente.».
Aqui chegado o Tribunal recorrido analisa o caso concreto e conclui pela responsabilização do banco, nos seguintes termos: «(…) *decorre dos factos provados que o Banco 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 efectuar as operações de transferências e de pagamentos.*
O que resulta dos autos é que houve um acesso à conta bancária da Autora, 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. Acresce que não foi apurado qual o método informático utilizado pelos indivíduos que se apropriaram das quantias retiradas das contas da Autora. Nas palavras da própria Autora em documento escrito enviado ao Banco a situação poderá ter sido desencadeada da seguinte forma: "no dia 11/3/2019, por volta das 10h recebi um sms no meu telemóvel (962902414) vindo do M… (tudo levava a crer ser verdadeiro), em como o meu acesso ao net24 estava inactivo 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 activo"
Partindo do princípio de que esta foi a situação ocorrida, teremos que analisar a existência de negligência por parte da Autora de forma a excluir a responsabilidade do Banco pela reposição dos fundos retirados da conta bancária da cliente e pelos demais prejuízos causados. Além da descrição feita pela própria Autora do que ocorreu no dia 11/03/2019, sabemos ainda que no dia 12/03/2019 terceiros não identificados efectuaram 20 operações de pagamento de serviços, de idêntico valor, tendo para o efeito utilizado os fundos existentes na conta à ordem e mobilizado o restante montante existente na conta a prazo, através da utilização das credenciais de acesso da Autora ao sistema de homebanking, incluindo o código enviado por telemóvel. Encontra-se ainda demonstrado que a Autora nunca havia realizado antes operações de pagamento, tendo dado pouco uso ao serviço ao longo dos anos e apenas para consulta dos movimentos e estado das suas contas bancárias. Provou-se ainda que o Banco cumpriu, de forma genérica o dever de prestar informações sobre o modo de utilização do sistema e divulgou conselhos para evitar acessos fraudulentos, publicando exemplos de como os autores de crimes informáticos agem nesta área.
De posse destes elementos, poderemos dizer que a Autora teve um comportamento censurável e negligente, fazendo do serviço que lhe foi disponibilizado pelo Banco uma utilização descuidada e imprudente, facilitando culposamente a sua utilização por terceiros? Nos termos do novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, que transpõe para o direito interno a Diretiva (UE) 2015/2366, mais concretamente, do art.º 115º, o ordenante pode ser obrigado a suportar todas as perdas resultantes das operações efectuadas, nomeadamente, 3 - O ordenante suporta todas as perdas resultantes de operações de pagamento não autorizadas, se aquelas forem devidas a actuação fraudulenta ou ao incumprimento deliberado de uma ou mais das obrigações previstas no artigo 110.º, 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.
Não sendo de considerar, face aos factos, a existência de actuação fraudulenta ou incumprimento deliberado das obrigações que lhe cabem, a Autora só pode ser responsabilizada pelas perdas decorrentes das operações a que se referem os autos se pudermos classificar o seu comportamento como negligência

grosseira. O que deve entender-se por negligência grosseira ou culpa grave? Doutrinalmente, ensina-nos Ana Prata in "Cláusulas de Exclusão e Limitação da Responsabilidade Contratual", Reimpressão, págs. 306 a 308, que culpa grave é o mesmo que "negligência grosseira, erro imperdoável, desatenção inexplicável, incúria indesculpável – vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes", transcrevendo a impressiva afirmação de René Savatier, que caracteriza a culpa grave como "uma conduta em que a má fé é verosímil, mas não se encontra absolutamente demonstrada".
Daí que não possa imputar-se à Autora, atendendo às circunstâncias que ficaram demonstradas quanto ao seu comportamento, uma culpa grave no sentido de desatenção e incúria indesculpável. Se parece certo que a Autora não atendeu às advertências feitas pelo Banco, também é certo que a mesma não era uma utilizadora assídua dos serviços de homebanking, não tendo até aquela data utilizado os serviços de pagamento do Banco. Ora, essa circunstância desculpa a menor atenção dedicada pela Autora a essas advertências. Parecem até ser os Bancos os maiores interessados em que os seus clientes utilizem tais serviços, incentivando a sua utilização através da disponibilização de operações com menos custos para o cliente do que aquelas que são realizadas ao balcão ou com efeitos mais rápidos do que estas. Certamente terão os profissionais consciência que ao disponibilizar tais serviços ao público em geral, estão a colocar nas mãos de pessoas menos dotadas para a utilização de meios informáticos, que são simples utilizadores rudimentares de tais meios, uma poderosa e complexa máquina avidamente cobiçada por aqueles que não tem qualquer escrúpulo em apoderar-se do que é alheio e dispõem de conhecimentos técnicos avançados e de criatividade para enganar tanto os mais incautos como até os cautelosos. Visto que sobre o Banco impende a obrigação de prestar um serviço eficaz e seguro, a ele cabe, ilidir a presunção de culpa quanto a deficiências de funcionamento do sistema que utiliza para prestar esse serviço, correndo por conta dele o risco de acessos fraudulentos por parte de terceiros.
Todos hoje sabemos que os meios de comunicações electrónicos podem ser alvo de violação por terceiros que se imiscuem em tais meios de comunicação e os utilizam em seu proveito, mediante a apropriação ilícita das credenciais do seu utilizador legítimo ou mediante o desbloqueamento, por qualquer outra forma, das barreiras de protecção que essas credenciais se destinam a abrir. Impende sobre o Banco que aceita esse tipo de via de comunicação com os respectivos clientes um dever especial de protecção do património destes, por terem aquelas entidades elevados níveis de competência técnica, para garantir que a sua organização empresarial funciona com os meios humanos e

materiais adequados a assegurar condições apropriadas de qualidade e eficiência que não podem ser comparadas com as condições de que dispõe um mero consumidor, sendo esses mesmos níveis de competência susceptíveis de transmitir uma elevada confiança ao consumidor, na sua relação com aquele tipo de entidades, que o leva a ser menos defensivo. Tal dever especial de protecção exigiria que o Banco reforçasse as garantias de utilização do seu sistema de homebanking conferindo ao cliente meios de autenticação susceptíveis de denunciar a eventual utilização ilegítima desses mesmos meios, lhe disponibilizasse canais de comunicação que pudesse controlar (designadamente, através da detecção e bloqueio de padrões irregulares de utilização, diferentes dos habituais para aquele cliente, como aqueles a que se referem os autos) e que permitissem mais segurança nas transacções. Permite o novo regime para este sector que o Banco, mediante estipulação expressa no contratoquadro, ao prestador de serviços de pagamento pode reservar-se o direito de bloquear um instrumento de pagamento por motivos objectivamente fundamentados, que se relacionem designadamente, com: a) A segurança do instrumento de pagamento; b) A suspeita de utilização não autorizada ou fraudulenta desse instrumento.
Assim, nos casos em que o utilizador negue ter ordenado uma operação de pagamento, como acontece no caso em apreço, cabe ao Banco provar que o pagamento foi autorizado pelo titular da conta sobre a qual tal pagamento foi efectuado ou que este incorreu num comportamento gravemente negligente que permitiu o acesso de terceiros ao sistema.».
É relativamente a este entendimento que a recorrente se insurge, pretendendo sim que face aos factos se conclua pela negligência grosseira da Autora. Por um lado, refere que cumpriu com todas as suas obrigações contratuais e o seu sistema não revelou qualquer falha técnica nem foi alvo de qualquer quebra de segurança informática, não tendo o sítio institucional do Banco sido alvo de intrusão, ou qualquer outra violação de segurança. Por outro lado, a recorrente alude que cumpriu com todos os deveres, designadamente de informação e alerta dos seus clientes e usuários para as situações correntes de utilização fraudulenta do serviço, alertas de que a A. necessariamente teria tomado conhecimento em qualquer acesso ao serviço. No mais, entende que está consubstanciado o incumprimento da Autora, que adjectiva como sendo grave e grosseiro, facultando a terceiros dados pessoais e intransmissíveis de acesso à sua conta bancária através daquele meio de pagamento, clicando numa hiperligação recebida por SMS, dando o código e foto do cartão matriz. Entende ainda que em nada releva a circunstância de a A. não ser uma utilizadora assídua dos serviços de homebanking, pois tal não desculpa a menor atenção que dedicou às advertências de segurança e

cuidados do R. Banco publicadas desde logo na página inicial do acesso ao serviço Net24, o que exigiria sim redobrados cuidados e atenção.
Alude igualmente que neste acesso há um outro incumprimento contratual imputável a terceiro e de nenhuma forma controlado pelo R. Recorrente, pois algum funcionário da 2ª R. que, violando as obrigações contratuais a que funcionalmente estava adstrito (desconhecendo-se se também por negligência ou em conluio com os autores do acto criminoso), permitiu a apropriação ilegítima de outro dos elementos pessoais e intransmissíveis da A. – o número de telefone associado ao contrato de homebanking.
Considerando os vários passos que permitiam tal acesso e operações, entende a recorrente que é manifesto que foi ilidida a presunção de culpa prevista no artigo 799.º do C. Civil e logrou provar que a falta de cumprimento não procedeu de culpa sua, mas antes de culpa do seu cliente, ora A. Recorrida.
Tendo por base o decidido pelo Tribunal recorrido na sua exímia fundamentação quanto ás normas aplicáveis, importa apreciar se face aos factos provados se antevê uma actuação por parte da Autora de forma negligentemente grave e grosseira, pois só esta ilibará a ré da sua responsabilidade, face às normas jurídicas aludidas e plasmadas na decisão sob recurso.
Em concreto nada releva o eventual comportamento de um terceiro, ou terceiros envolvidos em toda a operação e encadeamento de actos necessários para o efeito, ainda que resulte manifesto que todas as operações foram efectuadas através da utilização do número de cliente da Autora, código PIN e coordenadas aleatórias do seu cartão matriz, mas igualmente validadas com código de autorização, enviado por “SMS” (“Short Message Service”) para o telemóvel associado à conta, por terceiros que lograram pedir e obter a segunda via do referido cartão junto da 2ªRé, pois é a ré Banco que é chamada como responsável face à relação contratual que estabeleceu com os AA. e as normas supra referidas.
Compete nesta sede aferir da negligência grave da Autora, pois a intervenção de um terceiro desconhecido de forma a ser perpetrado o acesso ilícito à conta dos AA. apenas afasta igualmente a negligência grave da Autora. Com efeito, no que concerne à utilização de uma segunda via do cartão do telemóvel da mesma, tal determina que mesmo a ser considerado o comportamento negligente da ré este por si só já não seria de molde a permitir as operações, pois estas foram efectuadas com a conjugação nos termos supra aludidos: PIN, coordenadas do cartão matriz e código de autorização enviado por “SMS”.
Na verdade, a adopção do “SMS Code” - credencial de segurança que complementa os processos de autenticação e confirmação de operações, através da introdução de um código de autenticação enviado por SMS para o

seu telemóvel previamente registado no sistema- destinou-se a incrementar a segurança nos pagamentos digitais, tal como resulta das Orientações da Autoridade Bancária (EBA) relativas à segurança dos pagamentos efectuados através da internet e que veio a ser implementada, em conformidade com a previsão de estabelecimento de uma "autenticação forte" – cfr. artigo 97.º da Directiva 2015/2366 e artigo 104.º do D.L. n.º 98/2018. No caso, a autora aderiu a tal "autenticação forte", porém, esta falhou não por actuação directa da Autora, mas sim a intervenção de um terceiro, que de forma ilícita logrou obter a 2ª via do cartão do telefone afecto a tal operação de homebanking, permitindo assim, na conjugação referida, as operações bancárias subsequentes.
Mas e que mais dizer do comportamento da Autora? Mormente para se poder concluir pelo afastamento da presunção que impende sobre a recorrente?
Não há dúvidas que os meios designados de Homebanking são frequentemente alvo de ataque, com o objectivo de se apropriarem, de forma ilícita, dos fundos existentes nas contas bancárias, através de diversos esquemas fraudulentos, como, entre outros, os designados "phishing" e o "pharming".
Ambas as modalidades de fraude informática caracterizam-se pela introdução de uma pessoa não autorizada numa rede informática e consequente movimentação de fundos das contas bancárias dos clientes para contas de terceiros. De todo o modo, enquanto o "phishing" utiliza como "isco" uma mensagem de correio electrónico, no "pharming" (modalidade mais perigosa que a anterior, por surgir de forma quase imperceptível), o utilizador do serviço é enganado sem se aperceber, uma vez que, esta técnica passa pela instalação de um ficheiro oculto que, por sua vez, vai permitir a redirecção do utilizador para uma página forjada, sempre que digite o site do seu banco. (neste sentido Acórdão desta Relação datado de 13/10/2022, proc. nº 344/21.8T8AGH.L1-2, in www.dgsi.pt).
Na verdade, tem sido entendido que age, censuravelmente, demonstrando negligência grave – cometendo erro imperdoável, desatenção inexplicável, incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes – e violação do seu dever de segurança e confidencialidade sobre os seus dispositivos, o utilizador que – embora sendo utilizador frequente do sistema de pagamento "homebanking" - não se limita a inserir as credenciais de segurança que habitualmente lhe são solicitadas pelo seu banco, mas disponibiliza as coordenadas do cartão matriz.
Porém, para aferir de tal culpa (grave e grosseira) haverá que considerar todas as nuances do caso concreto, pois ao prestador de serviços, para se

eximir de responsabilidade, “não basta que (…) prove que o utilizador desse serviço introduziu no instrumento de pagamento os seus dados confidenciais para acesso ao mesmo, para que se conclua pela culpa do utilizador nas subsequentes operações fraudulentas de homebanking efectuadas por terceiro” (assim, o Acórdão do Tribunal da Relação de Lisboa de 12-10-2017, Pº 4761/15.4T8VNG-2, in endereço da net aludido).
No que concerne à caracterização da negligência grave do utilizador de instrumentos de pagamento bancários, é certo que a doutrina e jurisprudência aludem a casos de inserção de todos os elementos exigidos, indicando nomeadamente Raquel Sofia Ribeiro de Lima (in “A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento electrónico na jurisprudência portuguesa”, in Revista Electrónica de Direito; Outubro 2016, n.º 3, p. 48) como caso exemplificativo aquele que: “O utilizador é constantemente alertado para os indícios de fraude, de maneira a estar, naturalmente, consciente de que os pedidos feitos nestas páginas falsas não são legítimos. Responder a um pedido incomum na página clonada, por exemplo com a indicação de todas as combinações do cartão matriz, demonstrará um enorme descuido e desatenção do titular do IP [instrumento de pagamento]”. Ou ainda na mesma linha Maria Raquel Guimarães (in “As operações fraudulentas de homebanking na jurisprudência recente: Ac. do STJ de 18.12.2013, Proc. 6479/08”, in Cadernos de Direito Privado, nº 49, pp. 9 – 33, ponto 3) que indica aqueles casos em que “o procedimento que tenha de levar a cabo seja muito distinto do habitual e o seu banco o tenha alertado para este tipo de fraude”, mas que, todavia, “já censurável o seu comportamento se fornece mais informações do que aquelas que habitualmente lhe é pedida – se, nomeadamente, facultar todas as coordenadas do seu cartão matriz, quando o banco enuncia que estas nunca são pedidas para a mesma operação”. Igual entendimento resulta enunciado por Bruno da Silva Palhão (in “Operações não autorizadas e repartição dos prejuízos: O homebanking na jurisprudência do RSP, UCP, 2018, p. 44) quando expõe que “perante fraude informática qualificável como pharming, age de modo censurável, potencialmente com especial descuidado, o utilizador que não se limita a inserir as credenciais de segurança que habitualmente lhe são solicitadas pelo seu Banco mas, antes, divulga a quase totalidade das combinações do cartão matriz ou outras informações que o PSP não tenha por hábito solicitar aquando da confirmação da ordem de pagamento”.
Também na jurisprudência na aferição da negligência grave do utilizador de serviços ou instrumentos de pagamento tem sido entendido que consubstancia a mesma a circunstância de tal utilizador transmitir quer o número de contrato, código e a totalidade dos dados do seu cartão matriz (v. g. Acórdão

do Tribunal da Relação de Lisboa de 01-10-2020, proc. nº 19530/17.9T8LSB.L-8, Acórdão do Tribunal da Relação do Porto de 14-07-2020, Pº 22158/17.0T8PRT.P1; Acórdão do Tribunal da Relação de Guimarães de 09-06-2020, Pº 51/18.9T8PRG.G1 todos in www.dgsi.pt).
Importa ainda ter presente que tal como se decidiu no Acórdão desta Relação e secção, Processo nº 18/18.7T8TVD.L1-6, Acórdão datado de 11/04/2019 (*in* endereço da net aludido) "o prestador de serviços é quem está em melhores condições, do que qualquer outro (incluindo o consumidor), para trazer a factualidade demonstrativa do modo como as coisas se passaram. Isto porque o funcionamento do "sistema informático" homebanking pertencente à sua esfera de risco, funcionando como critério suplementar de distribuição do ónus da prova, de acordo com a denominada teoria das esferas de risco.
No caso em apreço e perante os factos demonstrados haverá que considerar toda a actuação da Autora, quer quanto à forma como utilizava tais serviços, quer ainda o comportamento do Banco. É perante estes factos nas suas especificidades que importa apreciar o caso, pois todas as decisões supra referidas que aludem à entrega de todas as coordenadas do cartão matriz como sendo concretizadora da negligência grave do utilizador partem sempre do comportamento que resultou provado no seu todo em cada acção, ou seja, não é pelos simples facto de a utilizadora do serviço facultar cópia do cartão matriz que origina por si só tal culpa grave e grosseira.
Aqui chegados não há que olvidar que a Autora raramente utilizou o referido serviço, sendo que todas as utilizações foram para consulta do saldo da conta à ordem e realizadas através do seu computador pessoal.
Como bem se expõe no Acórdão da Relação e Guimarães, datado de 10/07/2019, proc. nº 2406/17.7T8BCL.G1): "A circunstância de um utilizador do sistema de homebanking, desde a adesão, nunca ter efectuado nenhuma operação com o cartão-matriz, só utilizando o referido serviço para consultas – circunstância que permite considerar como natural que o mesmo não atentasse nos procedimentos relativos à utilização do cartão-matriz e aos alertas com tal utilização relacionados – associada à circunstância de, no momento do fornecimento dos dados do cartão-matriz, o utilizador não se encontrar no site do prestador de serviço, onde os avisos da entidade prestadora do serviço de homebanking surgem, deverão conduzir a considerar como não-grave a negligência do mesmo ao inconscientemente fornecer a terceiros, que para o efeito actuaram fraudulentamente, os dados do seu cartão-matriz.".
Haverá ainda que considerar que o acto que determinou o acesso à conta dos AA. poderá ter origem nos seguintes pontos provados: 12. Em 11/03/2019, pelas 10h, a Autora recebeu um "SMS" ("Short Message Service"), no seu

telemóvel (…), remetido alegadamente pelo Réu Banco, referindo que o seu acesso à NET24 se encontrava inactivo e que teria de aceder ao site do Banco ali mencionado, com designação M… e com hiperligação directa e alterar o seu Código PIN de modo a voltar a ter acesso à NET24 e ao cartão matriz. 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 inactivo 17. Pelo que, acreditando na veracidade da mensagem escrita recebida, a Autora seguiu os passos ali referidos para reactivar 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.
Ainda que não resulte do ponto 17., importa ter presente que resultou provado que a Autora emitiu e subscreveu uma declaração manuscrita, datada de 14/03/2019, que enviou ao Réu M…, com o seguinte teor: " (…) no dia 11/3/2019, por volta das 10h recebi um sms no meu telemóvel (…) vindo do M… (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 (…)". Com efeito, resulta de tal declaração que a Autora terá facultado cópia do cartão matriz, sendo certo ainda que ficou demonstrado que 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". A recorrente não indicou em sede de recurso a alteração do ponto 17. onde se elenca a actuação da Autora cuja origem teve as consequências ilícitas em causa nos autos, mas ainda que considere tal "confissão" inserta na declaração reproduzida, a cedência pela Autora de cópia do cartão matriz visou reactivar o acesso ao serviço.
Ora, dos factos a considerar resultou que em data anterior àquela (11/03/2019) e pelo menos por duas vezes, a Autora já havia sido contactada pelo Réu Banco no sentido de reactivar o seu acesso ao homebanking, por não ter aquela logrado utilizá-lo por longo período, pelo que, não estranhou a recepção do referido "SMS" ("Short Message Service"). A recorrente nada provou ou alegou sobre a forma como tal reactivação por iniciativa da própria teria e foi efectuado pela Autora, nomeadamente tendo em vista se esta comunicação fraudulenta recebida pela Autora e forma de actuar posterior era totalmente estranha às orientações do próprio Banco perante a inactividade

do serviço. Na verdade, o que resulta é que o próprio banco contactava a cliente através de SMS, pelo que mesmo perante a prova da negligência da Autora na entrega das suas credenciais e até eventualmente cartão matriz, a sua adjectivação necessária por forma a ilibar a ré da sua responsabilidade só ocorre se esta tivesse logrado provar que o modo de reactivar o serviço por iniciativa da mesma era muito diferenciado, sendo certo que como resulta dos autos a forma de contactar a cliente era idêntica. Mas e que dizer do aviso contido no cartão matriz e actuação da Autora em desconformidade com este? Como deixámos referido a Autora apenas utilizava esporadicamente o serviço de homebanking na consulta do saldo da sua conta à ordem, pelo que na utilização de tal serviço em nada releva o cartão matriz, tal consulta não é feita com o mesmo. Por outro lado, o "aviso" contido no cartão reportar-se-á às operações a ser feitas com este, é nestas que se alerta que nunca deverá ser indicado mais de 2 dígitos do Cartão Matriz, a cópia do cartão feita pela Autora teve a sua origem na reactivação de um serviço e não numa operação concreta, pelo que não efectuando a Autora operações com tal cartão a sua actuação negligente não se revela gravosa.
De tudo o exposto, e ficando demonstrado que a actuação da Autora é alheia relativamente a todos os elos do *modus operandi* que permitiu a retirada de fundos das suas contas bancárias, fica afastada a sua negligencia grave. Pois, a fraude na movimentação bancária atinente à saída de fundos, concretizada por terceiros, ainda que tenha sido 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. No que diz respeito à entrega de cópia deste, a negligencia da Autora ficará igualmente afastada, quer pela forma como o serviço era utilizado pela mesma, quer pela ausência de prova da forma como a própria ré solicitava a reactivação do serviço, resultando provado que a iniciativa desta era igual à ocorrida fraudulentamente.
Afastada a negligência grave, resta assim, confirmar a bem fundamentada e acertada sentença.
Improcede assim, a apelação.
*
IV. Decisão:
Por todo o exposto, Acorda-se em julgar improcedente o recurso de apelação interposto pela Ré e, consequentemente, mantém-se a decisão recorrida nos seus precisos termos.
Custas pela apelante.
Registe e notifique.

Lisboa, 13 de Julho de 2023
Gabriela de Fátima Marques
Vera Antunes
Anabela Calafate (com voto de vencida)

Voto de vencida
Fiquei vencida como relatora pois entendo que este é um caso flagrante de negligência grosseira pois a autora/apelada forneceu todas as coordenadas do seu cartão matriz, enviando foto do mesmo, como resulta do escrito referido no ponto 92 da matéria de facto que dirigiu ao M... e cuja existência omitiu na petição inicial, indo ao ponto de nesse articulado alegar que não as cedeu a terceiro, dizendo:
«As operações foram efectuadas através da utilização dos dados pessoais da Autora: número de cliente, código PIN e com coordenadas aleatórias do seu cartão matriz» (art.º 98),
«Coordenadas que não foram cedidas pela Autora» (art.º 99).
Ora, nesse documento, por si manuscrito e assinado, com data de 14/03/2019, lê-se, além do mais:
«Para: M…
Eu, S..., cliente (…) venho expor o meu caso de fraude:
No dia 11/3/2019, por volta das 10h recebi um sms no meu telemóvel (962902414) vindo do M... (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. Como já por 2 x anteriormente, o acesso à net 24 24 tinha ficado inativo e eu mudei o código no site e resolveu, pensei que realmente fosse verdade.
Acedi ao net 24 e verifiquei que estava tudo bem, isto dia 11/3/2019.
(…)».
Portanto, essa alegação da autora ao negar expressamente ter fornecido a terceiro as coordenadas do cartão matriz, consubstancia até, litigância de má fé.
Cabe lembrar ainda que está 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 M...24, rubricado e subscrito pela autora, consta que o cliente se compromete a guardar sob segredo as suas credenciais de autenticação, que apenas o legítimo possuidor do cartão

matriz conhece todas as coordenadas do cartão matriz, o qual é remetido ao cliente via CTT em estado pré-activo e apenas é passível de ser activado mediante a validação de códigos de acesso ao NET24 (Número de utilizador e password) adstrito ao cartão expedido, e que na mesma face em que constam as 72 posições de 3 dígitos cada, contém esta advertência: “Atenção: Nunca indique mais do que 2 dígitos deste Cartão Matriz”. Mais são de lembrar os avisos existentes no site da apelante elencados nos pontos 93 a 95, designadamente perante contactos por sms ou emails contendo indicação para aceder a links.
Também não podemos ignorar que nas declarações de parte prestadas na audiência final a autora identificou-se com a profissão de professora, pelo que não é pessoa de parca instrução.
Em suma, julgaria procedente a apelação.
Anabela Calafate