# Acórdão do Tribunal da Relação de Lisboa

| | |
|---|---|
| **Processo:** | **11019/23.3T8SNT.L1-2** |
| **Relator:** | **HIGINA CASTELO** |
| **Descritores:** | **HOMEBANKING**<br>**SERVIÇOS DE PAGAMENTO**<br>**TYPOSQUATTING**<br>**PHISHING**<br>**PHARMING** |
| **Nº do Documento:** | **RL** |
| **Data do Acordão:** | **13-03-2025** |
| **Votação:** | **UNANIMIDADE** |
| **Texto Integral:** | **S** |
| **Texto Parcial:** | **N** |
| **Meio Processual:** | **APELAÇÃO** |
| **Decisão:** | **PROCEDENTE** |
| **Sumário:** | **I. O contrato de *homebanking* é um contrato acessório do de abertura de conta, pelo qual o banco disponibiliza ao cliente o acesso seguro e exclusivo à sua conta bancária, através de canais digitais; o cliente é responsável pela preservação e não transmissão das suas credenciais de acesso e tem o dever de, ao aceder ao sistema, cumprir um conjunto de regras destinadas a assegurar a fiabilidade das comunicações.**<br>**II. A execução de «*operações de pagamento*», entre as quais se incluem as designadas «*transferências bancárias*», reconduz-se ao conceito de «*serviços de pagamento*» para efeitos de aplicação do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, aprovado pelo DL 91/2018 (RJSPME); quando o *homebanking* é utilizado como *serviço de pagamento*, aplica-se-lhe o mencionado Regime.**<br>**III. A autora, querendo entrar no *website* do Novo Banco, fez uma pesquisa no Google e entrou num *site* terceiro, designado «novohanco»; aí chegada, não cuidou de verificar na barra de endereços se teria entrado no sítio pretendido; em seguida, introduziu nesse site parte das suas credenciais de segurança personalizadas e as demais enviou-as em resposta a um *email*, pelo qual lhe foram solicitadas, depois de ter introduzido o seu endereço eletrónico na mesma página. Com o descrito comportamento, a autora violou grosseiramente o dever de tomar as medidas razoáveis para preservar a segurança das suas credenciais.**<br>**IV. Na posse de todas as credenciais fornecidas pela autora, incluindo PIN de 6 dígitos, 3 posições aleatórias do cartão matriz e OTP (one time password), foi realizada uma primeira transferência de 1 €, da conta da autora para um IBAN espanhol (situação de que a autora tomou conhecimento antes de facultar ao terceiro a OTP, pois essa informação constava de SMS pelo qual lhe chegou a OTP), com certificação do destinatário até 20.000 €; em seguida, foi realizada uma segunda transferência no valor de 4.999 €, apenas com introdução do PIN.**<br>**V. À *autenticação forte* do cliente – baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo** |

**que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é) –, aplica-se o Regulamento Delegado (UE) 2018/389 da Comissão, que estabelece que *os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente, sob reserva do cumprimento dos requisitos gerais de autenticação, sempre que o ordenante inicie uma operação de pagamento a favor de um beneficiário constante de uma lista de beneficiários de confiança previamente criada pelo primeiro*.**

**VI. Aparentemente, a autora foi vítima de *typosquatting*, espécie de *cybersquatting* em que se regista um nome de domínio que corresponde a um provável erro de digitação de um outro nome de domínio, pertencente a uma entidade conhecida, com a finalidade de capturar tráfego destinado ao *site* da dita entidade; para consumar ações de apropriação indevida de dados bancários alheios, o *typosquatter*, além de registar o domínio, cria um *site* similar ao do banco pelo qual se pretende fazer passar e ao qual o utilizador incauto vai aceder.**

**VII. O *typosquatting* distingue-se do *phishing* e do *pharming* essencialmente porque: *i.* no *phishing*, o lesado recebe um e-mail (ou outra mensagem digital, v.g. via SMS, MMS ou WhatsApp) com um *link* e, ao clicar neste, é direcionado para um *site* falso; *ii.* no *typosquatting*, espécie de *cybersquatting*, o lesado acede por lapso seu ao *site* falso, seja através de um motor de busca, seja pela errada digitação do endereço na respetiva barra; *iii.* no *pharming* o utilizador digita o endereço certo, ou escolhe o *site* certo, mas é redirecionado para o falso porque o seu *cache* de DNS foi previamente viciado por um vírus ou porque (caso muito raro) o próprio servidor de DNS foi atacado.**

**VIII. Só a autora (e sem prejuízo da responsabilidade do *typosquatter*) é responsável pelo uso das suas credenciais, que não lhe foram roubadas, nem furtadas, e que nem sequer perdeu; facultou-as a terceiros, inserindo-as numa página de Internet e num email desconhecidos.**

**IX. O banco réu cumpriu todas as suas obrigações, nomeadamente, a de executar as ordens que a autora autorizou e consentiu; estando reunidas todas as condições previstas no contrato-quadro celebrado com o ordenante, o prestador de serviços de pagamento que gere a conta deste não pode recusar a execução de uma ordem de pagamento autorizada, ordem que, quando foi, e bem, executada pelo banco, era irrevogável.**

**Decisão Texto Parcial:**
**Decisão Texto Integral:**

**Acordam os abaixo identificados juízes do Tribunal da Relação de Lisboa:**

**<u>I. Relatório</u>**

**NOVO BANCO, S. A., réu na ação que lhe é movida por "A", notificado da sentença condenatória proferida em 2 de maio de**

**2024 e com ela não se conformando, interpôs o presente recurso.**
**Na petição inicial, a autora alega, em síntese que: tem conta bancária aberta no banco réu; em 13 de junho de 2022 entrou na sua página de *homebanking* com vista a atualizar dados pessoais; foram-lhe pedidas por email 3 posições do cartão matriz e a introdução de código enviado por telemóvel, pedidos a que acedeu; foi-lhe pedida autorização para efetuar uma transferência de 1€ (um euro), para um determinado IBAN, o que estranhou, mas realizou, pensando tratar-se de custos da operação; após, consultou os movimentos da sua conta bancária e constatou que, a seguir à transferência de 1€ (um euro), que autorizou, constava outro movimento bancário com a transferência da quantia de 4.999€ (quatro mil novecentos e noventa e nove euros), para o mesmo IBAN, que nunca autorizou, acrescida de custos das transferências e imposto de selo.**
**Termina pedindo que o Banco réu seja condenado a repor na conta bancária da autora a quantia de 5.000€ (cinco mil euros), acrescida dos encargos das transferências e do imposto de selo, e a pagar à autora 1.300€ (mil e trezentos euros), a título de indemnização por danos patrimoniais e não patrimoniais, tudo acrescido de juros de mora à taxa legal, vencidos e vincendos.**
**Citado, o réu negou qualquer responsabilidade pelos alegados danos da autora; os movimentos efetuados na conta da autora foram todos autorizados pela mesma, com recurso a códigos pessoais e intransmissíveis de que só a autora dispõe e que tem o dever contratual de não divulgar a terceiros; o réu sempre cumpriu os seus deveres de informação e divulgação de alertas de segurança junto dos seus clientes, e cancelou os canais digitais da autora assim que teve conhecimento de que alguns movimentos não eram por esta reconhecidos.**
**Pede que a ação seja julgada totalmente improcedente, por não provada, com a sua consequente absolvição dos pedidos formulados.**
**O processo seguiu os regulares termos e, após julgamento, foi proferida sentença que julgou a ação parcialmente procedente, condenando o réu a pagar à autora a quantia de 5.000 €, acrescida dos encargos das transferências e imposto de selo, no valor de 4,18 € e juros de mora, vencidos e vincendos, calculados à taxa supletiva legal, atualmente de 4%, acrescidos de 10 pontos percentuais; condenou, ainda, o réu a indemnizar a autora por danos não patrimoniais com a quanta de 1.000 €, acrescida de juros de mora vencidos e vincendos até efetivo e integral pagamento à taxa legal em vigor.**
**<u>O Banco réu não se conformou e recorreu, concluindo as suas alegações de recurso da seguinte forma:</u>**
**«(…) B. Salvo o devido respeito, a sentença recorrida padece de vícios que a tornam nula, por um lado, e, por outro lado, operou um incorreto julgamento da matéria de facto e uma errada**

**subsunção dos factos às normas legais aplicáveis;**
**C. Em primeiro lugar, a Recorrida peticionou a condenação do Recorrente no pagamento de juros de mora, vencidos e vincendos, calculados à taxa legal – em singelo – sobre os montantes reclamados a título de danos patrimoniais e não patrimoniais;**
**D. Porém, no que à condenação nos danos patrimoniais diz respeito (a reposição do montante de € 5.000,00), o tribunal *a quo* condenou o Recorrente no pagamento à Recorrida de juros legais calculados à taxa de 4% acrescido de 10 pontos percentuais.**
**E. Assim, nos termos da leitura conjugada dos artigos 609.º, n.º 1, e 615.º, n.º 1, alínea e), ambos do CPC, a sentença é nula, porquanto condenou em quantidade superior ao pedido (*ultra petitum*);**
**F. Em segundo lugar, em face da prova produzida e carreada para os autos, resulta que factos há que deviam ter sido considerados provados e não foram (erro de julgamento);**
**G. Por um lado, pese embora se tenha verificado que, das duas operações bancárias, apenas a primeira tenha sido executada com métodos de autenticação forte (*i.e.*: "*one time password*" ("OTP") enviado por SMS para o número de segurança adicional previamente definido, três posições aleatórias do cartão matriz e PIN de acesso aos canais digitais), com certificação do beneficiário, impunha-se incluir na factualidade provada que as operações em crise foram devidamente autenticadas, registadas e contabilizadas, não tendo sido afetadas por qualquer avaria técnica ou qualquer outra deficiência do serviço efetuado pelo Recorrente (conforme vinha alegado nos artigos 50.º e 51.º, da contestação). Assim,**
**H. Compulsados os documentos n.º 5 e 6 juntos pelo Recorrente com a sua contestação, os quais contêm o detalhe das operações em crise nestes autos, verifica-se que nada houve, da banda do Recorrente, que contribuísse para a intromissão que terceiros desconhecidos lograram alcançar no *homebanking* associado aos canais digitais da Recorrida;**
**I. A este propósito, atente-se no depoimento prestado na audiência de julgamento do dia 20.03.2024 pela testemunha AA entre os minutos 00:14:45 e 00:15:56, segundo o qual as operações reclamadas foram concretizadas segundo padrões de segurança e normalidade, sem que o Banco Recorrente tenha registado qualquer interferência, erro ou avaria no seu sistema;**
**J. Também dos documentos juntos pelo Recorrente na contestação resulta claramente que todas as operações foram concretizadas segundo padrões de segurança adequados, tendo sido registadas devidamente nos sistemas do Banco.**
**K. Em face da prova produzida e acabada de indicar, impõe-se o aditamento do seguinte facto aos factos julgados provados:**
***Todas as operações foram devidamente autenticadas, registadas e***

***contabilizadas, não tendo sido afetadas por avaria técnica ou qualquer outra deficiência do serviço efetuado pelo R.***

**L. Por conseguinte, o facto b) deverá ser eliminado dos factos não provados.**

**M. Por outro lado, da prova produzida resultou também que a Autora (por intermédio do seu irmão) recebeu no número de segurança adicional diversas mensagens contendo OTP cuja utilização permitia a concretização de transferências bancárias.**

**Assim,**

**N. Ao contrário daquilo que Autora e o seu irmão "B" pretenderam fazer valer nestes autos, é falso que o ataque a que foram sujeitos tenha sido levado a cabo de uma forma isolada e sem que nada o que pudesse fazer prever, beneficiando a Autora (e o irmão), na ótica do tribunal *a quo*, de uma certa *atenuação de culpa* atendendo a que alegadamente desconheciam os procedimentos adotados pelo Recorrente aquando da atualização dos dados bancários dos seus clientes, bem como eventuais custos associados.**

**O. A este respeito, veja-se o depoimento prestado na audiência de julgamento do dia 28.02.2024 pela testemunha "B" entre os minutos 00:33:02 e 00:45:38 e o documento por este exibido e ordenado juntar aos autos pelo Mm.º Juiz de Direito;**

**P. Com efeito, do confronto entre os documentos juntos aos autos com o depoimento da testemunha "B", resulta que a primeira operação reclamada foi concretizada entre as 16:19:22 horas e as 16:23:24 horas;**

**Q. Pelas 16:21:53 horas, "B" recebeu no seu telemóvel a mensagem SMS que continha o código OTP que, uma vez utilizado – juntamente com a inserção correta de três posições aleatórias do cartão matriz – permitiu a concretização da operação;**

**R. Todavia, da captura de ecrã exibida por "B" resulta que este terá recebido naquele mesmo dia 13.06.2022, pelas 16:14 horas, uma OTP cuja utilização autorizava a realização de uma transferência no valor de € 1,00 para o IBAN (espanhol) ES88 0049 2333 0922 1404 2891 – mensagem que ignorou, conforme lhe era exigível e exigido atendendo a que não pretendia a concretização de qualquer transferência naquelas circunstâncias;**

**S. Assim, deverá ser aditado aos factos provados a seguinte factualidade:**

**No dia 13.06.2022, a Autora – por intermédio do seu irmão – recebeu no número de segurança adicional diversas mensagens contendo a "one time password" cuja utilização correta permitia a autorização de transferências bancárias.**

**T. Em terceiro lugar, de acordo com a fundamentação de direito constante da sentença, o tribunal recorrido não valorou corretamente a conduta da Autora (por si e por intermédio do seu irmão "B");**

**U. Com efeito, do debate e instrução da causa resultou a seguinte factualidade julgada provada: (…) [factos 7, 10, 11, 15, 16 a 20]**
**V. É certo que os bancos, ao recorrerem a sistemas financeiros digitais que possibilitam um elenco de transações a poderem ser operadas por essa via, passam a ter um dever acrescido de zelar, dentro daquilo que é exigível e até possível, pela integridade e segurança do património dos seus utilizadores;**
**W. Esta circunstância não pode, contudo, invalidar aqueles que são os cuidados mínimos exigíveis a qualquer utilizador que, não esqueçamos, retira também inúmeros benefícios deste tipo de serviços *online*;**
**X. Não será despiciendo recordar que é a própria testemunha "B" quem assegura que a(s) mensagem(ns) que recebeu no seu telemóvel no dia 13.06.2022 era(m) *tal e qual* as mensagens que recebia sempre que estava em curso um pedido de autorização de transferência bancária e com as quais estava plenamente familiarizado!**
**Y. Portanto, a testemunha tinha esse conhecimento e ignorou o concreto teor das mensagens que recebeu;**
**Z. Com um agravante: a Autora (por intermédio do seu irmão) transmitiu, por email, não só a OTP que lhe havia sido enviado sem solicitação, como transmitiu ainda, também por email, três posições aleatórias do seu cartão matriz;**
**AA. Ora, este procedimento era absolutamente anómalo e devia ter alertado a Autora (por intermédio do seu irmão) para algo de invulgar que se estaria a passar – o que efetivamente se veio a verificar;**
**BB. Não colhe, por isso, o entendimento vertido na sentença recorrida segundo o qual o Recorrente não havia explicado à Autora e ao seu irmão os concretos procedimentos utilizados aquando de uma atualização de dados bancários online e se os mesmos tinham algum custo associado, porquanto, para qualquer homem minimamente diligente, perspicaz e sagaz, quando colocado perante a mesma circunstância e a mesma solicitação externa, sempre teria de constatar estar a ser alvo de um pedido de transferência bancária imediata para o IBAN (espanhol) concretamente identificado na mensagem, com a agravante de a Autora (por si e por intermédio do seu irmão), enquanto utilizadora regular do sistema de *homebanking*, saber (ou, pelo menos, não poder ignorar) que a solicitação de códigos de segurança por via de email era uma situação absolutamente anómala, conforme os alertas de segurança amplamente divulgados pelo Recorrente e cuja existência está provada nos autos;**
**CC. A conduta descrita preenche, sem margem para dúvidas, o conceito de negligência grosseira por parte da Autora, devendo o Recorrente ser totalmente exonerado de responsabilidade sobre as transações que estão no centro da fraude que aqui se discute,**

**nos termos do disposto no 115.º, n.º 4, do Decreto-Lei n.º 91/2018, de 12 de novembro;**
**DD. Sem conceder e apenas por mera cautela de patrocínio, teria de ser sempre aplicado o regime da culpa do lesado (previsto no artigo 570.º, do Código Civil), reduzindo, no limite, a responsabilidade que aqui se pretendia fazer recair totalmente sobre o banco;**
**EE. Ademais, o tribunal *a quo* considerou ainda que o Recorrente incumpriu o seu dever de proteção do património do utilizador e que, como tal, será responsável pelo prejuízo reclamado pela Recorrida;**
**FF. Salvo o devido respeito, é manifesto que a sentença recorrida labora em lapso ao considerar que as operações deviam ter sido recusadas pelo Recorrente, porquanto não haviam sido autorizadas;**
**GG. Todas operações em causa nestes autos foram, por um lado, efetivamente autorizadas pela Autora (ou por alguém a quem esta cedeu as suas credenciais pessoais e intransmissíveis) e, por outro lado, concretizadas segundo padrões de segurança adequados, sem que da banda do Recorrente tivesse havido qualquer erro, avaria ou falha de segurança;**
**HH. Deste modo, em caso algum pode o Recorrente considerar ter violado os seus deveres de proteção do património da Recorrida;**
**II. Pelo contrário, foi esta quem, com a sua atuação (por si ou por intermédio do seu irmão), permitiu, numa circunstância de tempo e de modo cabalmente apurada nestes autos, que terceiros tivessem acesso às suas credenciais, transmitindo-as num contexto altamente censurável e que lhe é plenamente imputável;**
**JJ. De facto, aquilo que se verificou foi que a Recorrida, querendo aceder ao sítio da internet do Recorrente, pesquisou "Novo banco" no motor de busca Google e ali acedeu ao primeiro resultado que lhe foi apresentado sem cuidar de garantir que estava a aceder a um sítio legítimo; transmitiu a terceiros, por email, as específicas posições do cartão matriz que lhe haviam sido solicitadas e o código OTP recebido no número de segurança adicional – um procedimento absolutamente anómalo e em violação dos mais elementares deveres de cuidado e zelo pelas credenciais de segurança associados ao sistema de *homebanking* disponibilizado pelo Recorrente;**
**KK. Por fim, quanto à condenação nos danos não patrimoniais: não foi o Recorrente quem subtraiu as quantias reclamadas da conta bancária da Recorrida e, bem assim, não foi o Recorrente quem possibilitou ou sequer criou condições para que tal ocorresse;**
**LL. Na realidade, conforme resultou demonstrado, foi a própria Recorrida, por si ou por intermédio do seu irmão "B", quem forneceu a terceiros as credenciais pessoais e intransmissíveis que**

**possibilitavam o acesso e a movimentação da sua conta bancária através do *homebanking*;**
**MM. Ainda que se entendesse que a Recorrida agiu com culpa leve ou levíssima – no que não se concede e apenas por mera facilidade de raciocínio se equaciona –, o certo é que foi a sua conduta que contribuiu para o resultado verificado: a realização de uma transferência bancária da sua conta, no valor de € 5.000,00;**
**NN. Não há qualquer nexo de causalidade entre a conduta do Recorrente e os danos não patrimoniais reclamados pela Recorrida.**
**OO. A intranquilidade, o nervosismo, a ansiedade, apenas terão nexo de causalidade com o ato fraudulento praticado por terceiros que subtraíram o dinheiro da conta da Recorrida!**
**PP. Nem há, salvo melhor entendimento, qualquer disposição no Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica que permita responsabilizar o Banco Recorrente por danos não patrimoniais, quando há culpa do lesado.**
**QQ. Salvo melhor entendimento, foram violadas as disposições dos artigos 483.º e 487.º do Código Civil, não tendo sido alegada e muito menos demonstrada a responsabilidade do Recorrente pelos danos não patrimoniais peticionados por manifesta ausência de nexo de causalidade.**
**Normas violadas: artigos 609.º, n.º 1, 615.º, n.º 1, alínea e), ambos do CPC; 483.º, 487.º e 570.º, do Código Civil; 110.º, 113.º e 115.º, do Decreto-Lei n.º 91/2018, de 12 de novembro.**
**NESTES TERMOS, E NOS MAIS DE DIREITO APLICÁVEIS, deve o presente recurso de apelação ser julgado totalmente procedente, e, em consequência:**
**a) Julgar nula a sentença recorrida por haver condenado o R. *ultra petitum*, nos termos do disposto no artigo 615.º, n.º 1, alínea e), do CPC; *Em qualquer caso,***
**b) Julgar procedente a modificação da decisão de facto, nos termos do disposto no artigo 662.º, n.º 1, do CPC; e**
**c) Revogar a decisão recorrida, substituindo-a por outra que absolva o Recorrente dos pedidos contra si formulados.**
***Fazendo-se, assim, a costumada* JUSTIÇA!»**
**A apelada contra-alegou, pugnando pela improcedência do recurso.**
**Foram colhidos os vistos e nada obsta ao conhecimento do mérito.**
**Objeto do recurso**
**Sem prejuízo da apreciação de eventuais questões de conhecimento oficioso, são as conclusões das alegações de recurso que delimitam o âmbito da apelação (artigos 635.º, 637.º, n.º 2, e 639.º, n.ºs 1 e 2, do CPC).**
**Tendo em conta o teor daquelas, colocam-se as seguintes questões:**
**a) A sentença é nula por ter condenado além do pedido?**

**b) A devida apreciação da prova conduz à alteração da matéria de facto?**
**c) A subsunção dos factos ao direito conduz à total improcedência da ação, devendo a sentença ser revogada e o réu absolvido dos pedidos?**

**II. Fundamentação de facto**

**II.1. Estão provados os seguintes factos (que correspondem aos adquiridos em 1.ª instância, com a extensão sinalizada sob o n.º 42 e o aditamento do n.º 43, com os fundamentos expressos em III.2.):**

**1. A Autora nasceu a .....1951.**
**2. A Autora é reformada, vivendo da sua pensão e da poupança que acumulou durante a sua vida.**
**3. No dia 20.12.1993, a Autora abriu conta junto da Ré, à qual foi atribuído o n.º …08, IBAN PT50 …09, para depósito dos seus valores.**
**4. No dia 24.11.2010, a Autora aderiu aos canais digitais disponibilizados pela Ré, tendo associado o n.º telemóvel …27.**
**5. O número de telemóvel associado pertence a "B", irmão da Autora.**
**6. A utilização dos canais digitais era feita exclusivamente por "B".**
**7. "B" utilizava sempre o motor de busca Google para entrar na página da Ré.**
**8. O primeiro login no computador ocorreu no dia 12.02.2011, tendo sido efetuados 1726 logins com sucesso até ao respetivo cancelamento no dia 13.06.2022.**
**9. Para acesso aos canais digitais, a Autora utilizava PIN numérico, Cartão de acesso (cartão matriz) e Código SMS.**
**10. Em fevereiro de 2022, a ré emitiu um alerta de segurança para "E-mails de Phishing Atualização de Dados Pessoais".**
**11. Em maio de 2022 a Ré emitiu um alerta de segurança, comunicando designadamente "NUNCA forneça os códigos do sistema de segurança adicional por SMS através de chamadas telefónicas, e-mails ou sites desconhecidos".**
**12. Entre os dias 20.05.2022 e 09.06.2022, a Autora efetuou os seguintes movimentos a débito na sua conta à ordem:**
**…**
***[fotografia de extratos de transferências online e de pagamentos de serviços online]***
**13. A Ré por diversas vezes, solicitou Autora que efetuasse a atualização de dados pessoais da sua conta.**
**14. No dia 13.06.2022, a Autora deslocou-se ao escritório do seu irmão "B" para este atualizar os seus dados junto da Ré.**
**15. "B" pesquisou no motor de busca Google o nome "Novo Banco".**
**16. Após lhe serem apresentados diversos resultados de pesquisa, "B" clicou no primeiro resultado e foi direcionado para uma**

**página da internet idêntica à da Ré, mas não coincidente com a mesma, porquanto se tratava de uma página com a designação "Novo Hanco".**
**17. Na referida página foram solicitados os dados pessoais e intransmissíveis associados aos canais digitais da Autora os quais foram efetivamente cedidos.**
**18. Na mesma ocasião, foi solicitado ao utilizador o endereço de correio eletrónico, o qual foi inserido por "B" na referida página.**
**19. Seguidamente, foram pedidas, por email, 3 posições do cartão Matriz e introdução de código enviado por telemóvel e por voz.**
**20. A autora e o seu irmão estranharam, mas autorizaram a operação.**
**21. O texto SMS enviado para o número de telemóvel de "B", e ali recebido, foi o seguinte: "*novobanco Online. Transferências Imediatas. ATENÇÃO: Não divulgue este código a terceiros, nem através de chamadas telefónicas. Valor: 1,00 EUR para IBAN ES43 …69. Acum. Dia: 1,00 EUR (…)".***
**22. Pelas 16:18 horas, foi efetuado o acesso ao *novobanco Online* (MBnet) com a adesão n.º ...9...65, em nome da Autora, e inserção correta do código secreto (PIN) de seis dígitos.**
**23. Entre as 16:19:22 horas e as 16:23:24 horas, foi feito um pedido de execução de transferência imediata da quantia de € 1,00 (um euro), para débito na conta da Autora (n.º …08) e crédito na conta com o IBAN ES43 …69.**
**24. A referida transferência imediata foi executada e validada com recurso às seguintes credenciais de segurança (autenticação forte do cliente):**
**a. Código de seis dígitos enviado por SMS para o número de telemóvel da Autora (…27) – um código único e irrepetível, gerado automaticamente para cada transação;**
**b. 3 posições aleatórias do Cartão Matriz;**
**c. PIN de acesso aos canais digitais, composto por seis dígitos.**
**25. A referida transferência imediata no montante de € 1,00 foi realizada com certificação de beneficiário da transferência até ao limite de € 20.000,00.**
**26. Pelas 16:24 horas, na mesma sessão e após a realização da transferência imediata com certificação de beneficiário, foi realizada uma segunda transferência imediata, no valor de € 4.999,00, da mesma conta da Autora para a mesma conta beneficiária.**
**27. Para a concretização desta operação, foi apenas utilizado o PIN de seis dígitos, tendo sido dispensada a validação com recurso a posições aleatórias do Cartão Matriz e código SMS.**
**28. Logo após a Autora consultou os movimentos da sua conta bancária e constatou que a seguir à transferência de 1,00 € constava outro movimento bancário com a transferência da quantia de 4.999,00 para o mesmo IBAN, acrescida de custos das transferências e imposto de selo.**

**29. De imediato, a Autora, através do seu irmão, reclamou perante o Novo Banco, S.A. e exigiu a devolução do valor que lhe foi retirado da identificada conta.**
**30. Entre as 17:25 e as 18:00, teve a Ré conhecimento de que alguns movimentos a débito da conta bancária da Autora não eram por esta reconhecidos.**
**31. A Ré cancelou de imediato a adesão da Autora aos canais diretos.**
**32. A Autora apresentou várias reclamações nos canais de atendimento da Ré, por email e por carta.**
**33. Em 06.07.2022, a Autora apresentou queixa na PSP – CM LSB – Divisão Policial de Sintra, à qual foi atribuído o NUIPC: ...22.7PLSNT.**
**34. Por carta datada de 23.11.2022, a Ré comunicou à Autora que "***… transferência imediata de 1,00 EUR foi realizada com certificação de beneficiário de transferências até ao limite de 10.000,00 EUR, o que significa que, em futuras transferências para beneficiário certificado, é dispensada a matriz e SMS até ao montante definido. Em relação ao Pedido n.º ..., referente a transferência imediata de 4.999,00 EUR para o IBAN ES43 …69, foi utilizado o PIN do acesso. Acresce indicar que esta operação foi realizada para o beneficiário certificado na operação anterior, dispensando assim a validação por Matriz e SMS".*
**35. A Ré não devolveu qualquer montante à Autora.**
**36. Face à posição da Ré, a Autora sofreu episódios de grande intranquilidade, nervosismo, ansiedade, dificuldade em dormir.**
**Mais ficou provado que:**
**37. Os números IBAN iniciados por *ES* respeitam a contas sediadas em Espanha.**
**38. Consta do documento intitulado "PEDIDO CARTÃO P/ ADESÃO CANAIS DIRECTOS" que:**
***"2. Acesso***
***2.1. Para aceder aos Canais Diretos, o Cliente tem de se identificar perante o operador do canal em causa.***
***2.2. Para efeitos do disposto em 2.1., o BES, a pedido do Cliente, emitirá:***
***i) um Cartão de Acesso aos Canais Diretos, que consiste um elemento de identificação secreto, pessoal, único e intransmissível, do qual constam dois códigos de acesso ao serviço: o número de adesão e uma chave alfanumérica;***
***ii) um Código Secreto (PIN), único, pessoal e intransmissível, composto por seis dígitos.***
***(...)***
***3. Movimentação***
***3.1. Ao pedir o acesso aos Canais Diretos, o Cliente aceita que qualquer pessoa que cumpra o disposto em 2. terá acesso à Conta D/O e às contas e produtos a ela associadas, bem como a outras contas bancárias e produtos de que o Cliente seja titular e com***

***poderes suficientes para a movimentar, podendo realizar quaisquer operações, nomeadamente, pedidos de débito, pedidos de crédito, resgates ou constituição de aplicações, independentemente das condições de movimentação constantes das respetivas Fichas de Abertura de Conta."***

**39. Consta da secção de "Abertura de Conta de Depósito à Ordem", das Condições Gerais do documento intitulado "Contrato de Abertura de Conta" que:**

***"2.2. Representação***

***A Conta D/O pode ser movimentada, a débito, por terceiros a quem tenham sido atribuídos, pelos respetivos titulares, poderes para o efeito. No caso de contas plurais, os titulares que não sejam mandantes deverão expressamente autorizar a movimentação da conta pelos mandatários ao abrigo dos poderes conferidos".***

**40. A Autora pagou 4,16 euros de comissões de transferência e imposto de selo.**

**41. O Novo Banco sucedeu ao BES (Banco Espírito Santo).**

**42. Consigna-se neste acórdão que o documento parcialmente transcrito nos factos 38 e 39 é aquele a que se refere o facto 4, pelo qual a autora pediu cartão para adesão aos canais diretos, subscrito pela autora em 24/11/2010, e que desse documento constam, ainda e entre outras, as seguintes condições:**

**«4. Responsabilidade**

**4.1. Em caso de (…)divulgação dos elementos referidos em 2.2., o Cliente deve comunicar de imediato ao BES a ocorrência (…).**

**4.2. O Cliente assume todos os prejuízos resultantes da utilização dos Canais Diretos por terceiros caso tenha, por qualquer forma, divulgado os elementos referidos em 2.2.**

**4.3. O BES apenas é responsável pelos prejuízos decorrentes da utilização abusiva dos Canais Diretos por terceiros ocorridos após a receção da comunicação referida em 4.1.»**

**43. As operações de 13/06/2022, postas em causa pela autora nos presentes autos, foram devidamente autenticadas, registadas e contabilizadas, não tendo sido afetadas por avaria técnica ou qualquer outra deficiência do serviço efetuado pelo réu.**

**II. 2. Não se provou o seguinte facto (que corresponde ao primeiro dos indicados como não provados na sentença, tendo o segundo, al. b), transitado para a matéria provada sob o n.º 43, com os fundamentos expressos em III.2.):**

**a) A Autora e "B" permitiram que terceiros instalassem programas de *malware* nos dispositivos por si utilizados, com o intuito de se apropriarem de informação confidencial neles contido, designadamente dados bancários e credenciais pessoais.**

## III. Apreciação do mérito do recurso

### III.1. Da nulidade da sentença

**O apelante suscita a nulidade da sentença por condenação além do pedido.**

**O *pedido formulado* no autos foi o de condenação do réu a repor a**

**quantia de 5.000 €, acrescida dos encargos das transferências e do imposto de selo; a pagar a quantia de 1.300 € a título de danos patrimoniais e não patrimoniais sofridos pela autora; e, a pagar juros de mora, à taxa legal, vencidos e vincendos, referentes aos valores supramencionados.**
**A *decisão final* importou na condenação do réu a pagar à autora 5.000 €, acrescidos dos encargos das transferências e imposto de selo, no valor de 4,18 €, e juros de mora, vencidos e vincendos, calculados à taxa supletiva legal, atualmente de 4%, acrescida de 10 pontos percentuais; e, ainda, a quantia de 1.000 €, acrescida de juros de mora vencidos e vincendos até efetivo e integral pagamento à taxa legal em vigor, a título de indemnização por danos não patrimoniais.**
**A sentença não pode condenar em quantidade superior ou em objeto diverso do que se pedir (artigo 609.º, n.º 1, do CPC).**
**Se o fizer, é nula (artigo 615.º, n.º 1, al. e), do CPC).**
**A limitação quantitativa da condenação reporta-se ao valor global do pedido e não a cada um dos valores parcelares que o integram (neste sentido, exemplificativamente, o Ac. do TRC de 05/05/2021, proc. 345/18.3JALRA.C1, e o do TRP de 07/10/2024, proc. 564/12.6TBPVZ.P1).**
**Em termos de capital, a condenação ficou aquém do pedido em 300 €. Porém, a condenação em juros sobre a parcela de 5.004,18 € foi de 14% ao ano, quando tinham sido pedidos juros de 4%. Um só ano de juros já importaria num acréscimo superior a 500 €, pelo que temos de concluir que houve condenação além do pedido, com a consequente nulidade da sentença.**
**Em todo o caso, há que apreciar o objeto da apelação, ao abrigo do disposto no artigo 665.º do CPC, o que faremos em seguida.**
**<u>III.2. Da impugnação da matéria de facto</u>**
**No recurso, nomeadamente em sede de conclusões, o apelante pede o aditamento de dois factos, cuja redação indica, bem como a exclusão do da alínea b) dos não provados (porque o conteúdo deste passará a integrar um dos factos que deseja aditar aos provados). Independentemente da bondade da sua pretensão, fundamenta-a cabalmente, indicando os meios de prova em que a alicerça e, no caso de prova gravada, as passagens em que as testemunhas se pronunciaram em conformidade.**
**Com o descrito procedimento, o apelante cumpriu os ónus que, por força do disposto no artigo 640.º do CPC, impendem sobre quem impugna a matéria de facto, a saber:**
**a) Especificação dos concretos pontos de facto que considera incorretamente julgados;**
**b) Explicitação dos concretos meios probatórios, constantes do processo ou de registo ou gravação nele realizada que impunham decisão, sobre os pontos da matéria de facto impugnados, diversa da recorrida, indicando com exatidão as passagens da gravação em que se funda o seu recurso;**

**c) A decisão que, no seu entender, deve ser proferida sobre as questões de facto impugnadas.**
**Alega o recorrente (conclusões G a L) que, pese embora se tenha verificado que, das duas operações bancárias, apenas a primeira foi executada com métodos de autenticação forte (i.e.: OTP – *one time password* – enviada por SMS para o número de segurança adicional previamente definido, três posições aleatórias do cartão matriz e PIN de acesso aos canais digitais), nela foi feita a certificação do beneficiário, pelo que se impõe incluir na factualidade provada que as operações em crise foram devidamente autenticadas, registadas e contabilizadas, não tendo sido afetadas por qualquer avaria técnica ou qualquer outra deficiência do serviço efetuado pelo recorrente.**
**Invoca especificadamente vários meios de prova e pede o aditamento do seguinte facto aos factos julgados provados:**
***Todas as operações foram devidamente autenticadas, registadas e contabilizadas, não tendo sido afetadas por avaria técnica ou qualquer outra deficiência do serviço efetuado pelo R.***
**Consequentemente, pede a eliminação da al. b) dos factos não provados, a saber: «b) Todas as operações foram devidamente autenticadas (com recurso a métodos de autenticação forte), registadas e contabilizadas».**
**Mais alega (conclusões M a S) que, ao contrário daquilo que autora e o seu irmão pretenderam fazer crer, é falso que desconhecessem os procedimentos adotados pelo recorrente aquando da atualização dos dados bancários dos seus clientes, bem como eventuais custos associados.**
**A este respeito, veja-se o depoimento prestado na audiência de julgamento do dia 28.02.2024 pela testemunha "B" entre os minutos 00:33:02 e 00:45:38 e o documento por este exibido e ordenado juntar aos autos pelo Mm.º Juiz de Direito, dos quais resulta que a primeira operação reclamada foi concretizada entre as 16:19:22 horas e as 16:23:24 horas; que, pelas 16:21:53 horas, "B" recebeu no seu telemóvel a mensagem SMS que continha o código OTP que, uma vez utilizado – juntamente com a inserção correta de três posições aleatórias do cartão matriz – permitiu a concretização da operação; todavia, da captura de ecrã exibida pela testemunha resulta que esta terá recebido naquele mesmo dia 13.06.2022, pelas 16:14 horas, uma OTP cuja utilização autorizava a realização de uma transferência no valor de € 1,00 para o IBAN (espanhol) ES88 ...4... 2333 – mensagem que ignorou, conforme lhe era exigível e exigido atendendo a que não pretendia a concretização de qualquer transferência naquelas circunstâncias.**
**Assim, pede que se adite: «No dia 13.06.2022, a autora – por intermédio do seu irmão – recebeu no número de segurança adicional diversas mensagens contendo a "one time password" cuja utilização correta permitia a autorização de transferências**

**bancárias».**
**Apreciando e decidindo.**
**Começando pelo último ponto. Este facto, que não foi alegado nos articulados, é irrelevante. Pode haver várias explicações para se ter ignorado a primeira OTP, e a própria autora disse que estranhou estarem-lhe a pedir a transferência, mas pensou que fosse uma comissão para atualizar os dados. De todo o modo, o facto, meramente secundário, é irrelevante, pois a autora não podia deixar de conhecer os procedimentos, que lhe foram claramente transmitidos, quando pediu a adesão aos canais digitais, em documento que assinou. Canais digitais que usou durante cerca de 12 anos. Acresce que, para além dos deveres contratuais, são igualmente pormenorizados, explícitos e lógicos os deveres legais que impunham à autora diferente comportamento. O desconhecimento da lei não lhe aproveita (artigo 6.º do CC).**
**Quanto à primeira situação, conjugando os factos 15 a 27 (atentando especialmente nos factos 23 a 26), remetendo para a análise que deles fazemos adiante (*maxime* de III.3.5. em diante), considerando as normas aplicáveis e adiante pormenorizadas (especialmente em III.3.7. e III.3.8.), não podemos deixar de concluir que *as operações de 13/06/2022, postas em causa pela autora nos presentes autos, foram devidamente autenticadas, registadas e contabilizadas, não tendo sido afetadas por avaria técnica ou qualquer outra deficiência do serviço efetuado pelo réu*, facto que se adita, excluindo consequentemente a alínea b) dos não provados. Com efeito, os factos evidenciam que a execução das transferências foi conforme ao comportamento da autora e causada por esse comportamento, sem que tenha coexistido qualquer avaria ou deficiência do serviço prestado pelo réu. O depoimento da testemunha AA, empregado do réu no departamento dos canais diretos desde 2001 também asseverou que nenhuma avaria, mau funcionamento ou deficiência do serviço ocorreu, e que as ordens chegaram ao banco emitidas com as credenciais necessárias, pessoais e intransmissíveis da autora. Em suma, exclui-se a alínea b) dos factos não provados e adita-se aos provados:**
**43. As operações de 13/06/2022, postas em causa pela autora nos presentes autos, foram devidamente autenticadas, registadas e contabilizadas, não tendo sido afetadas por avaria técnica ou qualquer outra deficiência do serviço efetuado pelo réu.**
**<u>III.3. Da responsabilidade pelas transferências bancárias feitas a partir da conta da autora em 13/06/2022</u>**
**<u>III.3.1. Recordemos os acontecimentos relevantes de forma resumida e num discurso mais articulado do que aquele que é próprio do elenco dos factos provados.</u>**
**A autora, titular de uma conta bancária no Novo Banco, com recurso aos canais digitais desde 2010, em 13/06/2022, acedeu ao**

**_homebanking_ com o intuito de atualizar dados pessoais. Como sempre, pediu ao seu irmão que o fizesse por si, sendo a atuação do irmão meramente material, a pedido e segundo as instruções da autora que, inclusivamente, se encontrava no mesmo espaço físico aquando do acesso e das operações realizadas. Por facilidade de expressão, e porque o irmão nada mais foi que «o dedo da autora no teclado», reportar-nos-emos sempre à autora.**
**No mencionado dia, para aceder ao site do Novo Banco, a autora pesquisou no motor de busca Google a expressão «Novo Banco», surgiu-lhe no ecrã uma lista de resultados, vários websites, e escolheu o primeiro.**
**Foi aberto um site de aspeto semelhante ao do Novo Banco, mas que não era o site do Novo Banco, não tinha o respetivo endereço, https://www.novobanco.pt/, tratando-se antes de um site que tinha no nome «novohanco».**
**Na referida página, foram solicitados os dados pessoais e intransmissíveis associados aos canais digitais da autora, os quais foram efetivamente cedidos. Na mesma ocasião, foi-lhe solicitado o endereço de correio eletrónico, que também facultou, inserindo-o na referida página (factos 17 e 18).**
**Pelas 16:18 horas, foi efetuado o acesso ao _novobanco Online_ (MBnet) com a adesão n.º ...9...65, em nome da autora, e inserção correta do código secreto (PIN) de seis dígitos (facto 22).**
**Entre as 16:19 horas e as 16:23 horas, foi feito um pedido de execução de transferência imediata da quantia de € 1,00 (um euro), para débito na conta da autora (n.º …08) e crédito na conta com o IBAN ES43 …69 (facto 23).**
**Para tanto, foram pedidas à autora por email 3 posições do cartão matriz e introdução de código enviado por telemóvel e por voz. A autora estranhou, mas autorizou a operação. O texto SMS enviado para o número de telemóvel associado à conta da autora, e ali recebido, foi o seguinte: "_novobanco Online. Transferências Imediatas. ATENÇÃO: Não divulgue este código a terceiros, nem através de chamadas telefónicas. Valor: 1,00 EUR para IBAN ES43 …69. Acum. Dia: 1,00 EUR (…)"_ (factos 19 a 21).**
**A referida transferência imediata foi executada e validada com recurso às seguintes credenciais de segurança (autenticação forte do cliente): a. código de seis dígitos enviado por SMS para o número de telemóvel da autora (…27) – um código único e irrepetível, gerado automaticamente para cada transação; b. 3 posições aleatórias do Cartão Matriz; c. PIN de acesso aos canais digitais, composto por seis dígitos (facto 24).**
**A mesma referida transferência foi realizada com certificação de beneficiário da transferência até ao limite de € 20.000,00 (facto 25), o que significa que as futuras transferência para esse beneficiário, até ao indicado valor, não necessitariam de posições do cartão matriz, nem de código único enviado por SMS.**
**Pelas 16:24 horas, na mesma sessão e após a realização da**

**transferência imediata com certificação de beneficiário, foi realizada uma segunda transferência imediata, no valor de € 4.999,00, da mesma conta da autora para a mesma conta beneficiária, para a qual foi inserido apenas o PIN de seis dígitos (factos 26 e 27).**
**Só depois, ao consultar os movimentos da sua conta bancária, a autora constatou que a seguir à transferência de 1,00 € havia outro movimento a débito com o valor de 4.999,00 € para o mesmo IBAN, acrescido de custos de transferência e imposto de selo (facto 28) e contactou a ré que, ao tomar conhecimento de que a autora não reconhecia o segundo movimento referido, prontamente cancelou a adesão da autora aos canais diretos (factos 29 a 31).**
**III.3.2. Analisando os factos, inserindo-os num tipo ou padrão social (no caso, ilícito), e distinguindo este último de padrões análogos.**
**Ponderando os factos essenciais vindos de descrever, os demais que os contextualizam e chamando ao raciocínio regras da experiência comum, não duvidamos de que a autora foi ludibriada por um terceiro, sem conluio da autora com o mesmo terceiro. O banco réu também não pôs em causa a boa-fé da autora.**
**Na descrita situação, um terceiro adquiriu ou (criou e) registou um domínio com um nome muito parecido ao Novo Banco, mais precisamente «Novo Hanco», com o objetivo de capturar buscas dirigidas ao Novo Banco, e de com isso obter informações necessárias à utilização de contas bancárias alheias para desviar fundos dessas contas em seu benefício, e sem que o lesado tivesse consciência da intervenção desse terceiro no processo.**
**Repare-se que o domínio fraudulento – novohanco – resulta da substituição de um «b» do domínio original «novobanco» por um «h»; não apenas o «b» e o «h» são graficamente parecidos (quer em minúscula, quer em maiúscula), como no teclado português o «h» fica imediatamente por cima do «b», um pouco à direita. É fácil uma pessoa que pretende digitar Novo Banco enganar-se e escrever Novo Hanco.**
**O registo de nomes de domínio que correspondem a um erro de digitação provável de uma marca, empresa ou outra entidade conhecida, com fins ilícitos, normalmente acompanhado da criação de um site similar àquele pelo qual o agente se pretende fazer passar ou relativamente ao qual pretende capitalizar ilegitimamente, tem sido designado por *typosquatting*, uma das variantes mais comuns do chamado *cybersquatting*.**
**Ambos os conceitos têm presença em https://en.wikipedia.org e em dicionários jurídicos, designadamente no disponível em https://www.law.cornell.edu/wex, da Universidade de Cornell.**
**Para o que a seguir escrevemos foram, ainda e entre outros, consultados os textos das páginas https://www.bankrate.com/**

**personal-finance/what-is-typosquatting/ e https://www.kaspersky.com/resource-center/preemptive-safety/cybersquatting.**

**O *cybersquatting* refere-se ao registo e uso de nomes de domínio da Internet idênticos ou semelhantes a marcas, empresas ou pessoas registadas ou notórias, com intenção de se confundir com essas entidades, com vários objetivos ilícitos, como aquele que se verifica no caso destes autos.**

**Em muitos casos, os *cybersquatters* registam esses domínios com a intenção de posteriormente os vender aos donos das marcas ou à entidades cujos domínios copiaram, outras vezes, usam os domínios para criar sítios de Internet (sítios, *sites, websites*, páginas) de *phishing*, efetivar burlas variadas, realizar inquéritos com a finalidade de obter dados alheios, etc.**

**O *typosquatting* é uma espécie de *cybersquatting* que, como o nome (*typo*) indica, conta com prováveis erros de digitação habitualmente cometidos, passa pela aquisição ou registo de nomes de domínio com grafia semelhante ou incorreta com a finalidade de capturar tráfego destinado a outro site. O endereço fraudulento pode ser uma variação subtil do original, com uma letra diferente ou o aditamento de um hífen.**

**Os *typosquatters*, como qualquer dono de *website*, podem pagar publicidade aos motores de busca para que o seu *site* apareça em primeiro lugar e, além disso, podem indicar as palavras ou expressões que, se forem digitadas, espoletam o retorno do *site* nas pesquisas. Pensando no caso concreto, o «novohanco» poderia aparecer listado em primeiro lugar não apenas quando o utilizador digitou «Novo Hanco», mas também quando digitou «Novo Banco».**

**Noutros países, sem prejuízo da previsão e punição de vários tipos de cibercrime, existe legislação específica para *prevenir* estes casos, com destaque para o Anticybersquatting Consumer Protection Act (ACPA), lei federal dos Estados Unidos que proíbe registos de nomes de domínio idênticos ou semelhantes a marcas registradas ou nomes pessoais. Um utilizador não autorizado pode ser responsabilizado perante o dono de uma marca registada por pretender lucrar ilicitamente com a mesma marca.**

**As formas de evitar ser-se vítima de *typosquatting* são simples: digitar o endereço do sítio ao qual se pretende aceder na barra de endereço (em vez de se fazer uma pesquisa por nome no motor de busca) e verificar se se escreveu bem o endereço desejado; caso se pretenda mesmo aceder através de pesquisa prévia em motor de busca, depois de escolher o sítio de Internet (*website*, sítio, *site*, página), verificar na barra de endereço que se trata mesmo do endereço correto e verificar as informações sobre o *site* que se encontram à esquerda do endereço, nomeadamente que a ligação é segura (pois só assim se garante que as informações que se inserem através desse *site* são privadas quando enviadas para esse**

**_site_, não podendo ser acedidas por terceiros).**
**Quem acede a um _website_ diferente daquele a que queria aceder e aí introduz dados, ou faculta dados a terceiros de acordo com instruções que encontra no mesmo site, "só de si se pode queixar", sem prejuízo, obviamente, das responsabilidades do burlão se vier a ser conhecido e encontrado. Incluindo responsabilidade criminal: quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, mediante interferência no resultado de tratamento de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, incorre em pena de prisão até 3 anos ou em pena de multa (no tipo simples e consumado), nos termos do disposto no n.º 1 do artigo 221.º do Código Penal.**
**De referir que o comportamento do terceiro descrito nos autos, que identificámos como uma burla com recurso a _typosquatting_, é diferente da atuação através de _phishing_ e da, mais rara, designada por _pharming_.**
**Recorrendo a trechos do Ac. do TRL de 12/07/2018, proc. 2256/17.0T8LSB.L1-7, da ora relatora, acessível em www.dgsi.pt (como todos os demais citados), relativo a uma situação de phishing, «O _phishing_ assemelha-se à pesca, mas em vez de tentar capturar peixes, tenta apropriar-se de informações pessoais. O autor do _phishing_ envia _e-mail_ que parece proveniente de outra entidade, nomeadamente bancária, referindo que a atualização ou validação de dados é necessária e pedindo para os introduzir, depois de o destinatário clicar num dado _link_ contido no _e-mail_. Depois de clicar no _link_, o destinatário do e-mail de _phishing_ entra num _site_ falso, provavelmente de aspeto parecido ao da entidade pela qual o autor do _phishing_ se quer fazer passar, e introduz os dados necessários para o _login_, como o _username_ (no caso o número de cliente) e a _password_ (no caso o pin de 6 dígitos), entre outros. Mesmo que o visitante da página falsa apenas introduza a sua identidade e palavra-passe, isso permite ao _phisher_ aceder à conta verdadeira e aceder a muitos mais dados. Sobre o conceito de _phishing_, as várias modalidades, as diferenças relativamente ao _pharming_ a que aludiremos em seguida, consultem-se por exemplo https://pc.net/glossary, […], https://en.wikipedia.org/wiki/Phishing. Na literatura jurídica portuguesa, v. Pedro Verdelho, «Phishing e outras formas de defraudação nas redes de comunicação», _in Direito da sociedade da informação_, vol. 8, Coimbra Editora, 2009, pp. 407-419; Ana Vaz Geraldes, «Phishing: fraude on line», _Revista da Faculdade de Direito da Universidade de Lisboa_, Coimbra, vol. 54, n.ºs 1-2 (2013), pp. 87-102, Maria Raquel Guimarães, «As operações fraudulentas de homebanking na jurisprudência recente: acórdão do Supremo Tribunal de Justiça de 18.12.2013», _Cadernos de Direito Privado_, n.º 49 (jan.-mar. 2015), pp. 9-33; Carolina França**

**Barreira, *A repartição dos prejuízos decorrentes de fraude informática*, 2015, tese de mestrado disponível em https://run.unl.pt/bitstream/10362/15191/1/Barreira_2015.pdf; […]». Substituímos por […] páginas de Internet que já não estão acessíveis.**

**Adiante prosseguimos: «O *pharming* é outra forma de internautas malfeitores manipularem os utilizadores de internet. Mas enquanto o *phishing* tenta obter informação pessoal levando os utilizadores a visitar uma página falsa, à qual chegam por terem clicado num *link* de um *e-mail* malfeitor, o *pharming* redireciona os utilizadores para *sites* falsos de forma diferente. Uma página Web (*site*) usa um *nome de domínio* para seu endereço, mas a sua localização real é determinada por um *endereço IP*. Quando um utilizador digita um nome de domínio no campo de endereço do seu navegador (*browser*) e clica «entrar» (*enter*), o nome do domínio é convertido num endereço IP por meio de um servidor DNS. O navegador da Web conecta-se, então, ao servidor nesse endereço IP e carrega os dados da página da Web. Depois de um utilizador visitar um determinado *site*, a entrada de DNS desse *site* é geralmente armazenada no computador do utilizador num *cache* de DNS (*cache* – dispositivo de acesso rápido interno a um sistema, que serve de intermediário entre um operador de um processo e o dispositivo de armazenamento ao qual esse operador acede – pt.wikipedia.org). Dessa forma, o computador não precisa aceder ao servidor DNS sempre que o utilizador visita o *site*.**

**Uma das formas pelas quais o *pharming* ocorre é através de um *e-mail* malfeitor que transporta um vírus (programa de computador que destrói ou altera programas ou equipamentos informáticos alheios sem autorização do visado) que vicia o cache de DNS local do utilizador. Assim, por exemplo, em vez de ter o endereço IP 12.345.6.789 dirigido para www.montepio.pt, dirige-o para outro *site* determinado pelo malfeitor. Para que o programa de vírus se instale no computador do utilizador é necessário que o utilizador faça algo no *e-mail* (clique em alguma ligação, não basta abri-lo e fechá-lo) e tenha alguma vulnerabilidade no seu computador (falta ou desatualização de antivírus ou de outro *software*).**

**De notar que, de acordo com o relato da autora, não terá sucedido assim (a autora terá acedido à página falsa pelo motor de busca, e não pela linha do navegador ou *browser*).**

**Em todo o caso, na modalidade de *pharming* a que acabámos de aludir também a responsabilidade pelo logro recai sobre o ludibriado que não tem o seu computador suficientemente seguro, com o necessário antivírus, ou tem programas desatualizados que lhe causam vulnerabilidades, permitindo a entrada do aludido vírus que lhe vicia o cache.**

**Há, no entanto, uma outra possibilidade de *pharming*: o *pharmer***

**(o autor do ilícito) também pode envenenar servidores DNS inteiros, o que significa que qualquer utilizador que use o servidor DNS afetado será redirecionado para o *site* errado. Em tal caso, o utilizador pode não ter como se aperceber de que entrou numa página errada. É para situações como a agora descrita (e que não tem correspondência com a do caso *sub judice*) que Maria Raquel Guimarães escreve: «[N]ão podemos acompanhar o mesmo tribunal supremo quando, afastando a hipótese de *phishing* sustentada pelo tribunal *a quo* em benefício do *pharming*, afirma que, "quer fosse uma das técnicas ou a outra, qualquer delas consubstancia fraudes informáticas, conduzindo aos mesmos resultados em termos de responsabilidade"). Entendemos que o comportamento do utilizador de um serviço de *homebanking* que acede a uma página falsa, "pirateada", para a qual foi direcionado quando escreveu a morada do seu banco com recurso ao teclado de um computador, e aí introduz os códigos que lhe são solicitados, dificilmente será passível de um juízo de censura, a menos que o procedimento que tenha que levar a cabo seja muito distinto do habitual e o seu banco o tenha alertado para este tipo de fraudes» (Maria Raquel Guimarães, «As operações fraudulentas de homebanking…», *cit.*, p. 26).**

**Felizmente, a maioria dos servidores DNS possui recursos de segurança suficiente e eficazes que os protegem contra esses ataques. Por isso, tal espécie de *pharming* é muito rara.**

**Ainda assim, Raquel Guimarães não deixa de dizer que, 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» (id., p. 27)».**

**O citado acórdão, de onde extratámos os trechos acabados de reproduzir, foi proferido ainda na vigência do regime jurídico que regulava o acesso à atividade das instituições de pagamento e a prestação de serviços de pagamento, aprovado pelo DL 317/2009, de 30 de outubro, subsequentemente alterado e republicado com a denominação regime jurídico dos serviços de pagamento e da moeda eletrónica pelo DL 242/2012, de 7 de novembro, e, ainda, alterado pelo DL 141/2013, de 18 de outubro.**

**Atualmente vigora o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, aprovado pelo DL 91/2018, de 12 de novembro – alterado pelo DL 66/2023, de 8 de agosto, pela Lei 82/2023, de 29 de dezembro, e pela Lei 1/2025, de 6 de janeiro –, de ora em diante RJSPME. Tal como o anterior regime, também**

**vigente foi fruto de transposição de Diretiva, desta feita da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, também conhecida por *DSP revista* ou *DSP2*. O objeto de ambos os citados regimes que no tempo se sucederam é a regulação dos serviços de pagamento, incluindo das *relações entre prestadores* dos mesmos, *entre prestadores de serviços de pagamento e fornecedores de outros serviços ou bens* (que utilizam os serviços de pagamento para receber dos seus clientes), e, ainda, *entre prestadores de serviços de pagamento e utilizadores finais de serviços de pagamento* (que os utilizam para efetuar pagamentos de outros bens e serviços ou realizar outros tipos de transferências de fundos). Os conceitos acima referidos, que se reportam a atuações ilícitas de terceiros que tentam fazer-se passar por prestadores de serviços de pagamento, não têm lugar nos citados diplomas, nem foram afetados por eles.**

**Fechado este parênteses, muito singelamente concluímos que: *i.* no *phishing*, o lesado recebe um e-mail (ou outra mensagem digital, v.g. via SMS, MMS ou WhatsApp) com um *link* e, ao clicar neste, é direcionado para um *site* falso; *ii.* no *typosquatting*, espécie de *cybersquatting*, o lesado acede por lapso seu ao *site* falso, seja através de um motor de busca, seja pela errada digitação do endereço na respetiva barra; *iii.* no *pharming* o utilizador digita o endereço certo, ou escolhe o *site* certo, mas é redirecionado para o falso porque o seu *cache* de DNS foi previamente viciado por um vírus ou porque (caso muito raro) o próprio servidor de DNS foi atacado.**

**Todos estes tipos de fraude ou burla para terem credibilidade e eficácia carecem da prévia criação de uma cópia realista de um sítio da Internet.**

**<u>III.3.3. A relação contratual entre as partes</u>**

**A relação entre as partes – autora e banco réu – tem na sua origem num *contrato de abertura de conta* (também designado por *contrato de conta bancária* – José A. Engrácia Antunes, *Direito dos Contratos Comerciais*, Almedina, 2009, pp. 483 e ss.). Trata-se de um contrato celebrado entre um banco e um seu cliente que enquadra e disciplina uma relação duradoura entre as partes e no âmbito do qual irão surgir outros contratos que implicam existência e movimentação de fundos (na maioria dos casos haverá, pelo menos, um contrato de depósito bancário, podendo também existir, apenas ou cumulativamente, um contrato de conta-corrente bancária ou uma de várias espécies de contratos de crédito). De acordo com esta nossa noção, consentânea com outras que encontramos na doutrina e na jurisprudência, o modelo em causa tem as características de um *contrato-quadro* (sobre esta categoria contratual genérica, Maria Raquel de Almeida Graça Silva Guimarães, *O contrato-quadro no âmbito da utilização de meios de pagamento eletrónicos*, Coimbra Editora,**

**2011).**

**III.3.4. O contrato acessório de *homebanking***

**Outros acordos contratuais podem, ainda, surgir no âmbito da relação bancária, como acessórios do contrato génese de abertura de conta, ou de um dos demais referidos. É esse o caso do vulgarmente designado *contrato de homebanking*.**

**O *homebanking* – também designado por *online banking*, *internet banking*, *e-banking*, banca ao domicílio, banca eletrónica, banco *online* – consiste num sistema de canais digitais disponibilizado pelo banco via Internet que permite aos clientes obter informações sobre a sua conta bancária, efetuar transferências e pagamentos, entre outras operações bancárias, e que tradicionalmente apenas eram feitas "ao balcão", nos espaços físicos de agências e sucursais.**

**O contrato de *homebanking* é um contrato acessório do de conta bancária e que regula os direitos e deveres das partes no acesso e movimentação da(s) conta(s) bancária(s) pelo cliente bancário através de canais digitais disponibilizados pelo banco. Apesar de a lei não lhe atribuir um nome nem um conjunto concentrado de regras que o visem em exclusivo, é já um tipo social bem reconhecido na comunidade jurídica, e na sociedade em geral, por força da sua frequente e generalizada repetição na prática bancária, e pelo sequente tratamento que tem na doutrina – v.g., além dos textos supra citados, Calvão da Silva, «Conta corrente bancária, operação não autorizada e responsabilidade civil, STJ, Acórdão de 18 de dezembro de 2013», *Revista de Legislação e de Jurisprudência*, Ano 144, n.º 3991 (mar.-abr. 2015), pp. 290-326, Bruno Silva Palhão, «Os serviços de pagamento e as operações não autorizadas», *Cadernos de Direito Privado*, n.º 65 (jan.-mar. 2019), pp. 3-17, Hugo Luz dos Santos, «Plaidoyer por uma "distribuição dinâmica do ónus da prova" e pela "teoria das esferas de risco" à luz do recente Acórdão do Supremo Tribunal de Justiça, de 18/12/2013 , o (admirável) "mundo novo" no homebanking?», *O Direito*, Ano 147, n.º 3 (2015), pp.715-743 –, e na jurisprudência (v.g., Ac. STJ de 23/01/2024, proc. 379/21.0T8FAR.E1.S1, Cons. Nelson Borges Carneiro).**

**Apesar de legalmente atípico, não deixa de se encontrar regulado a um nível de abstração mais elevado, no já referido RJSPME, quando utilizado como *serviço de pagamento*. De notar que o serviço de *homebanking* não implica necessariamente serviços de pagamento, podendo ser contratado com âmbito mais restrito de consulta de dados e transferências entre contas do mesmo titular. Geralmente, porém, e no caso dos autos assim foi, por via do contrato de *homebanking*, o banco disponibiliza a possibilidade de o utilizador lhe dar ordens, e o utilizador tem o direito de exigir do banco a execução das ordens que lhe dá por via da plataforma eletrónica.**

**No caso dos autos, a autora, que já tinha um contrato de conta**

**bancária com o banco réu desde 1993, aderiu aos canais digitais em 2010, assumindo ambas as partes um conjunto de deveres relativos a esta nova relação.**
**Além de deveres legais a que adiante nos referiremos, as partes acordaram por escrito que, *para aceder aos Canais Diretos, a autora teria de se identificar perante o operador do canal em causa; que o banco, a pedido da autora emitiria um Cartão de Acesso aos Canais Diretos, que consiste num elemento de identificação secreto, pessoal, único e intransmissível, do qual constam dois códigos de acesso ao serviço: o número de adesão e uma chave alfanumérica; e, ainda, um Código Secreto (PIN), único, pessoal e intransmissível, composto por seis dígitos. Pelo mesmo documento, a autora aceitou que qualquer pessoa que dispusesse dos códigos de acesso teria acesso à conta D/O da autora e às contas e produtos a ela associados, bem como a outras contas bancárias e produtos de que seja titular e com poderes suficientes para as movimentar, podendo realizar quaisquer operações, nomeadamente, pedidos de débito, pedidos de crédito, resgates ou constituição de aplicações, independentemente das condições de movimentação constantes das respetivas fichas de abertura de conta* (facto 38).**
**Mais acordaram que a *conta D/O pode ser movimentada, a débito, por terceiros a quem tenham sido atribuídos, pelos respetivos titulares, poderes para o efeito* (facto 39).**
**<u>III.3.5. A situação litigiosa e análise de responsabilidades à luz do ordenamento aplicável</u>**
**Relembramos que a autora entrou num *site* que não era o do banco réu, tinha outro endereço, pertencia a um terceiro. Mais, a autora, ou digitou o nome desse terceiro, Novo Hanco, por engano, ou escolheu o site desse terceiro que lhe surgiu quando digitou Novo Banco no motor de busca, e, quando entrou no dito *site*, não cuidou de verificar o endereço. Endereço que constava como *novohanco*, não *novobanco*. Apenas a autora pode ser responsável pela entrada num *site* alheio desta forma e pela permanência nele. Ainda assim, se tivesse entrado, lido o endereço na barra de endereços e saído, nenhum mal lhe teria sucedido.**
**Porém, a atuação da autora foi muito além desta negligente entrada. A autora, contra todas as regras contratuais e legais, facultou a terceiros, com quem interagiu através do dito site, dados pessoais e intransmissíveis associados aos seus canais digitais – número de adesão e código secreto (PIN) de seis dígitos –, e facultou, ainda, na sequência de pedido formulado pelo dito site, um endereço de correio eletrónico.**
**Depois, foram-lhe pedidas por email 3 posições do cartão matriz e a introdução de código enviado por telemóvel e a autora, sem qualquer motivo para isso, facultou.**
**No SMS que recebeu lia-se «novobanco Online. Transferências Imediatas. ATENÇÃO: Não divulgue este código a terceiros, nem**

**através de chamadas telefónicas. Valor: 1,00 EUR para IBAN ES43 …69. Acum. Dia: 1,00 EUR (…)».**
**A autora, apesar de não ter solicitado nenhuma transferência acedeu em, por email, como lhe tinha sido pedido, informar o código recebido por SMS e as três solicitadas posições do cartão matriz.**
**A responsabilidade do banco réu nesta atuação e nas consequências da mesma é nula.**
**Do lado do banco a operação decorreu dentro da normalidade e regular funcionamento dos sistemas: a transferência imediata de 1 € foi executada e validada com recurso a todas as credenciais de segurança (autenticação forte do cliente): *i.* PIN de acesso aos canais digitais, composto por seis dígitos; *ii.* 3 (três) posições aleatórias do Cartão Matriz; e, *iii.* código de seis dígitos enviado por SMS para o número de telemóvel da autora (…27) – um código único e irrepetível, gerado automaticamente para cada transação.**
**Com estas credenciais, ao realizar-se uma transferência, pode certificar-se o beneficiário, e foi o que sucedeu, até ao limite de € 20.000. Do ponto de vista do banco réu, de acordo com os seus sistemas operacionais e funcionais, tudo se passa como se todas as credenciais tivessem sido introduzidas pela mão da autora, pois apenas esta tinha acesso àquelas credenciais, estava obrigada a não as divulgar, e tinha contratualmente aceitado que, se o fizesse, se divulgasse as credenciais, quem as tivesse teria total acesso à conta (v. condições contratuais do acesso aos canais digitais). Certificado que estava o beneficiário da transferência, e na posse do PIN de seis dígitos que a autora lhe forneceu, foi realizada a segunda transferência imediata, no valor de € 4.999,00, da mesma conta da autora para a mesma conta beneficiária. Para o banco réu, uma vez mais, tudo se passou como se tivesse sido o dedo da autora a introduzir os dados. Que mais deveria o banco réu ter feito para evitar a situação, além de tudo o que fez (contratação clara sobre os deveres e responsabilidades da autora relativos à guarda e utilização das credenciais, informação sobre os *modi operandi* das transferências, avisos constantes sobre esquemas fraudulentos)? Não só não se encontram deveres que a entidade bancária não tenha cumprido, como a mesma estava obrigada, por contrato e por lei, a acatar e executar as ordens que lhe foram transmitidas.**
**<u>III.3.6. Aplicação às transferências em causa nos autos do RJSPME (DL 91/2018)</u>**
**As transferências bancárias efetuadas pela autora e/ou com as suas credenciais, em 13/06/2022, via *homebanking*, qualificam-se como operações de pagamento para efeitos de aplicação do citado Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, aprovado pelo DL 91/2018 (RJSPME).**
**Com efeito, os «serviços de pagamento» estão listados no artigo**

**4.º destacando-se, para o que ora releva, a *execução de operações de pagamento, incluindo a transferência de fundos depositados numa conta de pagamento aberta junto do prestador de serviços de pagamento do utilizador* ou de outro prestador de serviços de pagamento, e o envio de fundos. Por seu turno, uma «conta de pagamento», para efeitos de aplicação do diploma, é uma *conta detida em nome de um ou mais utilizadores de serviços de pagamento, que seja utilizada para a execução de operações de pagamento* (al. g) do artigo 2.º, que contém uma longa lista de definições). Finalmente, uma «operação de pagamento» é um *ato*, iniciado pelo ordenante ou em seu nome, ou pelo beneficiário, de *depositar, transferir ou levantar fundos*, *independentemente de quaisquer obrigações subjacentes entre o ordenante e o beneficiário* (al. ii) do artigo 2.º). Se a operação de pagamento for iniciada através da Internet ou através de um dispositivo que possa ser utilizado para comunicação à distância designa-se «operação de pagamento remota» (al. kk) do artigo 2.º).**

**Recordando os factos, em especial os descritos sob os n.ºs 3, 4 e 22 a 27, e relacionando-os com as definições do RJSPME acima referidas, concluímos, conforme adiantámos, que as transferências bancárias efetuadas pela autora em 13/06/2022 se qualificam como *operações de pagamento* para efeitos de aplicação do citado Regime.**

**O acesso "em linha" (online, via Internet, por canais digitais) à conta de pagamento e as operações possíveis por essa via são referenciadas nos artigos 104.º a 107.º, relativos à autenticação, à confirmação da disponibilidade de fundos, aos serviços de iniciação de pagamento, e ao acesso às informações sobre a conta de pagamento e à sua utilização em caso de serviços de informação sobre contas.**

**III.3.7. Autenticação forte**

**A autenticação forte do cliente é necessária em três situações: no *acesso* à sua conta de pagamento; quando *inicia* uma operação de pagamento eletrónico; e quando realiza uma ação, através de um canal remoto, que *possa envolver um risco de fraude* no pagamento ou de outros abusos (n.º 1 do artigo 104.º do RJSPME). O n.º 7 do mesmo artigo expressa que tudo quanto nele disposto está sujeito aos termos do ato delegado da Comissão Europeia que adota as normas técnicas de regulamentação, ao abrigo do disposto o n.º 1 do artigo 98.º da Diretiva (UE) 2015/2366, do Parlamento Europeu e do Conselho, de 25 de novembro de 2015. Esse ato é constituído pelo Regulamento Delegado (UE) 2018/389 da Comissão, de 27 de novembro de 2017, que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas à *autenticação forte do cliente* e às normas abertas de comunicação comuns e seguras. Nos termos do artigo 13.º do Reg. Delegado (UE) 2018/389, epigrafado**

**«Beneficiários fiáveis», *os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente, sob reserva do cumprimento dos requisitos gerais de autenticação, sempre que o ordenante inicie uma operação de pagamento a favor de um beneficiário constante de uma lista de beneficiários de confiança previamente criada pelo primeiro* (n.º2).**

**Concluímos, portanto, tal como de resto fez o tribunal *a quo*, que a atuação do banco réu não violou nenhuma disposição legal que exigisse uma autenticação forte para a realização da segunda operação de transferência de fundos, no valor de 4.999 €, uma vez que foi utilizada autenticação forte para a inserção do beneficiário da primeira transferência como beneficiário certificado, fiável.**

**III.3.8. Mais alguns deveres das partes**

**Entre as obrigações do prestador de serviços de pagamento associadas aos instrumentos de pagamento encontramos, em primeiro lugar, a de assegurar que as credenciais de segurança personalizadas do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento (al. a) do n.º 1 do artigo 111.º do RJSPME). O banco réu cumpriu. A autora, por seu turno, enquanto utilizadora de serviços de pagamento tinha o dever de *tomar todas as medidas razoáveis para preservar a segurança das suas credenciais de segurança personalizadas* (artigo 110.º, n.º 2, do RJSPME). A autora incumpriu grosseiramente este dever e, não só não tomou as medidas razoáveis para preservar a segurança das suas credenciais de segurança personalizadas, como as facultou a desconhecidos, colocando-as em parte numa página de internet que não pertencia ao banco réu (o que a autora facilmente poderia ter detetado se tivesse lido o endereço da página em que entrou), e noutra parte enviando-as por email (!), para um endereço de email que não podia saber pertencer ao banco. E ainda que pertencesse, seria um procedimento absolutamente anómalo, inexistente em qualquer sistema de acesso a conta bancária via *homebanking*.**

**Entre as obrigações da autora, como utilizadora de serviços de pagamento com direito a utilizar um instrumento de pagamento contam-se a utilização do mesmo instrumento de acordo com as condições que regem a sua emissão e utilização, as quais têm de ser objetivas, não discriminatórias e proporcionais (al. a) do n.º 1 do artigo 110.º do RJSPME).**

**A autora violou todas as regras de utilização. Apenas depois de entrar num qualquer site, sem ter o cuidado de verificar que se tratava efetivamente do site do banco réu, de aí introduzir parte das suas credenciais, de enviar para um qualquer endereço de email posições do cartão matriz e um código que lhe chegou por SMS para uma transferência que não solicitou e de, mais tarde nesse dia, verificar um débito de 4.999 €, a autora comunica ao**

**banco que não reconhecia aquela transferência.**
**A autora foi enganada, mas perante o banco, a transação foi autorizada pela autora. E de facto, a autora – ainda que se conceda que não estaria consciente do que estava a fazer – autorizou os movimentos que põe em causa nestes autos, foi com as suas credenciais, que cedeu e porque as cedeu a terceiros, que as transações foram feitas. Só a autora (e sem prejuízo da responsabilidade do *typosquatter*) é responsável pelo uso das suas credenciais que, note-se, não lhe foram roubadas, nem furtadas, e que nem sequer perdeu. Facultou-as, deu-as a terceiros, inserindo-as num email desconhecido e numa página de Internet desconhecida.**
**As ordens foram, portanto, autorizadas e consentidas (artigos 103.º, n.ºs 1 a 3, 104.º, do RJSPME, e 13.º do Regulamento Delegado (UE) 2018/389).**
**Quando o banco réu soube que a autora não reconhecia o movimento de 4.999 €, imediatamente cancelou os acessos da autora aos canais digitais, como era seu dever (artigo 111.º, n.º 1, al. e) do RJSPME).**
**O banco réu cumpriu todas as suas obrigações, nomeadamente, a de executar as ordens que a autora, cidadã na posse de total capacidade jurídica, autorizou e consentiu. Lembramos que, estando reunidas todas as condições previstas no contrato-quadro celebrado com o ordenante, o prestador de serviços de pagamento que gere a conta deste não pode recusar a execução de uma ordem de pagamento autorizada (artigo 120.º do RJSPME), ordem que, quando foi, e bem, executada pelo banco, era irrevogável (artigo 121.º do RJSPME).**
**Provou-se que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo banco réu. A prova destas circunstâncias recai sobre o prestador de serviço de pagamento caso o utilizador negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada (artigo 113.º, n.º 1, do RJSPME). No caso, a autora negou ter autorizado a operação, mas provou-se que a autorizou, pelo que nem teria o réu de fazer prova das aludidas circunstâncias.**
**A autora utilizou as credenciais que o banco lhe forneceu para aceder ao *homebanking* com frontal incumprimento dos seus deveres contratuais e legais, dando-as a terceiros de uma forma, mais que incauta, despropositada e contraditória com a lógica do sistema de segurança para que as credenciais servem.**
**O recurso procede plenamente e a ação proposta pela autora é totalmente improcedente.**

**IV. Decisão**
**Face ao exposto, acordam os juízes desta Relação em julgar a**

**apelação procedente e, revogando a sentença, julgam a ação totalmente não provada e improcedente, absolvendo o réus de todos os pedidos.**
**Custas pela autora.**

**Lisboa, 13/03/2025**
**Higina Castelo**
**João Paulo Raposo**
**Laurinda Gemas**