Acórdão do Tribunal da Relação de Lisboa

Processo:	**344/21.8T8AGH.L1-2**
Relator:	**CARLOS CASTELO BRANCO**
Descritores:	**CONTRATOS BANCÁRIOS** **HOMEBANKING** **PHISHING** **RESPONSABILIDADE PELO PAGAMENTO**
Nº do Documento:	**RL**
Data do Acordão:	**13-10-2022**
Votação:	**UNANIMIDADE**
Texto Integral:	**S**
Texto Parcial:	**N**
Meio Processual:	**APELAÇÃO**
Decisão:	**IMPROCEDENTE**
Sumário:	**I) Autónomo, mas interdependente em relação a outros contratos bancários, inserindo-se, normalmente, no âmbito de um contrato-quadro de abertura de conta, da celebração do acordo de *"homebanking"* decorre uma complexidade de direitos e deveres que regulam a relação obrigacional, duradoura, entre as partes, relativamente ao utilizador e prestador de serviços de pagamento, constituindo uma das funcionalidades habituais desse acordo, a da possibilidade de o cliente bancário poder realizar e ordenar ao seu banco a realização de operações de pagamento.** **II) De harmonia com o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (abreviadamente RJSPME, aprovado pelo D.L. n.º 317/2009, de 30 de outubro, alterado pelo D.L. n.º 242/2012, de 7 de novembro e pelo D.L. n.º 157/2014, de 24 de outubro, que transpôs para a ordem jurídica portuguesa a Diretiva 2007/64/CE, regime jurídico este que, por força da transposição para a ordem jurídica portuguesa da Diretiva (UE) 2015/2366, do Parlamento Europeu e do Conselho, de23 de novembro de 2015, pelo D.L. n.º 91/2018, de 12 de novembro, veio a ser revogado ulteriormente) que, à data dos factos, regulava os deveres inerentes a cada uma das partes celebrantes do acordo respetivo:** **a) Constituem deveres do utilizador dos serviços de pagamento os de:** **- Utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, devendo tomar todas as medidas razoáveis, em especial ao receber um instrumento de pagamento, para preservar a eficácia dos seus dispositivos de segurança personalizados;** **- Comunicar, sem atrasos injustificados, ao prestador de serviços de pagamento ou à entidade designada por este último, logo que deles tenha conhecimento, a perda, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento; e** **b) Constituem obrigações do prestador de serviços de pagamento associadas aos instrumentos de pagamento, as seguintes:** **- Assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de**

serviços de pagamento que tenha direito a utilizar o referido instrumento (sem prejuízo das obrigações do utilizador do serviço de pagamento);
- Abster-se de enviar instrumentos de pagamento não solicitados, salvo quando um instrumento deste tipo já entregue ao utilizador de serviços de pagamento deva ser substituído;
- Garantir a disponibilidade, a todo o momento, de meios adequados para permitir ao utilizador de serviços de pagamento proceder à notificação de comunicação de perda, roubo, apropriação abusiva ou utilização não autorizada do instrumento de pagamento ou de solicitação de desbloqueio nos termos do n.º 4 do artigo 66.º do RGSPME;
- Facultar ao utilizador do serviço de pagamento, a pedido deste, os meios necessários para fazer prova, durante 18 meses após a notificação de comunicação de perda, roubo, apropriação abusiva ou utilização não autorizada do instrumento de pagamento, de que efetuou essa notificação; e
- Impedir qualquer utilização do instrumento de pagamento logo que a notificação da mencionada comunicação tenha sido efetuada.
III) À entidade bancária cabe, a título principal, aceitar os sucessivos mandatos para pagamentos emitidos mediante a correta autenticação por parte do cliente, nos limites do saldo disponível da conta à ordem, ou na medida em que tenha sido previsto anteriormente a possibilidade de realizar operações a descoberto, ou do crédito concedido nos casos de abertura de crédito.
IV) Como dever secundário acessório desta prestação principal, o banco deve entregar ao utilizador o cartão matriz e todos os códigos de acesso necessários à utilização do serviço de banca eletrónica, o que constitui um pressuposto essencial do acesso legítimo ao serviço uma vez que, sem os dispositivos de segurança personalizados na sua posse, o utilizador não consegue aceder ao serviço online.
V) Todavia, os referidos meios – possibilitando a Internet, designadamente, o anonimato, a celeridade de transações e atividades transfronteiriças – são frequentemente alvo de ataque, pelos vulgarmente designados "hackers", com objetivo de se apropriarem, de forma ilícita, dos fundos existentes nas contas bancárias, através de diversos esquemas fraudulentos, como, entre outros, o *"phishing"* e o "*pharming"*.
VI) Estas duas 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 eletrónico, no *"pharming"* (modalidade mais perigosa que a anterior, por surgir de forma quase impercetível), 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.
VII) Dado que, apenas o banco, enquanto prestador do serviço de pagamentos pode assegurar a operacionalidade do complexo sistema informático utilizado e a regularidade do seu funcionamento, garantindo, também, a confidencialidade dos dispositivos de segurança que permitem aceder ao instrumento de pagamento, tem o prestador do serviço de pagamento o ónus de provar que as ordens de pagamento dadas pelo cliente foram devidamente autorizadas através da utilização efetiva dos mecanismos de autenticação disponibilizados, bem como foram corretamente registadas e contabilizadas, e que a sua execução foi isenta de qualquer avaria técnica ou devido a deficiência do serviço prestado pelo prestador de serviços de pagamento, tendo o ónus de provar a ocorrência de comportamento negligente, gravemente negligente ou doloso do utilizador (cfr. artigo 70.º e 72.º do RJSPME).
VIII) Se tal prova não for realizada pela instituição bancária, a mesma será responsável pelo imediato pagamento – que se não for efetuado terá as consequências a que se refere o n.º 2 do artigo 71.º do RJSPME – do montante da operação de pagamento não autorizada, repondo a conta na situação em que estaria se a operação de pagamento não autorizada, não tivesse sido executada (cfr. artigo 71.º, n.º 1, do RJSPME).
IX) Se, ao invés, for apurada responsabilidade do ordenante por operações de pagamento não autorizadas, regerá o citado artigo 72.º do RJSPME, dispondo que:
- Se as operações de pagamento não autorizadas resultantes de perda, de roubo ou da apropriação abusiva de instrumento de pagamento, com quebra da confidencialidade dos dispositivos de segurança personalizados for imputável ao ordenante, este suporta as perdas relativas a essas operações dentro do limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, até ao máximo de (euro) 150;
- Se as perdas forem devidas a atuação fraudulenta ou ao incumprimento deliberado de uma ou mais obrigações previstas no artigo 67.º, o ordenante suporta todas as perdas resultantes de operações de pagamento não autorizadas (sem que seja aplicável o referido limite do saldo disponível ou da linha de crédito associada à conta/instrumento de pagamento);
- Se ocorrer negligência grave 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/ instrumento de pagamento, ainda que superiores a (euro) 150, dependendo da natureza dos dispositivos de segurança personalizados do instrumento de pagamento e das

circunstâncias da sua perda, roubo ou apropriação abusiva.
X) 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 (a autora) 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 (2 posições de coordenadas, que respeita ao cartão matriz, aviso que o banco disponibilizava no seu *site* e que constava aposto no cartão matriz), mas que, ao invés, divulga 50% das 72 coordenadas do cartão matriz.

Decisão Texto Parcial:
Decisão Texto Integral:

Acordam na 2.ª Secção do Tribunal da Relação de Lisboa:
*****
1. Relatório:
*****
1. NC, UNIPESSOAL, LDA., identificada nos autos, instaurou a presente ação declarativa, de condenação, sob a forma comum contra CAIXA ECONÓMICA MONTEPIO GERAL – Caixa Económica Bancária, S.A., também identificada nos autos, pedindo a condenação da ré a *"pagar-lhe a quantia de 22.497,00€, fraudulentamente retirada da conta bancária da A., com o número …, acrescida de juros desde a sua citação, até integral e efetivo pagamento".*
Para tanto, alegou, em suma, que:
- Desde 2011 é titular de uma conta de depósito à ordem domiciliada na agência da Ré em Angra do Heroísmo, movimentada por cartão de débito e acesso ao netbank pelo serviço designado por NET24;
- Em novembro de 2015 quando acedeu à página de homebanking foi direcionada para uma página de Internet previamente forjada e em tudo idêntica à página oficial da Ré, solicitando a atualização do cartão matriz e/ou a indicação de determinadas coordenadas do mesmo;
- Com o seu preenchimento, pessoa ou pessoas cuja identidade não foi possível apurar usaram as credenciais de acesso da Autora para realizar várias transferências bancárias no valor global de 22.497,00€ (vinte e dois mil quatrocentos e noventa e sete euros) contra a vontade e prejuízo daquela;
- Quando tomou conhecimento do sucedido o representante legal da Autora dirigiu-se à Ré para proceder ao cancelamento das aludidas transferências, o que não sucedeu;
- A Autora solicitou vária informação à Ré e esta não colaborou, tendo só conhecimento que as transferências foram realizadas via homebanking na sequência de processo crime;

- As transferências em causa só foram possíveis pela falta de segurança garantida pela Ré, que à data não fornecia a segurança SMS TOKEN, pelo que a mesma deverá ser responsabilizada pelo dano patrimonial sofrido pela Autora.
*****
2. Citada, a ré contestou, excecionando a incompetência relativa do Tribunal e impugnando os factos alegados pela autora, alegando, em suma, que:
- Para realização de uma transferência através do serviço homebanking o utilizador tem de efectuar o login, na página da internet da Ré, colocar a sua password, selecionar a operação e colocar as duas coordenadas do seu cartão matriz, pelo que um acesso à primeira tentativa sem erro, comprovou a identidade do ordenante e obriga a Ré a realizar a transferência em causa;
- A Autora confessa que por meio do seu sócio gerente acedeu a uma página não oficial e facultou as coordenadas do seu cartão matriz o que revela uma negligência grave no cuidado e tratamento dos meios de pagamento da Autora, pelo que as transferências em causa se deveram por actuação apenas imputável ao Sr. NC;
- Nos termos do contrato a Autora e o seu Sócio Gerente comprometeram-se a utilizar este meio de pagamento de acordo com as instruções e normas de segurança emitidas pela Ré;
- O sistema da Ré não foi alvo de qualquer intrusão e nunca solicitou qualquer actualização de dados nos termos sustentados pela Autora, sendo que no próprio cartão matriz está escrito «nunca indique mais do que 2 dígitos deste Cartão Matriz».
*****
3. A autora - nos termos do requerimento de 15-09-2021 - pronunciou-se no sentido da improcedência da exceção invocada pela ré.
*****
4. Foi julgada não verificada a exceção de incompetência territorial do Tribunal e teve lugar audiência prévia, sendo elaborado despacho saneador, com fixação do objeto do litígio e enunciação dos temas da prova.
*****
5. Teve lugar audiência de discussão e julgamento, com produção probatória, na sequência do que, em 06-04-2022, foi proferida sentença a julgar improcedente a ação, absolvendo a ré de todos os pedidos.
*****
6. Não se conformando com a referida sentença, dela apela a autora, pugnando pela procedência do recurso, com revogação da decisão recorrida e sua substituição por outra que condene a ré "*na restituição das quantias ilegitimamente apropriadas por terceiros, devido às fragilidade que sistema informático do banco apresentava à data dos factos*", tendo formulado as seguintes

conclusões:
"(…) I - A decisão proferida pelo tribunal a quo padece de vício de erro, no que se refere ao julgamento da matéria de facto.
II - Com o devido respeito, os factos constantes das alíneas d) e e) da matéria de facto foram indevidamente julgados como não provados, sendo que a prova produzida nos autos não permitia chegar a essa conclusão.
II - O sistema informático da recorrida apresentava, à data dos factos, fragilidades que possibilitaram a intromissão de terceiros na conta da recorrente.
IV - Isto porque, à data dos factos, o banco recorrido não adotava a medida de segurança SMS token.
V - A adoção desta medida estava perfeitamente ao alcance da recorrida, sendo, aliás, recomendada pela autoridade reguladora europeia, nas suas Orientações sobre Serviços de Pagamento (autenticação forte do cliente).
VI - Por outro lado, não se logrou provar como e por que motivo terão terceiros acedido à conta da recorrente, antes de o representante legal haver introduzido as suas credenciais.
VII - Pelo que não se poderá concluir, sem sombra de dúvidas, que a falha de segurança se deu no computador da recorrente, pela atuação do representante legal desta.
VIII - O representante legal da recorrente, ao atuar da forma descrita nos autos agiu sem culpa, pois que introduziu os seus dados inadvertidamente numa página web em tudo idêntica à do banco recorrido, fazendo-lhe crer que estava na página web verdadeira.
IX – A confiança do representante legal da recorrente foi reforçada pelo facto de, ao aceder à página de homebanking da recorrida, pôde logo consultar o seu saldo atual e movimentos, facto que deveria ter sido devidamente atendido e, atentas as declarações de parte da recorrida, dado como provado.
X – O risco subjacente a ataques informáticos, ao abrigo do contrato-quadro celebrado entre recorrente e recorrida corre por conta do banco recorrido, quer por força do disposto no art.º 796.º do CC, quer por força do disposto nos artigos 70.º e 71.º do RJPSME, na versão em vigor à data dos factos.
XI – Cabia ao banco recorrido provar que a conduta da recorrente, ao fornecer dados através da página em tudo idêntica à sua, era gravemente negligente o que, atentos os fundamentos supra aduzidos não logrou fazer.
XII – A recorrente tomou as precauções devidas ao usar o serviço de homebanking do banco recorrido, na medida em que dispunha de antivírus atualizado e acedeu à página pelos meios habituais, verificando o endereço respetivo, facto que se impunha dar como comprovado (…)".
*****
7. A ré contra-alegou, pugnando pela improcedência do recurso e

manutenção da decisão recorrida, tendo concluído o seguinte:
"(…) A. Conforme começa por esclarecer a Meritíssima Juíza a quo, a Recorrida tinha "o ónus de fornecer a prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por qualquer outra deficiência."
B. Sem prejuízo do formulado na fundamentação das presentes alegações, é certo que a Recorrente não colocou em causa a Sentença em crise quanto ao conhecimento do seu Sócio Gerente sobre os mecanismos de segurança, validação de operações e cuidados a ter na utilização do meio de pagamento. [Facto provado n.º 28, 29 e 30]
C. De igual forma, resulta da prova produzida, que foram inseridas corretamente as coordenadas pessoais e intransmissíveis da Autora [Facto provado n. º27 e 31]
D. Mais resultando que o Sócio Gerente era o único conhecedor dessas credenciais [Facto provado n.º 20, 21, 22, 23, 24, 25 e 26]
E. A testemunha DC confirmou que o sistema do Banco Montepio não foi alvo de qualquer ataque informático e que as ordens transmitidas foram corretamente executadas [Facto provado n.º 34]
F. Informação corroborada pelo Documento n.º 7 junto com a Contestação, onde se encontram explanados os registos informáticos da correta execução e introdução das coordenadas associadas aos movimentos em crise nos presentes autos.
G. Resultando, assim que o sistema informático da Recorrida é seguro e as ordens transmitidas foram corretamente executadas. [Facto provado n.º 31 e 34]
H. Conforme esclareceu a Testemunha DC não poderá retirar-se uma qualquer fragilidade pela não adoção de mecanismos adicionais de segurança.
I. Na verdade, a obrigatoriedade da adoção de tal mecanismo apenas veio a surgir 3 anos depois dos factos com a aprovação do Decreto-Lei 91/2018, de 12 de novembro [Doc. 2 junto com a Contestação]
J. Tão só a introdução de tal mecanismo apenas adveio no seguimento da evolução tecnológica e simplificação da utilização do meio de pagamento e não, motivada por uma qualquer falha de segurança.
K. Ainda assim, em causa nos presentes autos não está a fragilidade do sistema informático como tenta passar a Recorrente, mas o cuidado na correta salvaguarda das suas credenciais.
L. Termos em que resulta provada a correta execução das ordens inseridas, com recurso às credenciais da Recorrente e a segurança do sistema informático do Banco Montepio.
M. Por outro lado, esclareceu a Meritíssima Juíza a quo que a Recorrida "Terá igualmente de provar que este último [Cliente] agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 67 [RSP]" [Anotações nossas]

N. Nessa medida resulta das declarações prestadas pelo Sócio Gerente da Recorrida que terá acedido a uma página fraudulenta, indicado o seu número de utilizador, password, e introduzindo as coordenadas o seu cartão matriz. [Facto provado n.º 43]
O. O que fez contrariando as obrigações contratualmente assumidas, as informações, e os avisos de segurança facultados pela Recorrida [Facto provado n.º 28, 29, 30, 31, 32, 33 e 35]
P. A acompanhar as declarações do Sr. NC, consta documentado que a Recorrente entregou uma declaração no balcão gestor onde indica que facultou as suas credenciais a terceiros. [Conforme fls. 51 da Certidão Judicial junta como Documento n.º 3 com a petição inicial]
Q. O que confirmou em declarações à P.S.P. e ao Ministério Público. [Conforme fls. 1, 2 e 35 da certidão judicial junta aos autos como Documento n.º 3 com a petição Inicial]
R. Contrariando os avisos de segurança e os alertas de fraude que era identifico à situação que o Sócio Gerente descreve no seu depoimento. [Facto provado n.º 28, 29, 33 e 35]
S. Pelo que entende a Recorrida que o Tribunal a quo fez uma correta apreciação da prova e subsunção dos factos ao direito ao considerar que o Banco Montepio ilidiu a sua presunção de culpa nos termos do disposto no número 1 do artigo 799.º do C.C.
T. A atuação descrita do Sócio Gerente da Recorrente foi grosseiramente negligente porquanto contrariando a lógica de funcionamento do sistema, os avisos de segurança opta por facultar informação que estava obrigado a guardar sob segredo. [Artigo 67.º do Decreto-Lei 317/2009, de 30 de outubro]
U. Pelo que com o devido respeito, se a Recorrida opta por contrariar os deveres e indicações de segurança a que estava obrigado o risco das consequências que advém da utilização grosseiramente negligente terão de correr necessariamente por conta do utilizador deste meio de pagamento.
V. Neste sentido acompanha a eloquente fundamentação de direito formulada pela Meritíssima Juíza a quo:
"O sócio gerente da A ao fornecer o conteúdo do seu cartão matriz – apesar dos avisos no site da Ré quanto a fraudes e do aviso claro no próprio cartão matriz de não revelar mais do que dois algarismos – actuou com culpa e negligência grave/grosseira, colocando em causa as regras básicas da segurança.
Actuação essa não cautelosa, contrária ao bom pai de família, sendo-lhe plenamente exigível não só estar a par das informações fornecidas pela Ré quanto a fraudes, como também questionar incongruências lógicas - se o cartão refere que não posso colocar mais de dois dígitos, porque irei fornecer mais? – sendo bastante divulgado já na altura dos factos (pela comunicação social e redes sociais) a existência de fraudes informática e o zelo adicional que se deve possuir ao lidar com sites bancários e os dados e passwords pessoais.

Acresce que a cláusula 23.17, primeira parte, do contrato de homebanking que a autora celebrou com a ré consta, ipsis verbis, «O Cliente e o Representante comprometem-se, igualmente, a guardar sob segredo as suas Credenciais de Autenticação, bem como a prevenir adequadamente a sua utilização abusiva por parte de terceiros ». (sublinhado nosso).
Por sua vez, a clásula 23.20 sustenta « A responsabilidade do Cliente ou Representante por todas as operações irregulares efectuadas utilizando as Credenciais de Autenticação, ou através da utilização abusiva das mesmas, motivadas por perda, extravio, furto, roubo, falsificação ou outros meios de apropriação ilegítima, cessa no momento em que seja efectuada a comunicação acima referida, salvo se forem devidas a dolo e/ou negligência grosseira do Cliente, Representante ou Utilizador». (sublinhado nosso) Nos termos do disposto no artigo 67.º do R.S.P a Autora tinha a obrigação de utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização. Com a sua atuação violou de forma muito grave normas contratuais e legais expressas. A ré, por seu turno, demonstrou o bom funcionamento do sistema e as muitas medidas que tomou para que a autora tivesse efetivo conhecimento da forma como devia utilizar o cartão (nomeadamente que nunca lhe seriam pedidas mais do que duas posições do mesmo – frase que inclusive está escrita no cartão) e dos perigos de fraude mais comuns entre os quais visavam a mesma fraude de que a A foi alvo."
W. Nestes termos o Tribunal a quo efetuou uma correta apreciação da prova produzida e melhor subsunção jurídica dos factos ao direito, pelo que não merece a sentença recorrida qualquer reparo (…)".
*

8. Em 15-09-2022 foi proferido despacho de admissão liminar da apelação.
*

9. Foram colhidos os vistos legais.
*

<u>2. Questões a decidir:</u>
Sendo o objeto do recurso balizado pelas conclusões do apelante, nos termos preceituados pelos artigos 635º, nº 4, e 639º, nº 1, do CPC - sem prejuízo das questões de que o tribunal deva conhecer oficiosamente e apenas estando adstrito a conhecer das questões suscitadas que sejam relevantes para conhecimento do objeto do recurso - , as questões a decidir são:
*

<u>I) Impugnação da matéria de facto:</u>
A) Do não conhecimento do objeto do recurso atinente à impugnação da matéria de facto invocada na parte II (intitulada "Da inexistência de culpa na atuação do representante legal da recorrente"), nos pontos 63 e 64 e na conclusão IX, das alegações

de recurso
B) Se a matéria constante das alíneas d) e e) dos factos não provados deve ser dada como provada?
*****
II) Mérito do recurso:
C) Se não existiu culpa na atuação do representante legal da recorrente e se deve a ré ser condenada no pedido formulado pela autora?

*****
3. Fundamentação de facto:
*****
A DECISÃO RECORRIDA CONSIDEROU COMO PROVADA A SEGUINTE FACTUALIDADE:
1. A A. é titular, desde 2011, de uma conta na conta de depósito à ordem nº …, domiciliada na Caixa Económica Montepio Geral, pessoa coletiva nº 500792615, agência de Angra do Heroísmo, sita na Rua de São João, freguesia da Sé, Angra do Heroísmo, com o número ….
2. A conta de depósito à ordem era movimentada de cartão de débito e acesso ao netbank (private banking) pelo serviço designado por NET24.
3. No início de novembro de 2015, a A. através do seu sócio gerente Sr. NC, quando acedeu à página do homebanking da Caixa Económica Montepio Geral, foi direcionando para uma página de Internet previamente forjada e em tudo idêntica à página oficial daquela instituição, solicitando a atualização do cartão matriz e a indicação de determinadas coordenadas do mesmo.
4. Pessoa ou pessoas (hacker(s)) cuja(s) identidade(s) não foi apurada conseguiu, assim, que a A., na qualidade de cliente da Caixa Económica Montepio Geral fornecesse os seus códigos de ativação do serviço homebanking.
5. Após o que a pessoa ou pessoas cuja identidade não foi possível apurar, hacker(s), munido(s) das respetivas credenciais de acesso, obtidas de forma fraudulenta, acederam à conta bancária da A. como se se tratasse do seu verdadeiro titular, tomou conhecimento dos saldos bancários daquela conta e movimentou-a determinando, através da Internet, diversas transferências de valores, tudo sem o conhecimento, contra a vontade e em prejuízo da A..
6. Atuando desta forma, o indivíduo ou os indivíduos cuja identidade não foi possível apurar, hacker(s), com a intenção de obter vantagem patrimonial, conseguiram através do acesso ilegítimo, via internet, com utilização de meios informáticos, o acesso à conta bancária da A. e procederam a uma subsequente subtração de valores que aí se encontrassem, transferindo-os para contas bancárias, tituladas por si e por terceiros, sobre as quais

mantivesse algum tipo de domínio.
7. Tal pessoa, ou pessoas, acedeu ou acederam, assim, através do serviço de homebanking, à conta bancária titulada pela A. com o número 2131.10.605744-2., domiciliada no Montepio Geral, agência de Angra do Heroísmo, sem o conhecimento e contra a vontade do seu titular efetuando no dia 13 de novembro de 2015 e no dia 15 de novembro de 2015, respetivamente, 4 e 13 acessos ilegítimos / levantamentos / transferências internacionais, o que totaliza 17 acessos ilegítimos / levantamentos/ transferências internacionais para pagamento a pessoas desconhecidas, dos seguintes montantes:
I. 2015-11-13 PAG. SERV. 21547 400000067 €2.500,00
II. 2015-11-13 PAG. SERV. 21547 400000067 €2.499,00
III. 2015-11-13 PAG. SERV. 21547 400000066 €1.250,00
IV. 2015-11-13 PAG. SERV. 21547 400000068 €1.249,00
V. 2015-11-15 PAG. SERV. 21547 400000158 €2.250,00
VI. 2015-11-15 PAG. SERV. 21547 400000157 €2.250,00
VII. 2015-11-15 PAG. SERV. 21547 400000156 €250,00
VIII. 2015-11-15 PAG. SERV. 21547 400000155 €249,00
IX. 2015-11-15 PAG. SERV. 21547 400000156 €1.250,00
X. 2015-11-15 PAG. SERV. 21547 400000156 €500,00
XI. 2015-11-15 PAG. SERV. 21547 400000155 €750,00
XII. 2015-11-15 PAG. SERV. 21547 400000148 €2.000,00
XIII. 2015-11-15 PAG. SERV. 21547 400000147 €2.250,00
XIV. 2015-11-15 PAG. SERV. 21547 400000146 €250,00
XV. 2015-11-15 PAG. SERV. 21547 4000000146 €500,00
XVI. 2015-11-15 PAG. SERV. 21547 400000145 €1.250,00
XVII. 2015-11-15 PAG. SERV. 21547 400000144 €1.250,00
8. O Autor, no dia 16 de novembro de 2015, pelas 9:00h, ao aceder à sua conta bancária identificada em 1, verificou que tinham sido efectuados, sem o seu conhecimento e autorização, as transferências supra identificadas.
9. O sócio gerente da A, deslocou-se de imediato ao balcão da agência do Montepio na Rua de S. João, em Angra do Heroísmo, no sentido de serem canceladas as operações de pagamento de serviços.
10. O sócio gerente da A., entregou à Ré uma comunicação escrita a relatar o sucedido.
11. No dia 17 de novembro de 2015, ao saber-se que os movimentos tinham sido efetuados
para o BANIF, o Autor assinou uma declaração a autorizar a R. a reclamar junto do Banif os 17 movimentos fraudulentos da sua conta para esta instituição bancária.
12. A A. tentou obter junto da Ré informação relativa à sua conta quanto às datas de 13/11/2015 e 15/11/2015, nomeadamente os seguintes elementos:
I. "todos os registos informáticos referentes às movimentações da conta n.º 2131.10.605744-2.

II. todos os registos e logs referentes aos acessos informáticos através da internet à minha conta bancária nomeadamente números IP do(s) equipamento(s) informático(s) utilizados para esse efeito, data e hora de acessos e tempo de duração do acesso;
III. todos os registos das autorizações facultadas para todos os movimentos nas datas em questão;
IV. todos os registos de utilizadores, passwords, senhas utilizadas para os acessos à minha conta bancária nos dias em questão;
V. toda a informação adicional que entendam poder ser relevante para o apuramento da verdade nesta questão e identificação dos autores das acções de sonegação não autorizada e fraudulenta de fundos."

13. A A., no dia 16 de novembro de 2015, participou criminalmente contra desconhecidos relativamente ao sucedido processo que correu termos com o número …/…, MINISTÉRIO PÚBLICO - Procuradoria da República da Comarca dos Açores Departamento de Investigação e Ação Penal - Secção de Angra do Heroísmo, tendo o processo sido arquivado pelo seguinte: *"não obstante as diligências efetuadas, não se logrou apurar a identidade dos agentes dos factos denunciados, inexistindo quaisquer elementos que permitam aferir da identidade dos seus autores".*

14. Na sequência do processo crime acima identificado, é que R. veio aos autos informar que os levantamentos foram efetuados através do serviço homebanking – Net 24, com utilização dos IPs (internet protocole service) 212.83.40.239, 207.244.70.35, 79.172.193.32, 166,70.207.2 e 46.186.106.190, tendo a conta beneficiária sido a entidade 21547 do Banif SaBanco Internacional do Funchal, destacando-se:
I. O IP … foi utilizado às 19:00 do dia 13.11.2015, tendo como local de operação a Alemanha
II. O IP … foi utilizado às 19:02:54 do dia 13.11.2015, tendo como local de operação os EUA -Manassas
III. O IP … foi utilizado às 18:15 e às 20:02:44 do dia 15.11.2015, tendo como local de operação a Hungria -Budapeste
IV. O IP … foi utilizado às 00:13:43 e às 00:17:02 do dia 15.11.2015, tendo como local de operação a os EUA- Salt Lake City.
V. O IP … foi utilizado às 01:01:31 do dia 16.11.2015, tendo como local de operação a Holanda.

15. A informação solicitada em 12. não foi entregue pela Ré directamente à A

16. À data dos presentes factos, a Ré não fornecia aos seus clientes a segurança do SMS TOKEN.

17. A Ré é uma caixa económica cuja atividade se caracteriza pela prática de todos os atos, por lei, permitidos aos bancos.

18. A adesão da A ao sistema homebanking ocorreu no dia 18 de novembro de 2011 e activada a 6 de fevereiro de 2012.

19. Após novo pedido de adesão e renovação o Sr. NC, no dia 16

de janeiro de 2014 procedeu à activação do cartão matriz associado aos movimentos em causa neste processo, sendo inativado no dia 16 de novembro de 2015.
20. Foram atribuídos ao sócio gerente da A, pela Ré, códigos de acesso/credenciais de utilização.
21. Que à data dos factos funcionavam em 3 níveis de segurança, designadamente:
I. Número de utilizador;
II. Password;
III. Cartão matriz;
22. O número de utilizador correspondente ao número de cliente Montepio e pode ser personalizado.
23. A password, composta por seis dígitos, que após o primeiro login, tem de ser obrigatoriamente alterada por uma da autoria e do exclusivo conhecimento do cliente.
24. Por sua vez, o cartão matriz é composto por 72 posições, cada uma com 3 dígitos, para validação de operações passíveis de alterar o património detido pelos clientes, junto do Banco Montepio.
25. Cujo processo de produção é externo à Ré e não envolve qualquer atuação humana, uma vez que as coordenadas são geradas por computador.
26. Sendo remetido via CTT para o endereço dos clientes, e apenas passível de ser ativado mediante a validação de códigos de acesso ao Net24 (número de utilizador e password) adstrito ao cartão expedido.
27. Para a realização de uma operação com alterações patrimoniais, o utilizador teria de efetuar o login, na página da internet da Ré, colocar a sua password, selecionar a operação e colocar as duas coordenadas do seu cartão matriz, e só mediante a sua correta validação, é que se confere validade à ordem transmitida.
28. Foram explicados ao Sócio Gerente da A todos os procedimentos de segurança e de utilização do referido serviço.
29. A informação encontra-se disponível no site da Ré.
30. O sócio gerente da Ré é um utilizador frequente do sistema de pagamento homebanking, e desde a sua contratação que nunca nenhum evento similar ocorreu.
31. Os movimentos indicados, apenas foram possíveis porque, em cada um deles:
I. Foi introduzido o número de utilizador;
II. Foi introduzida a password – 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;
III. Foram introduzidas duas coordenadas do cartão matriz, que são sempre solicitadas de forma aleatória, pelo sistema e nunca repetidas.

32. Resulta do acordo celebrado entre a A, através do seu sócio gerente Sr. NC e a Ré, nas clausulas:

I. 23.17 «O Cliente e o Representante comprometem-se, igualmente, a guardar sob segredo as suas Credenciais de Autenticação, bem como a prevenir adequadamente a sua utilização abusiva por parte de terceiros. O Cliente é o único responsável por todos os prejuízos resultantes da utilização indevida do Serviço Montepio24 Empresas por parte de terceiros, com excepção do estabelecido no ponto 23.20.

II. 23.18. No caso de perda, extravio, furto, roubo, falsificação ou outros meios de apropriação ilegítima de Credenciais de Autenticação, ou, ainda, no caso de suspeita relativamente à utilização indevida das Credenciais de Autenticação, o Cliente ou o Representante deverão comunicar imediatamente ao Montepio tal facto, através do Serviço Montepio24 Empresas, via Phone24.

III. 23.19. O Cliente e o Representante autorizam a CEMG a efectuar o registo das suas comunicações e o respectivo arquivo em base de dados, nos termos permitidos por lei.

IV. 23.20. A responsabilidade do Cliente ou Representante por todas as operações irregulares efectuadas utilizando as Credenciais de Autenticação, ou através da utilização abusiva das mesmas, motivadas por perda, extravio, furto, roubo, falsificação ou outros meios de apropriação ilegítima, cessa no momento em que seja efectuada a comunicação acima referida, salvo se forem devidas a dolo e/ou negligência grosseira do Cliente, Representante ou Utilizador.»

33. Constava e consta no site institucional do Banco Montepio diversos avisos de segurança, nomeadamente:

I. «Nunca facultar a terceiros dados pessoais e identificativos, como os seus códigos ou outra informação que permita o acesso às suas contas bancárias online.».

II. «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».

III. «Não clique nos links de mensagens ou SMSs suspeitos. (…)».

IV. «Recordamos e alertamos para o facto de o Montepio apenas solicitar a indicação de posições do seu Cartão Matriz, pelo que, se lhe for solicitado que preencha o cartão completo ou qualquer outra combinação, deverá ser considerada como uma tentativa de fraude, devendo contactar de imediato a Linha Informativa Montepio, 808 20 26 26, disponível todos os dias do ano, entre as 07h00 e as 01h00.»

34. O sistema da Ré não foi alvo de qualquer intrusão ou ataque informático.

35. A Actualização do cartão matriz que a A se confrontou encontrava-se e encontra-se identificada no site institucional da Ré com o aviso “Exemplos de tentativa de Fraude”.

36. Consta do cartão matriz o seguinte: “Atenção: Nunca indique

mais do que 2 dígitos deste Cartão Matriz."
37. No dia 19/02/2016 a Ré remeteu um e-mail para o Banco Santander de forma a recuperar €2.250,00 por referência ao pagamento da referência ….
38. No dia 10/09/2015 a Ré remeteu um e-mail para o Banco Millennium BCP pedindo a devolução da quantia de € 440,00 por referência ao pagamento com a Referência ….
39. No dia 16/11/2015 remeteu à Direção de Auditoria Interna do Banif pedido de devolução da quantia de € 22.497,00 referente à totalidade dos 17 movimentos identificados pela Autora
40. Inicialmente, o BANIF respondeu no sentido que não seria possível proceder à devolução das quantias identificadas.
41. Contudo, no dia 17/11/2015 a DAI do Banif remete à DAI do Banco Montepio um email indicando que estaria em condições de devolver a quantia de € 7.750,00 pedindo, para o efeito a remessa de documentação.
42. O BANIF não logrou em efetuar o estorno da quantia indicada.
43. O sócio gerente da A, nos termos dos factos 3 e 4, preencheu 50% das coordenadas constantes do seu cartão matriz.
*****
<u>A DECISÃO RECORRIDA CONSIDEROU COMO NÃO PROVADA A SEGUINTE FACTUALIDADE:</u>
a) O sócio gerente da A teve conhecimento das aludidas transferências pelas 8.00h.
b) No dia estabelecido no ponto 9 o sócio gerente da A foi informado que o cancelamento das operações não seria possível.
c) A Ré não prestou colaboração à A.
d) O hacker aproveitou-se das fragilidades que o sistema de homebanking prestado pela Ré apresentava no seu serviço "Net 24".
e) As transferências em causa foram possíveis, unicamente pela falta de segurança garantida pela R.
*****
<u>4. Fundamentação de Direito:</u>
*****
<u>I) Impugnação da matéria de facto:</u>
Conclui a recorrente, na alegação de recurso –conclusões I) e II) – que a decisão do Tribunal recorrido, desde logo, que *o "tribunal a quo incorreu em erro de julgamento sobre a matéria de facto, ao dar como não provados os seguintes factos, que abaixo se transcrevem:*
"d) O hacker aproveitou-se das fragilidades que o sistema de homebanking prestado pela Ré apresentava no seu serviço "Net24".
e) As transferências em causa foram possíveis, unicamente pela falta de segurança garantida pela R."*, mais considerando que, da *"prova testemunhal produzida em audiência resultam elementos suficientes que revelam quer a existência de fragilidades no sistema

***de homebanking fornecido pela recorrida, quer o nexo de causalidade entre tais fragilidades e a verificação das transferências fraudulentas.”*, concluindo que, embora o tribunal recorrido concluísse pela não verificação de avaria técnica, não poderia ter dado como provada a *“inexistência de outras deficiências técnicas”* (cfr. pontos 2 a 7 da alegação de recurso). Convocou, designadamente, o depoimento da testemunha DC – que extratou nos pontos que considerou relevantes – e concluiu que: *“(…) da prova produzida e tendo em consideração todos os fundamentos aduzidos, impunha-se ao tribunal a quo dar como provados os factos d) e e) da matéria de facto não provada”* (cfr. ponto 38 da alegação de recurso).**

Com a alegação produzida, o recorrente/apelante pretende colocar em crise a factualidade apurada pelo Tribunal *a quo*.

No caso *sub judice*, a prova produzida em audiência foi gravada, pelo que, cumpre apreciar se deve este Tribunal *ad quem* proceder à reapreciação da matéria de facto impugnada.

Prescreve o artigo 639.º do CPC – sobre o ónus de alegar e de formular conclusões - nos seguintes termos:

“1 - O recorrente deve apresentar a sua alegação, na qual conclui, de forma sintética, pela indicação dos fundamentos por que pede a alteração ou anulação da decisão.

2 - Versando o recurso sobre matéria de direito, as conclusões devem indicar:

a) As normas jurídicas violadas;

b) O sentido com que, no entender do recorrente, as normas que constituem fundamento jurídico da decisão deviam ter sido interpretadas e aplicadas;

c) Invocando-se erro na determinação da norma aplicável, a norma jurídica que, no entendimento do recorrente, devia ter sido aplicada.

3 - Quando as conclusões sejam deficientes, obscuras, complexas ou nelas se não tenha procedido às especificações a que alude o número anterior, o relator deve convidar o recorrente a completá-las, esclarecê-las ou sintetizá-las, no prazo de cinco dias, sob pena de se não conhecer do recurso, na parte afetada.

4 - O recorrido pode responder ao aditamento ou esclarecimento no prazo de cinco dias.

5 - O disposto nos números anteriores não é aplicável aos recursos interpostos pelo Ministério Público, quando recorra por imposição da lei.”.

Por sua vez, dispõe o artigo 640.º do CPC que:

“1 - Quando seja impugnada a decisão sobre a matéria de facto, deve o recorrente obrigatoriamente especificar, sob pena de rejeição:

a) Os concretos pontos de facto que considera incorretamente julgados;

b) Os 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;
c) A decisão que, no seu entender, deve ser proferida sobre as questões de facto impugnadas.
2 - No caso previsto na alínea b) do número anterior, observa-se o seguinte:
a) Quando os meios probatórios invocados como fundamento do erro na apreciação das provas tenham sido gravados, incumbe ao recorrente, sob pena de imediata rejeição do recurso na respetiva parte, indicar com exatidão as passagens da gravação em que se funda o seu recurso, sem prejuízo de poder proceder à transcrição dos excertos que considere relevantes;
b) Independentemente dos poderes de investigação oficiosa do tribunal, incumbe ao recorrido designar os meios de prova que infirmem as conclusões do recorrente e, se os depoimentos tiverem sido gravados, indicar com exatidão as passagens da gravação em que se funda e proceder, querendo, à transcrição dos excertos que considere importantes.
3 - O disposto nos n.ºs 1 e 2 é aplicável ao caso de o recorrido pretender alargar o âmbito do recurso, nos termos do n.º 2 do artigo 636.º".
Assim, aos concretos pontos de facto, concretos meios probatórios e à decisão deve o recorrente aludir na motivação do recurso (de forma mais desenvolvida), sintetizando-os nas conclusões.
As exigências legais referidas têm uma dupla função: Delimitar o âmbito do recurso e tornar efetivo o exercício do contraditório pela parte contrária (pois só na medida em que se sabe especificamente o que se impugna, e qual a lógica de raciocínio expendido na valoração/conjugação deste ou daquele meio de prova, é que se habilita a contraparte a poder contrariá-lo).
O recorrente deverá apresentar *"um discurso argumentativo onde, em primeiro lugar, alinhe as provas, identificando-as, ou seja, localizando-as no processo e tratando-se de depoimentos a respectiva passagem e, em segundo lugar, produza uma análise crítica relativa a essas provas, mostrando minimamente por que razão se "impunha" a formação de uma convicção no sentido pretendido"* (assim, o Acórdão do Tribunal da Relação do Porto de 17-03-2014, Processo nº 3785/11.5TBVFR.P1, relator ALBERTO RUÇO).
Os aspetos de ordem formal devem ser modelados em função dos princípios da proporcionalidade e da razoabilidade (cfr. o Acórdão do STJ de 28-04-2014, P.º nº 1006/12.2TBPRD.P1.S1, relator ABRANTES GERALDES).
Não cumprindo o recorrente os ónus do artigo 640º, n.º 1 do C.P.C., dever-se-á rejeitar o seu recurso sobre a matéria de facto, uma vez que a lei não admite aqui despacho de aperfeiçoamento, ao contrário do que sucede quanto ao recurso em matéria de direito, face ao disposto no art. 639º, nº 3 do C.P.C. (cfr. Ac. do

Tribunal da Relação de Guimarães de 19-06-2014, P.º n.º 1458/10.5TBEPS.G1, relator MANUEL BARGADO).
Dever-se-á usar de maior rigor na apreciação da observância do ónus previsto no n.º 1 do art. 640.º (de delimitação do objeto do recurso e de fundamentação concludente do mesmo), face ao ónus do n.º 2 (destinado a possibilitar um acesso mais ou menos facilitado pela Relação aos meios de prova gravados relevantes, que tem oscilado em exigência ao longo do tempo, indo desde a transcrição obrigatória dos depoimentos até uma mera indicação e localização exacta das passagens da gravação relevantes) (neste sentido, Ac. do STJ de 29-10-2015, P.º n.º 233/09.4TBVNG.G1.S1, relator LOPES DO REGO).
O ónus atinente à indicação exata das passagens relevantes dos depoimentos gravados deve ser interpretado em termos funcionalmente adequados e em conformidade com o princípio da proporcionalidade, pelo que a falta de indicação, com exatidão, só será idónea a fundamentar a rejeição liminar se dificultar, de forma substancial e relevante, o exercício do contraditório, ou o exame pelo tribunal, sob pena de ser uma solução excessivamente formal, rigorosa e sem justificação razoável (cfr. Acs. do STJ, de 26-05-2015, P.º nº 1426/08.7CSNT.L1.S1, relator HÉLDER ROQUE, de 22-09-2015, P-º nº 29/12.6TBFAF.G1.S1, relator PINTO DE ALMEIDA, de 29-10-2015, P.º n.º 233/09.4TBVNG.G1.S1, relator LOPES DO REGO e de 19-01-2016, P.º nº 3316/10.4TBLRA-C1-S1, relator SEBASTIÃO PÓVOAS).
A apresentação de transcrições globais dos depoimentos das testemunhas não satisfaz a exigência determinada pela al. a) do n.º 2 do art. 640.º do CPC (neste sentido, Ac. do STJ de 19-02-2015, P.º nº 405/09.1TMCBR.C1.S1, relatora MARIA DOS PRAZERES BELEZA), o mesmo sucedendo com o recorrente que procede a uma referência genérica aos depoimentos das testemunhas considerados relevantes pelo tribunal para a prova de quesitos, sem única alusão às passagens dos depoimentos de onde é depreendida a insuficiência dos mesmos para formar a convicção do juiz (cfr. Ac. do STJ de 28-05-2015, P.º n.º 460/11.4TVLSB.L1.S1, relator GRANJA DA FONSECA).
Nas conclusões do recurso devem ser identificados com precisão os pontos de facto que são objeto de impugnação, bastando que os demais requisitos constem de forma explícita da motivação (neste sentido, Acs. do STJ de 19-02-2015, P.º nº 299/05.6TBMGD.P2.S1, relator TOMÉ GOMES, de 01-10-2015, P.º nº 824/11.3TTLRS.L1.S1, relatora ANA LUÍSA GERALDES, de 11-02-2016, P.º nº 157/12-8TVGMR.G1.S1, relator MÁRIO BELO MORGADO).
Note-se, todavia, que atenta a função do tribunal de recurso, este só deverá alterar a decisão sobre a matéria de facto se concluir que as provas produzidas apontam em sentido diverso ao

apurado pelo tribunal recorrido. Ou seja: *"I. Mantendo-se em vigor, em sede de Recurso, os princípios da imediação, da oralidade, da concentração e da livre apreciação da prova e guiando-se o julgamento humano por padrões de probabilidade e nunca de certeza absoluta, o uso, pelo Tribunal da Relação, dos poderes de alteração da decisão da 1ª instância sobre a matéria de facto só deve ser efectuado quando seja possível, com a necessária segurança, concluir pela existência de erro de apreciação relativamente a concretos pontos de facto impugnados. II: Assim, a alteração da matéria de facto só deve ser efectuada pelo Tribunal da Relação, quando este Tribunal, depois de proceder à audição efectiva da prova gravada, conclua, com a necessária segurança, no sentido de que os depoimentos prestados em audiência final, conjugados com a restante prova produzida, apontam em direcção diversa, e delimitaram uma conclusão diferente daquela que vingou na primeira Instância"* (assim, o Acórdão do Tribunal da Relação de Guimarães de 14-06-2017, Processo 6095/15T8BRG.G1, relator PEDRO DAMIÃO E CUNHA).

A insuficiência da fundamentação probatória do recorrente não releva como requisito formal do ónus de impugnação, mas, quando muito, como parâmetro da reapreciação da decisão de facto, na valoração das provas, exigindo maior ou menor grau de fundamentação, por parte do tribunal de recurso, consoante a densidade ou consistência daquela fundamentação (neste sentido, Ac. do STJ de 19-02-2015, P.º nº 299/05.6TBMGD.P2.S1, relator TOMÉ GOMES).

Contudo, *"não há lugar à reapreciação da matéria de facto quando o facto concreto objecto da impugnação for insusceptível de, face às circunstância próprias do caso em apreciação, ter relevância jurídica para a solução da causa ou mérito do recurso, sob pena de se levar a cabo uma actividade processual que se sabe, de antemão, ser inconsequente"* (assim, o Acórdão do Tribunal da Relação de Coimbra de 15-09-2015, Processo 6871/14.6T8CBR.C1, relator MOREIRA DO CARMO), sob pena de se praticar um acto inútil proibido por lei (cfr. artigo 130.º do CPC).

Estas as linhas gerais em que se baliza a reapreciação da matéria de facto na Relação.

*****

<u>A) Do não conhecimento do objeto do recurso atinente à impugnação da matéria de facto invocada na parte II (intitulada *"Da inexistência de culpa na atuação do representante legal da recorrente"*), nos pontos 63 e 64 e na conclusão IX, das alegações de recurso</u>

Ora, no caso dos autos, a respeito da matéria constante das alíneas d) e e) dos factos não provados, o recorrente observou os ónus impugnatórios acima referidos, a que se reporta o artigo 640.º do CPC, concretizando tais pontos, que considerou incorretamente julgados, especificando os meios probatórios

convocados (convocando, designadamente, as passagens da gravação dos depoimentos que se pretendem que sejam analisados) e indicando a decisão alternativa a proferir.
Contudo, na parte II da alegação – que o recorrente intitulou *"Da inexistência de culpa na atuação do representante legal da recorrente"* – o recorrente concluiu que o tribunal entendeu que o autor atuou com negligência grosseira ao fornecer os dados do seu cartão matriz, referindo-se que o Tribunal recorrido o fez *"sem sopesar todas as circunstâncias atinentes ao caso concreto, incorrendo igualmente em erro de julgamento sobre a matéria de facto, no que a este ponto respeita"* (cfr. pontos 39 e 40 das alegações), referenciando-se, contudo, a outros factos provados (cfr. facto provado n.º 3) e concluindo que se deveria ter considerado que o recorrente tomou todas as precauções exigidas, enquanto utilizador do serviço de homebanking, atuando de acordo com o padrão de diligência que se lhe impunha (vd., em particular, pontos 65 e 69 das alegações).
Ora, neste âmbito, apesar do propósito manifestado pela recorrente, certo é que, a mesma, não faz acompanhar tal propósito da indicação de quais os concretos pontos de facto que considera incorretamente julgados, nem qual a decisão que deveria ser tomada sobre as questões de facto impugnadas, não observando os ónus de impugnação referenciados na alíneas a) e c), do n.º 1, do artigo 640.º do CPC.
Na medida em que a recorrente não deu, neste conspecto, cumprimento ao preceito legal acima mencionado, não cuidando de indicar – quer na motivação, quer nas conclusões do recurso – tais elementos de impugnação, tal determina a rejeição da impugnação de facto, nesta parte.
Por outro lado, na conclusão IX, a recorrente pugnou no sentido de que:
"IX – A confiança do representante legal da recorrente foi reforçada pelo facto de, ao aceder à página de homebanking da recorrida, pôde logo consultar o seu saldo atual e movimentos, facto que deveria ter sido devidamente atendido e, atentas as declarações de parte da recorrida, dado como provado".
Neste ponto importa salientar que, face ao disposto no nº 1 do art.º 5º do Código de Processo Civil, a decisão da matéria de facto tem por objecto, desde logo, os factos essenciais alegados pelas partes, quer integrantes da causa de pedir, quer das excepções invocadas. Todavia, porque do n.º 2 do mesmo artigo 5.º do CPC resulta que o tribunal deve ainda considerar os factos instrumentais, bem como os factos complementares e concretizadores daqueles que as partes hajam alegado, e que resultem da instrução da causa, daí decorre que na decisão da matéria de facto devem esses factos ser tidos em consideração.
Tal não significa, no entanto, que a decisão da matéria de facto (provada e não provada) deva comportar toda a matéria alegada

pelas partes e, bem ainda, aquela que resulte da prova produzida, já que apenas a factualidade que assuma juridicidade relevante em razão das questões a conhecer é que deve ser objecto dessa decisão.
Isso mesmo salientam António Santos Abrantes Geraldes, Paulo Pimenta e Luís Filipe Pires de Sousa (Código de Processo Civil Anotado, vol. I, 2018, pp. 721-722), quando explicam que o juiz da causa deve optar *"por uma descrição mais ou menos pormenorizada ou concretizada, de acordo com as necessidades do pleito, desde que seja assegurada uma descrição natural e inteligível da realidade que, para além de revelar o contexto jurídico em que se integra, permita a qualquer das partes a sua impugnação (…)"* e que *"o regime consagrado no CPC de 2013 propugna uma verdadeira concentração naquilo que é essencial, depreciando o acessório, sendo importante que o juiz consiga traduzir em linguagem normal a realidade apreendida, explicitando, depois, os motivos que o determinaram, com destaque para a explanação dos factos instrumentais que o levaram a extrair as ilações ou presunções judiciais".*
Ora, conforme se referiu no Acórdão do Supremo Tribunal de Justiça de 17-05-2017, (Pº 4111/13.4TBBRG.G1.S1, relatado por FERNANDA ISABEL PEREIRA): *"O princípio da limitação dos actos, consagrado, no artigo 130.º do CPC, para os actos processuais em geral, proíbe, enquanto manifestação do princípio da economia processual, a prática de actos no processo – pelo juiz, pela secretaria e pelas partes – que não se revelem úteis para alcançar o seu termo. Nada impede que tal princípio seja igualmente observado no âmbito do conhecimento da impugnação da matéria de facto se a análise da situação concreta evidenciar, ponderadas as várias soluções plausíveis da questão de direito, que desse conhecimento não advirá qualquer elemento factual cuja relevância se projecte na decisão de mérito a proferir".*
Na decorrência destas considerações pode concluir-se que só há lugar à apreciação dos pontos indicados como impugnados na medida em que, não só devam constar do elenco de factos provados e não provados - no respeito pelo disposto no art.º 5º, nº 1 e nº 2, al b), do Código de Processo Civil – como, igualmente, correspondam a factos com efectivo interesse ou pertinência para a decisão do recurso.
Conforme se escreveu no Acórdão desta Relação de 26-09-2019 (Pº 144/15.4T8MTJ.L1, relatado pelo ora relator), *"não se deverá proceder à reapreciação da matéria de facto quando os factos objecto de impugnação não forem susceptíveis, face às circunstâncias próprias do caso em apreciação, de ter relevância jurídica, sob pena de se levar a cabo uma actividade processual que se sabe ser inútil, o que contraria os princípios da celeridade e da economia processuais (art.ºs 2º, nº 1, 137º e 138º, todos do C.P.C.)".*
Ou seja: *"Não se deverá proceder à reapreciação da matéria de*

facto quando os factos objecto de impugnação não forem susceptíveis, face às circunstância próprias do caso em apreciação, de ter relevância jurídica, sob pena de se levar a cabo uma actividade processual que se sabe ser inútil, o que contraria os princípios da celeridade e da economia processuais (art.ºs 2º, nº 1, 137º e 138º, todos do C.P.C.)" **(assim, o Acórdão do Tribunal da Relação de Guimarães de 15-12-2016, Processo 86/14.0T8AMR.G1, relatora MARIA JOÃO MATOS).**

E a respeito da enunciação dos factos instrumentais, decorre do nº 4 do art.º 607º do CPC, que os mesmos não carecem de ser discriminados no elenco de factos provados, mas apenas referidos na medida das ilações que forem tiradas dos mesmos, para a demonstração dos factos essenciais alegados pelas partes.

Isso mesmo explicam igualmente António Santos Abrantes Geraldes, Paulo Pimenta e Luís Filipe Pires de Sousa (Código de Processo Civil Anotado, vol. I, 2018, pp. 718 719), afirmando a necessidade de enunciação dos ***"factos essenciais (nucleares) que foram alegados para sustentar a causa de pedir ou para fundar as excepções, e de outros factos, também essenciais, ainda que de natureza complementar que, de acordo com o tipo legal, se revelem necessários para que a acção ou a excepção proceda",*** **e de** ***"enunciação dos factos concretizadores da factualidade que se apresente mais difusa"*** **(e sendo que** ***"a enunciação dos factos complementares e concretizadores far-se-á desde que se revelem imprescindíveis para a procedência da acção ou da defesa, tendo em conta os diversos segmentos normativos relevantes para o caso*****"), mas afirmando igualmente que, quanto aos factos instrumentais,** ***"atenta a função secundária que desempenham no processo, tendente a justificar simplesmente a prova dos factos essenciais, para além de, em regra, não integrarem os temas da prova, nem sequer deverão ser objecto de um juízo probatório específico",*** **já** ***que "o seu relevo estará limitado à motivação da decisão sobre os restantes factos, designadamente quando a convicção sobre a sua prova resulte da assunção de presunções judiciais".***

Ora, compulsados os articulados das partes e em particular a petição inicial, não se divisa qualquer alegação no sentido de que o representante legal da recorrente, ***"ao aceder à página de homebanking da recorrida, pôde logo consultar o seu saldo atual e movimentos"*****, aspeto que, embora instrumental ou acessório da alegação produzida pela recorrente na petição inicial – cfr. artigos 3.º e ss. – não tinha que ser elencado na selecção factual levada a efeito pelo Tribunal que, de todo o modo, considerou na motivação da decisão de facto, a respeito do depoimento de NC, que o mesmo:**

"Iniciou o seu depoimento revelando que utiliza o sistema homebanking há cerca de uma década da Caixa Geral de depósitos e da aqui Ré, sendo que ainda hoje a utiliza diariamente, sendo a

situação deste processo a única que lhe sucedeu até à data (facto provado 30).
Para complementar a sua petição inicial, visto que nesse âmbito a mesma não entrou em pormenores, o gerente da A revelou que clicou na secção de páginas gravadas na barra de ferramentas do seu computador relativa ao site da Ré, colocou as suas credenciais e na lateral direita viu um pedido de actualização do seu cartão matriz, o qual preencheu em dois dias distintos.
(…) Sustentou que como não estava a fazer transferências não estranhou estar a preencher mais de duas coordenadas do seu cartão matriz.
Mais alegou, em completa contradição com a petição inicial que não era uma página forjada, era a real [a]penas apareceu ao lado a possibilidade de actualizar.
Quando o gerente da A foi confrontado com o documento 11 da contestação que revela os alertas de segurança estabelecidos no site da Ré, que fornece exemplos de tentativas de fraude aquele confirmou que se trata da mesma situação, embora com grafismo diferente e que só 50% do cartão estaria por preencher, assim como confirmou que o seu cartão é igual ao documento 12 da contestação. (factos provados 35, 36 e 43) (…)".
Ora, não apresentando a factualidade invocada alguma autonomia com o juízo probatório formulado pelo Tribunal, correspondendo a um facto instrumental, designadamente a respeito do facto provado n.º 3, a indagação sobre a impugnação factual realizada, sempre conduziria à prática de um acto inútil.
Igual raciocínio é de adotar relativamente ao alegado nos artigos 63 e 64 da alegação de recurso, sendo que, inclusive, quanto a estes pontos, a recorrente nas conclusões não cuidou sequer de evidenciar pretender impugnar a correspondente matéria invocada na alegação.
De acordo com o exposto e com os fundamentos mencionados, há lugar à rejeição imediata do recurso no que respeita à impugnação da matéria de facto invocada na parte II (intitulada *"Da inexistência de culpa na atuação do representante legal da recorrente"*), nos pontos 63 e 64 e na conclusão IX das alegações de recurso.
*****
B) Se a matéria constante das alíneas d) e e) dos factos não provados deve ser dada como provada?
Como se viu, a recorrente visa que a matéria constante das alíneas d) e e) dos factos provados deve ser dada como provada.
Especificamente sobre a reapreciação probatória, importa referir que *"o recorrente que pretenda contrariar a apreciação crítica da prova feita pelo Tribunal a quo terá de apresentar razões objectivas para contrariar a prevalência dada a um meio de prova sobre outro de sinal oposto, ou o maior crédito dado a um depoimento sobre outro contrário, não sendo suficiente para o efeito a mera*

transcrição de excertos de alguns dos depoimentos prestados, já antes ouvidos pelo julgador sindicado e ponderados na sua decisão recorrida (art.º 640º do C.P.C.)" **(assim, o Acórdão do Tribunal da Relação de Guimarães de 02-11-2017 (Processo n.º 501/12.8TBCBC.G1, relatora MARIA JOÃO MATOS).**

O artigo 607.º, n.º 4, do CPC impõe ao julgador que na fundamentação da sentença declare ***"quais os factos que julga provados e quais os que julga não provados, analisando criticamente as provas, indicando as ilações tiradas dos factos instrumentais e especificando os demais fundamentos que foram decisivos para a sua convicção; o juiz toma ainda em consideração os factos que estão admitidos por acordo, provados por documentos ou por confissão consideração os factos que estão admitidos por acordo, provados por documentos ou por confissão reduzida a escrito, compatibilizando toda a matéria de facto adquirida e extraindo dos factos apurados as presunções impostas pela lei ou por regras de experiência."***

"A exigência de fundamentação da matéria de facto provada e não provada com a indicação dos meios de prova que levaram à decisão, assim como a fundamentação da convicção do julgador, devem ser feitas com clareza, objectividade e discriminadamente, de modo a que as partes, destinatárias imediatas, saibam o que o Tribunal considerou provado e não provado e a fundamentação dessa decisão reportada à prova fornecida pelas partes e adquirida pelo Tribunal" **(assim, o Acórdão do Supremo Tribunal de Justiça de 26-02-2019, Pº 1316/14.4TBVNG-A.P1.S2, rel. FONSECA RAMOS).**

Lebre de Freitas (A Acção Declarativa Comum à Luz do Código de Processo Civil, 3.ª ed., p. 315) refere, a este respeito, que: ***"No novo código, a sentença engloba a decisão de facto, e já não apenas a decisão de direito. Na decisão de facto, o tribunal declara quais os factos, dos alegados pelas partes e dos instrumentais que considere relevantes, que julga provados (total ou parcialmente) e quais os que julga não provados, de acordo com a sua convicção, formada no confronto dos meios de prova sujeitos à livre apreciação do julgador; esta convicção tem de ser fundamentada, procedendo o tribunal à análise crítica das provas e à especificação das razões que o levaram à decisão tomada sobre a verificação de cada facto (art.º 607, n.º 4, 1.ª parte, e 5) ".***

Conforme se sublinhou no já citado Acórdão do STJ de 26-02-2019, Pº 1316/14.4TBVNG-A.P1.S2, rel. FONSECA RAMOS): ***"Sendo os temas da prova enunciados de maneira sucinta, ainda que pressuponham ampla matéria de facto, a exigência de fundamentação desta justifica-se, de modo mais acentuado, porquanto não acontece, como no passado, quando a análise da peça processual onde se respondia aos quesitos permitia, em regra, saber de modo discriminado (os quesitos eram enumerados) o que tinha ficado provado e não provado e a***

fundamentação, que sempre se reputou não ter que ser exaustiva, mas devendo dar a conhecer os meios de prova em que acentuou a convicção quanto à prova submetida a julgamento".

Por seu turno, refere Francisco Manuel Lucas de Ferreira de Almeida (Direito Processual Civil, Vol. II, 2015, pp. 350-351) que: *"A estatuição do citado nº4 do art- 607º (1º- segmento) é, contudo, meramente indicadora ou programática, não obrigando o tribunal a descrever de modo exaustivo o iter lógico-racional da apreciação da prova submetida ao respectivo escrutínio; basta que enuncie, de modo claro e inteligível, os meios e elementos de prova de que se socorreu para a análise crítica dos factos e a razão da sua eficácia em termos de resultado probatório. Trata-se de externar, de modo compreensível, o itinerário cognoscitivo e valorativo percorrido pelo tribunal na apreciação da realidade ou irrealidade dos factos submetidos ao seu escrutínio. Deve, assim, o tribunal enunciar os meios probatórios que hajam sido determinantes para a emissão do juízo decisório, bem como pronunciar-se: - relativamente aos factos provados, sobre a relevância deste ou daquele depoimento (de parte ou testemunhal), designadamente quanto ao seu grau de isenção, credibilidade, coerência e objectividade; - quanto aos factos não provados, indicar as razões pelas quais tais meios não permitiram formar uma convicção minimamente segura quanto à sua ocorrência ou convencer quanto a uma diferente perspectiva da sua realidade ou verosimilhança […].Não impõe, contudo, a lei que a fundamentação das conclusões fácticas decisórias seja indicada separadamente por cada um dos factos, isolada e autonomamente considerado (podendo sê-lo por conjuntos ou blocos de factos sobre os quais a testemunha se haja pronunciado)".*

Conforme se assinalou no Acórdão do Tribunal da Relação do Porto de 26-10-2020 (Pº 258/18.9T8PNF-A.P1, rel. EUGÉNIA CUNHA): *"Podendo ser objeto de instrução tudo quanto, de algum modo, possa interessar à prova dos factos relevantes para a decisão da causa segundo as várias soluções plausíveis da questão de direito, vedado está aquilo que se apresenta como irrelevante (impertinente) para a desenhada causa concreta a decidir, devendo, para se aferir daquela relevância, atentar-se no objeto do litígio (pedido e respetiva causa de pedir e matéria de exceção); Havendo enunciação dos temas de prova, o objeto da instrução são os temas da prova formulados, densificados pelos respetivos factos, principais e instrumentais (constitutivos, modificativos, impeditivos ou extintivos do direito afirmado) –v. art.ºs 410º, do CPC e 341º e seguintes, do Código Civil e, ainda, artigo 5º, daquele diploma legal".*

Nesta linha é, pois, crucial que seja feita a indicação e especificação dos factos provados e não provados e a indicação dos fundamentos por que o Tribunal formou a sua convicção acerca de cada facto que estava em apreciação e julgamento, de acordo com os temas da prova fixados.

"A matéria de facto provada deve ser descrita pelo juiz de forma fluente e harmoniosa, técnica bem diversa de uma que continue a apostar na mera transcrição de respostas afirmativas, positivas, restritivas ou explicativas a factos sincopados, como os que usualmente preenchiam os diversos pontos da base instrutória (e do anterior questionário). Se, por opção, por conveniência ou por necessidade, se inscreveram nos temas de prova factos simples, a decisão será o reflexo da convicção formada sobre tais factos, a qual deve ser convertida num relato natural da realidade apurada… […]. O importante é que, na enunciação dos factos provados e não provados, o juiz use uma metodologia que permita perceber facilmente a realidade que considerou demonstrada, de forma linear, lógica e cronológica, a qual, uma vez submetida às normas jurídicas aplicáveis, determinará o resultado da acção."
(assim, Abrantes Geraldes, Paulo Pimenta e Luís Filipe Pires de Sousa, Código de Processo Civil Anotado, Vol. I, 2018, p. 717).
Ora, conforme se referiu no Acórdão do Supremo Tribunal de Justiça de 17-05-2018 (Pº 3811/13.3TBPRD.P1.S1, rel. ROSA TCHING), ***"[f]actos provados são os factos concretos assim julgados, na sentença final, após exame crítico das provas e não os factos tidos como assentes no despacho de identificação do objeto do litígio e enunciação dos temas da prova. Ainda que se admita não haver obstáculo a que o juiz, no âmbito do novo Código de Processo Civil, continue a proferir despacho de fixação da matéria de facto considerada assente, é inquestionável que tal despacho não pode deixar de ser visto como um "guião" ou mero "suporte de trabalho" para o julgamento, pelo que, mesmo depois de decididas as reclamações contra ele apresentadas, não se forma caso julgado formal sobre ele, podendo, por isso, os factos dados como assentes ser alterados pelo juiz do julgamento e/ou pelo juiz do tribunal de recurso".***
Ainda na mesma linha, cite-se o Acórdão do Tribunal da Relação do Porto de 23-11-2017 (Pº 3811/13.3TBPRD.P1, rel. MADEIRA PINTO) onde se escreveu que: ***"Sendo certo que a instrução tem por objecto os temas de prova enunciados e que no NCPC estes não se confundem apenas com factos podendo ser conclusões jurídicas ou versões contrárias de factos ou conclusões, é seguro para nós e de acordo com a generalidade da doutrina e da jurisprudência, que a enunciação dos temas de prova não constitui despacho que faça caso julgado formal sobre os factos essenciais, instrumentais ou complementares que interessam à decisão de direito segundo as diferentes soluções possíveis e alegados pelas partes de acordo com as regras dos artº 5º, nºs 1 e 2 e 607º, nº 4, NCPC".***
E conforme referem Antunes Varela, J. Miguel Bezerra e Sampaio e Nora (Manual de Processo Civil, 2.ª Ed., Coimbra Editora, Coimbra, 1985, p. 436), para que um facto se considere provado é necessário que, à luz de critérios de razoabilidade, se crie no espírito do julgador um estado de convicção, assente na

certeza relativa do facto. A prova *"assenta na certeza subjectiva da realidade do facto, ou seja, no (alto) grau de probabilidade de verificação do facto, suficiente para as necessidades práticas da vida".*

Essa certeza subjectiva, com alto grau de probabilidade, há-de resultar da conjugação de todos os meios de prova produzidos sobre um mesmo facto, ponderando-se a coerência que exista num determinado sentido e aferindo-se esse resultado convergente em termos de razoabilidade e lógica. Se pelo contrário, existir insuficiência, contradicção ou incoerência entre os meios de prova produzidos, ou mesmo se o sentido da prova produzida se apresentar como irrazoável ou ilógico, então haverá uma dúvida séria e incontornável quanto à probabilidade dos factos em causa serem certos, obstando a que se considere o facto provado.

Importa considerar que, em termos substanciais, a impugnação da matéria de facto traduz-se no meio de sindicar a decisão que sobre ela proferiu a primeira instância, procurando-se que a Relação reaprecie e repondere os elementos probatórios produzidos, averiguando se a decisão da primeira instância relativa aos pontos de facto impugnados se mostra conforme às regras e princípios do direito probatório, impondo-se se proceda à apreciação não só da valia intrínseca de cada um dos elementos probatórios, da sua consistência e coerência, à luz das regras da normalidade e da experiência da vida, mas também da sua valia extrínseca, ou seja, da sua consistência e compatibilidade com os demais elementos.

Como refere Abrantes Geraldes (Recursos no Novo Código de Processo Civil, 2013, pág. 127): *"Consistindo o processo jurisdicional num conjunto não arbitrário de actos jurídicos ordenados em função de determinados fins, as partes devem deduzir os meios necessários para fazer valer os seus direitos na altura/fase própria, sob pena de sofrerem as consequências da sua inactividade, numa lógica precisamente assente, em larga medida, na autorresponsabilidade das partes e, conexamente, num sistema de ónus, poderes, faculdades, deveres, cominações e preclusões".*

Assim, ressalvadas as modificações que podem ser oficiosamente operadas relativamente a determinados factos cuja decisão esteja eivada de erro de direito, por violação de regras imperativas, à Relação não é exigido que, de *motu proprio*, se confronte com a generalidade dos meios de prova sujeitos a livre apreciação e valorados pelo tribunal de 1ª instância, para deles extrair, como se se tratasse de um novo julgamento, uma decisão inteiramente nova.

Pelo contrário, as modificações a operar devem respeitar, desde logo, o que o recorrente - no exercício do seu direito de impugnação da decisão da matéria de facto - indicou nas respectivas alegações e cujo âmbito tem a função de delimitar o

objecto do recurso.
O ordenamento processual probatório português combina o sistema livre apreciação ou do íntimo convencimento com o sistema da prova positiva ou legal, dado que, *"a partir da prova pessoal obtida e da análise do teor dos documentos existentes nos autos ou doutra fonte probatória relevante, tomando em consideração a análise da motivação da respectiva decisão, importa aferir se os elementos de convicção probatória foram obtidos em conformidade com o princípio da convicção racional, consagrado pelo artigo 607º, nº 5, do Código de Processo Civil"* (assim, o Acórdão do Tribunal da Relação de Évora de 06-10-2016, Pº 1306/12.1TBSSB.E1, rel. JOSÉ TOMÉ DE CARVALHO).
A valoração da prova, nomeadamente a testemunhal, deve ser efectuada segundo um critério de probabilidade lógica, através da confirmação lógica da factualidade em apreciação, partindo da análise e ponderação da prova disponibilizada (cfr. Antunes Varela, Miguel Varela e Sampaio e Nora, Manual de Processo Civil, Coimbra Editora, pp. 435-436).
Os meios probatórios têm por função a demonstração da realidade dos factos, sendo que, através da sua produção não se pretende criar no espírito do julgador uma certeza absoluta da realidade dos factos, o que, obviamente implica que a realização da justiça se tenha de bastar com um grau de probabilidade bastante, em face das circunstâncias do caso, das regras da experiência da comum e dos conhecimentos obtidos pela ciência.
A prova não visa *"(...) a certeza absoluta (a irrefragável exclusão da possibilidade de o facto não ter ocorrido ou ter ocorrido de modo diferente) (...)"*, mas tão só, *"(...) de acordo com os critérios de razoabilidade essenciais à prática do Direito, criar no espírito do julgador um estado de convicção, assente na certeza relativa do facto"* (assim, Antunes Varela, Manual de Processo Civil, Coimbra Editora, 1984, págs. 419 e 420).
A apreciação das provas resolve-se, assim, na formulação de juízos, que assentam na elaboração de raciocínios que surgem no espírito do julgador *"(...) segundo as aquisições que a experiência tenha acumulado na mentalidade do juiz segundo os processos psicológicos que presidem ao exercício da actividade intelectual, e portanto segundo as máximas de experiência e as regras da lógica (...)"* (assim, Alberto dos Reis; Código de Processo Civil Anotado, vol. III, pág. 245).
Nessa actividade de livre apreciação da prova deve o tribunal especificar os fundamentos que foram decisivos para a convicção adquirida (art. 653º, nº 2 do CPC), permitindo, dessa forma, que se *"possa controlar a razoabilidade da convicção sobre o julgamento do facto como provado ou não provado"* (cfr. Teixeira de Sousa; Estudos Sobre o Novo Processo Civil, p. 348) e exercer um controle externo e geral do fundamento de facto da decisão.
A *"prova testemunhal, tal como acontece com a prova indiciária de*

qualquer outra natureza, pode e deve ser objecto de formulação de deduções e induções, as quais, partindo da inteligência, hão-de basear-se na correcção de raciocínio, mediante a utilização das regras de experiência [o id quod plerumque accidit] e de conhecimentos científicos.
Na transição de um facto conhecido para a aquisição ou para a prova de um facto desconhecido, têm de intervir as presunções naturais, como juízos de avaliação, através de procedimentos lógicos e intelectuais, que permitam, fundadamente, afirmar, segundo as regras da experiência, que determinado facto, não, anteriormente, conhecido, nem, directamente, provado, é a natural consequência ou resulta, com toda a probabilidade próxima da certeza, ou para além de toda a dúvida razoável, de um facto conhecido" **(assim, o Acórdão do Supremo Tribunal de Justiça de uniformização de jurisprudência, de 21-06-2016, Pº 2683/12.0TJLSB.L1.S1, rel. HÉLDER ROQUE).**
Neste enquadramento, a credibilidade firmada em torno de um específico meio de prova tem subjacente a aplicação de máximas da experiência comum, que devem enformar a opção do julgador e cuja validade se objectiva e se afere em determinado contexto histórico e jurídico, à luz da sua compatibilidade lógica com o sentido comum e com critérios de normalidade social, os quais permitem (ou não) aceitar a certeza subjectiva da sua realidade.
Todas estas circunstâncias deverão ser ponderadas na ocasião em que a Relação procede à reapreciação dos meios de prova, evitando a introdução de alterações quando, fazendo actuar o princípio da livre apreciação das provas, não seja possível concluir, com a necessária segurança, pela existência de erro de apreciação relativamente aos concretos pontos de facto impugnados.
Mas, não deverá esquecer-se que a função da Relação não é a de realizar um novo julgamento de facto: ***"Quando o Tribunal da Relação é chamado a pronunciar-se sobre a reapreciação da prova, no caso de se mostrarem gravados os depoimentos ou estando em causa a análise de meios prova reduzidos a escrito e constantes do processo, deve o mesmo considerar os meios de prova indicados pela partes e confrontá-los com outros meios de prova que se mostrem acessíveis, a fim de verificar se foi cometido ou não erro de apreciação que deva ser corrigido, seja no sentido de decidir em sentido oposto ou, num plano intermédio, alterar a decisão no sentido restritivo ou explicativo; Importa, porém, não esquecer que se mantêm-se em vigor os princípios de imediação, da oralidade e da livre apreciação da prova, pelo que o uso, pela Relação, dos poderes de alteração da decisão da 1ª instância sobre a matéria de facto só deve ser usado quando seja possível, com a necessária segurança, concluir pela existência de erro de apreciação relativamente a concretos pontos de facto impugnados. Assim, em caso de dúvida, face a depoimentos contraditórios entre si e à***

fragilidade da prova produzida, deverá prevalecer a decisão proferida pela primeira instância, em observância aos princípios da imediação, da oralidade e da livre apreciação da prova, com a consequente improcedência do recurso nesta parte" **(assim, o Acórdão do Tribunal da Relação de Guimarães de 30-11-2017, Processo 1426/15.0T8BGC-A.G1, relator ANTÓNIO JOSÉ SAÚDE BARROCA PENHA).**

Neste sentido, ***"não estando em causa formalidades especiais de prova legalmente exigidas para a demonstração de quaisquer factos e assentando a decisão da matéria de facto na convicção criada no espírito do juiz e baseada na livre apreciação das provas testemunhal e documental e pericial que lhe foram apresentadas, a sindicância de tal decisão não pode deixar de respeitar a liberdade da 1ª instância na apreciação dessas provas. O erro na apreciação das provas consiste em o tribunal ter dado como provado ou não provado determinado facto quando a conclusão deveria ter sido manifestamente contrária, seja por força de uma incongruência lógica, seja por ofender princípios e leis científicas, nomeadamente, das ciências da natureza e das ciências físicas ou contrariar princípios gerais da experiência comum (sendo em todos os casos o erro mesmo notório e evidente), seja também quando a valoração das provas produzidas apontarem num sentido diverso do acolhido pela decisão judicial mas, note-se, excluindo este. Em caso de dúvida sobre o sentido da decisão, face às provas que lhe são apresentadas, a 2ª instância deve fazer prevalecer a decisão da 1ª instância, em homenagem à livre convicção e liberdade de julgamento. A garantia do duplo grau de jurisdição em caso algum pode subverter o princípio da livre apreciação da prova, de acordo com a prudente convicção do juiz acerca de cada facto e, por isso, o objecto do recurso não pode ser nem a liberdade de apreciação das provas, nem a convicção que presidiu à matéria de facto, mas esta própria decisão"*** **(assim, o Acórdão do Tribunal da Relação de Évora de 05-05-2011, Processo 334/07.3TBASL.E1, relatora MARIA ALEXANDRA A. MOURA SANTOS).**

É que, na verdade, como escreve Abrantes Geraldes (Recursos no Novo Código de Processo Civil, 2013, p. 234): ***"… existem aspectos comportamentais ou reacções dos depoentes que apenas são percepcionados, apreendidos, interiorizados e valorados por quem os presencia e que jamais podem ficar gravados ou registados para aproveitamento posterior por outro tribunal que vá reapreciar o modo como no primeiro se formou a convicção do julgador. O sistema não garante de forma tão perfeita quanto a que é possível na 1ª instância a percepção do entusiamo, das hesitações, do nervosismo, das reticências, das insinuações, da excessiva segurança ou da aparente imprecisão, em suma, de todos os factores coligidos pela psicologia judiciária e de onde é legítimo ao tribunal retirar argumentos que permitam, com razoável segurança, credibilizar determinada informação ou deixar de lhe atribuir***

qualquer relevo. Além do mais, todos sabemos que, por muito esforço que possa ser feito na racionalização da motivação da decisão da matéria de facto, sempre existirão factores difíceis ou impossíveis de concretizar ou de verbalizar, mas que são importantes para fixar ou repelir a convicção acerca do grau de isenção que preside a determinados depoimentos".

Em suma: Para se considerarem provados ou não provados determinados factos, não basta que as testemunhas chamadas a depor se pronunciem sobre os factos num determinado sentido, para que o juiz necessariamente aceite esse sentido ou versão.

O julgamento dos factos, na sua valoração, mormente quando se reporta a meios de prova produzidos oralmente, não se reconduz a uma operação aritmética de número ou de adição de depoimentos, antes tem de atender a uma multiplicidade de factores, não se bastando com a palavra pronunciada, mas nele confluindo aspetos tão variados como, as garantias de imparcialidade, as razões de ciência, a espontaneidade dos depoimentos, a verosimilhança, a seriedade, o raciocínio, as lacunas, as hesitações, a linguagem, o tom de voz, o comportamento, os tempos de resposta, as coincidências, as contradições, o acessório, as circunstâncias, o tempo decorrido, o contexto sócio-cultural, a linguagem gestual (como por exemplo os olhares) e até interpretar as pausas e os silêncios dos depoentes, para poder perceber quem estará a falar com verdade e até que ponto é que, consciente ou inconscientemente, poderá a verdade estar a ser distorcida.

Aplicando estas considerações à impugnação de facto em questão (na parte não rejeitada), cumpre apreciar a matéria impugnada.

O Tribunal recorrido concluiu, no que consta vertido nas alíneas d) e e) dos factos não provados, que não se fez prova de que:

- O hacker se aproveitou das fragilidades que o sistema de homebanking prestado pela ré apresentava no seu serviço "Net 24"; e que,

- As transferências em causa foram possíveis unicamente pela falta de segurança garantida pela ré.

O Tribunal recorrido fundamentou a sua convicção sobre a ausência de demonstração probatória na circunstância de a própria autora alegar que foi dirigida a uma página que não era areal, pelo que o alvo não foi o sistema da ré, mas o da autora, já que a página (a que a autora acedeu) é alheia ao sistema informático da ré.

Será que o juízo probatório alcançado pelo Tribunal recorrido merece censura?

Importa referir que, tal matéria resultou do que a autora tinha alegado na petição inicial, nomeadamente, nos seguintes pontos:

"(…) 27º Em consequência da fraude informática, perpetrada por indivíduo(s) cuja identidade não foi possível apurar, que logrou movimentar o dinheiro da conta bancária da A- - que se encontrava

sediada na R. (Caixa Económica Montepio Geral)- para a sua, ficou a A. prejudicada nos valores transferidos, correspondentes aos acima mencionados.
28º Aproveitando-se das fragilidades que o sistema de homebanking prestado pelo requerido CAIXA ECONÓMICA MONTEPIO GERAL – Banco Montepio apresentava no seu serviço "Net 24", (…)
32º Operações forjadas que, obviamente, não tinham o consentimento da ora A.
33º Possíveis, unicamente, pela falta de segurança garantida pela R., Caixa Económica Montepio Geral - MONTEPIO.
34.º Sendo, ainda, de salientar que, a Ré, à data dos factos, não fornecia aos seus clientes a segurança do SMS TOKEN (…)".
Ora, ouvidos por este Tribunal de recurso todos os depoimentos prestados em audiência de discussão e julgamento, concatenados todos os meios probatórios documentais produzidos, não se alcança que o juízo obtido pelo Tribunal recorrido mereça algum reparo, coadunando-se e mostrando-se congruente com a prova produzida.
Assim, desde logo, importa salientar que se mostra assente – e não foi impugnada – matéria de facto que colide com a demonstração da vertida nas alíneas d) e e) dos factos não provados.
Na realidade, apurou-se, nomeadamente, que:
- No início de novembro de 2015, a A. através do seu sócio gerente Sr. NC, quando acedeu à página do homebanking da Caixa Económica Montepio Geral, foi direcionado para uma página de Internet previamente forjada e em tudo idêntica à página oficial daquela instituição, solicitando a atualização do cartão matriz e a indicação de determinadas coordenadas do mesmo (cfr. n.º 3 dos factos provados);
- Pessoa ou pessoas (hacker(s) cuja(s) identidade (s) não foi apurada conseguiu, assim que a autora, na qualidade de cliente da Caixa Económica Montepio Geral fornecesse os seus códigos de ativação do serviço homebanking (cfr. n.º 4 dos factos provados);
- Após o que, a pessoa ou pessoas cuja identidade não foi possível apurar, munidos das respetivas credenciais de acesso, obtidas de forma fraudulenta, acederam à conta bancária da autora, como se se tratasse do seu verdadeiro titular (…) (cfr. n.º 5 dos factos provados);
- Tal pessoa, ou pessoas, acedeu ou acederam, assim, através do serviço de homebanking, à conta bancária titulada pela A. com o número 2131.10.605744-2., domiciliada no Montepio Geral, agência de Angra do Heroísmo, sem o conhecimento e contra a vontade do seu titular efetuando no dia 13 de novembro de 2015 e no dia 15 de novembro de 2015, respetivamente, 4 e 13 acessos ilegítimos / levantamentos / transferências internacionais, o que

totaliza 17 acessos ilegítimos / levantamentos/ transferências internacionais para pagamento a pessoas desconhecidas, dos seguintes montantes:
I. 2015-11-13 PAG. SERV. 21547 400000067 €2.500,00
II. 2015-11-13 PAG. SERV. 21547 400000067 €2.499,00
III. 2015-11-13 PAG. SERV. 21547 400000066 €1.250,00
IV. 2015-11-13 PAG. SERV. 21547 400000068 €1.249,00
V. 2015-11-15 PAG. SERV. 21547 400000158 €2.250,00
VI. 2015-11-15 PAG. SERV. 21547 400000157 €2.250,00
VII. 2015-11-15 PAG. SERV. 21547 400000156 €250,00
VIII. 2015-11-15 PAG. SERV. 21547 400000155 €249,00
IX. 2015-11-15 PAG. SERV. 21547 400000156 €1.250,00
X. 2015-11-15 PAG. SERV. 21547 400000156 €500,00
XI. 2015-11-15 PAG. SERV. 21547 400000155 €750,00
XII. 2015-11-15 PAG. SERV. 21547 400000148 €2.000,00
XIII. 2015-11-15 PAG. SERV. 21547 400000147 €2.250,00
XIV. 2015-11-15 PAG. SERV. 21547 400000146 €250,00
XV. 2015-11-15 PAG. SERV. 21547 4000000146 € 500,00
XVI. 2015-11-15 PAG. SERV. 21547 400000145 €1.250,00
XVII. 2015-11-15 PAG. SERV. 21547 400000144 €1.250,00 (cfr. n.º 7 dos factos provados);
- Ao sócio gerente da autora tinham sido, em data anterior, fornecidos os códigos de acesso/credenciais para utilização do sistema homebanking (cfr. n.º 20 dos factos provados), que, à data dos factos funcionavam em 3 níveis de segurança (Número de utilizador – correspondendo ao nº de cliente Montepio e que pode ser personalizado - ; Password – compostas por 6 dígitos, que após o primeiro login tem de ser obrigatoriamente alterada por uma da autoria e do exclusivo conhecimento do cliente -; e Cartão matriz - composto por 72 posições, cada uma com 3 dígitos, para validação de operações passíveis de alterar o património detido pelos clientes, junto do Banco Montepio, cujo processo de produção é externo à Ré e não envolve qualquer atuação humana, uma vez que as coordenadas são geradas por computador, sendo remetido via CTT para o endereço dos clientes, e apenas passível de ser ativado mediante a validação de códigos de acesso ao Net24 -numero de utilizador e password- adstrito ao cartão expedido.) (cfr. n.ºs. 21 a 26 dos factos provados);
- Para a realização de uma operação com alterações patrimoniais, o utilizador teria de efetuar o login, na página da internet da Ré, colocar a sua password, selecionar a operação e colocar as duas coordenadas do seu cartão matriz, e só mediante a sua correta validação, é que se confere validade à ordem transmitida (cfr. n.º 27 dos factos provados);
- Foram explicados ao Sócio Gerente da A todos os procedimentos de segurança e de utilização do referido serviço (cfr. n.º 28 dos factos provados), encontrando-se a informação

disponível no site da ré (cfr. n.º 29, 33 e 35 dos factos provados);
- Os movimentos indicados, apenas foram possíveis porque, em cada um deles: Foi introduzido o número de utilizador; Foi introduzida a password – 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; Foram introduzidas duas coordenadas do cartão matriz, que são sempre solicitadas de forma aleatória, pelo sistema e nunca repetidas (cfr. n.º 31 dos factos provados);
- O sistema da Ré não foi alvo de qualquer intrusão ou ataque informático (cfr. n.º 34 dos factos provados); e
- Consta do cartão matriz o seguinte: "Atenção: Nunca indique mais do que 2 dígitos deste Cartão Matriz." (cfr. n.º 36 dos factos provados).
Ora, das declarações do legal representante da autora – que se caracterizou como utilizador do serviço de homebanking há cerca de 10 anos, utilizando diariamente tal "ferramenta", considerando-a uma boa "ferramenta" – resultou que foi, na decorrência da utilização levada a efeito por si – e não por deficiência ou avaria do sistema informático da ré – que as transferências foram proporcionadas, nos termos que explicitou e concretizou.
MM referenciou que na página inicial do Montepio, antes da aposição das credenciais existem vários alertas do que não se poderá fazer, inclusivamente com exemplos de fraudes ocorridas. Referiu que, à data as operações eram realizadas com a introdução dos códigos de acesso e que o movimento era validado, com o seu cartão matriz com duas posições aleatórias/ coordenadas. Referiu que do lado do banco não existiu quebra de segurança eletrónica ou de protocolos inerentes à ré.
Josué Cardoso referiu, em moldes semelhantes, quais os procedimentos de acesso ao homebanking e para a ativação do cartão matriz. Disse que *"em 2019 [com a reserva que apontou em termos temporais]"* o procedimento alterou, mas que se o representante da autora não tivesse fornecido as coordenadas os movimentos não seriam concretizados. Referiu que não há banco nenhum que solicite ao seu cliente para preencher todas as coordenadas.
PB disse que na participação dos factos realizada pelo cliente, o mesmo facultou os códigos de acesso, tendo sido confrontado com o correspondente documento n.º 10 junto com a contestação - de onde se lê, nomeadamente, que depois de entrar no site do Montepio e pedido o código pin, *"foi-me solicitado o preenchimento do quadro matriz com as coordenadas. Tendo o feito de forma involuntária acreditando que estava na página oficial do Montepio…"* - sendo que o banco nunca solicita este tipo de informação, tudo em termos compatíveis com as demais

testemunhas referidas. Confirmou que atualmente se encontra implementado o "SMS Code".
A testemunha RG também detalhou os procedimentos de acesso e as condições de informação sobre os procedimentos de segurança a ter pelo cliente e que o banco disponibiliza, em plena harmonia com os demais depoimentos, sublinhando que o cliente manifestou que tinha fornecido a terceiros as coordenadas de acesso, *"ao contrário de todas as informações e ao contrário de todas as orientações"* disponibilizadas pelo banco.
Depois, também o testemunho de DC – que explicitou, com detalhe, os procedimentos de segurança, a vários níveis, implementados pelo banco e aqueles que existiam na perspetiva do cliente - não permite concluir que tenha ocorrido por qualquer processo de aproveitamento do sistema de homebanking disponibilizado pela ré, nem que, perante os termos em que tal serviço era, à data disponibilizado, ocorresse - designadamente pela não implementação do sistema de certificação "TOKEN" (o que foi apurado no facto provado n.º 16), que veio, ulteriormente a ser implementado - alguma falta de segurança que tenha possibilitado a concretização das transferências bancárias:
"Mandatário da Ré: Muito obrigado. Relativamente… então… portanto, isto explicou relativamente aos sistemas de segurança informáticos do Banco. Agora, associado a este meio de pagamento, ao Net 24, ao homebanking do Banco Montepio, eu pergunto-lhe, em dois mil e quinze, novamente, quais é que eram os elementos de segurança que estavam do lado do cliente? Como é que o cliente se autenticava, e como é que se garantia que a ordem de pagamento que estava a ser inserida por uma pessoa legitimamente habilitada para o efeito e que estava a ser dada uma ordem correta?
Testemunha DC: Exatamente., o Banco, em dois mil e quinze tinha uma metodologia em que lhe dava um conjunto de elementos que pretendiam identificar e autenticar os clientes nos serviços online, da banca online. E para isso dotava-se de um conjunto dados, nomeadamente, o primeiro era um user, um username para poder fazer o acesso ao nosso homebanking. Isso era feito no processo de subscrição deste serviço de homebanking, Net 24, em que era dado esse serviço e era dado o Pin, um Pin de seis dígitos era dado ao cliente, e que era utilizado para fazer acesso ao homebanking.
Só que o primeiro Pin que é dado ao cliente, o cliente é obrigado a fazer a sua alteração. Ou seja, o primeiro acesso ao sistema só será possível após a alteração deste primeiro Pin, o que permite que apenas o cliente tenha o conhecimento efetivo desse, desse Pin alterado. …Passa a ser, a estar só da esfera do conhecimento do próprio. Claro que este primeiro Pin, que nós introduzimos através do teclado aleatório que aparece no nosso homebanking, teclado virtual, este Pin apenas permite ter acesso de consulta ou de movimentação do património financeiro. O cliente tem duas contas passa o seu dinheiro de uma conta para a outro. Como, não

havendo alteração do património (…). A própria operação exige a saída de património do cliente da sua esfera patrimonial, obrigando a um sistema de autenticação de segundo nível que em dois mil e quinze era fornecido através de um de um cartão de um cartão matriz de coordenadas. Esse cartão-matriz de coordenadas quando era produzido, ou seja, no momento em que o cliente faz a adesão de acesso ao homebanking estes elementos do cartão é produzido de uma forma automática, sem intervenção humana, e é executado um processo de printing, de uma carta, que é enviada via correio físico, para a morada do cliente.
Este cartão vai estar pré-ativo. Ou seja, o cartão mesmo que fosse intercetado por alguém este cartão nunca poderia ser utilizado porque não está ativo e o cartão também tem um conjunto de características que é só pode ser ativo para uma conta daquele cliente. Não é para qualquer conta. Ou seja, é um cartão que só poderá ter efeito na esfera do cliente para o qual foi produzido. Mas também precisa também de o ativar. E a ativação do cliente pressupõe que ele faça um login, um pin novo, no próprio site... Isto permite, desta forma, activar o cartão. Só com o cartão ativo é que efetivamente poderá ser usado ….
Nós, quer dizer, o sistema de cartão físico… este conceito de posse física … limita e restringe muito o universo … depois da informação. Nenhum órgão do Banco tem acesso a este pin, ele não é impresso pelo banco, ou gabinete do próprio Banco, é impresso através de um sistema de printing, uma entidade externa que faz a envelopagem da carta e envia milhares de cartas….Pelo que o único utilizador que tem um cartão que pode ser utilizado é o próprio cliente.
Bom, depois para qualquer operação financeira, este cartão-matriz vai ser utilizado, esta operação quando tem saída do património pede aleatoriamente duas posições desse cartão. Estas posições são geridas de uma forma aleatória através de um sistema de gestão de segurança.
Qualquer individuo que faz a operação,… segurança é uma componente interna deste homebanking, quais são as posições seguintes que devem ser solicitadas aleatoriamente. E o cartão… essa informação é pedida através da página ao cliente, o cliente introduz os valores… é o cartão-matriz introduz os dois valores… pronto e ele, depois, essa informação é passada para este módulo de segurança que verifica se efetivamente aquelas respostas coincidem ou não com aquilo que foi …".
Mais adiante no seu depoimento, a testemunha DC abordou, em particular, a questão da alteração de procedimentos de segurança e se a mesma revelava alguma fragilidade dos elementos anteriores, relacionada com a lei aplicável, ou se, foi o banco que percebeu se os seus sistemas não chegavam, respondendo:
"(…) a directiva dos sistemas de pagamentos exigia que aumentássemos os níveis ou que fosse sempre aumentados os níveis

de segurança tendo em atenção as realidades tecnológicas que existiam. O S.M.S. era uma delas. Ou seja, ter "algo que eu sei", algo que "eu tenho aqui", tem a ver com três, dois destes mecanismos," algo que eu tenho", "algo que eu sei" ou "algo que eu sou". É um pouco isso. O "algo que eu tenho" aqui, nós tínhamos o cartão-matriz, e o "algo que eu sei"… era dado pelo Pin, pelo login no sistema. O facto de termos aqui… ter-se introduzido também este elemento veio permitir também o token S.M.S. e mais recentemente as próprias apps de autenticação, também foi nesse sentido. O "algo que eu tenho" é o telemóvel e assim e o "algo que eu sei" é o Pin dessa aplicação ou a impressão digital para poder abrir a tal app ou... a impressão digital para poder aceder e o Pin para fazer a operação. Pronto. Mas é sempre dois desses itens. O Banco considerava que tinha um S.M.S code de capacidade. Do ponto de vista da fiabilidade e também, enfim, da directiva dos sistemas de pagamento também … o S.M.S. code … também tem essa característica ...".

Finalmente, os documentos juntos aos autos não permitem retirar alguma ilação no sentido pugnado pela recorrente, de que o acesso tenha sido conseguido por fragilidade ou falta de segurança do serviço ou sistema proporcionado pela ré, nem tal se pode inferir da circunstância de, à data, a ré não ter implementado a certificação por "SMS Code"(Token), elemento que, apenas foi exigido pela legislação que ulteriormente entrou em vigor.

Assim, tendo em conta os elementos de prova produzidos e a ausência de demonstração correspondente, conclui-se que o juízo probatório alcançado pelo Tribunal recorrido, nesta matéria, não merece algum reparo.

A impugnação de facto deduzida pela recorrente quanto às alíneas d) e e) dos factos não provados deverá, pois, improceder.

*****

II) Mérito do recurso:

*****

C) Se não existiu culpa na atuação do representante legal da recorrente e se deve a ré ser condenada no pedido formulado pela autora?

A recorrente, ao nível da decisão de Direito, concluiu que:

"VIII - O representante legal da recorrente, ao atuar da forma descrita nos autos agiu sem culpa, pois que introduziu os seus dados inadvertidamente numa página web em tudo idêntica à do banco recorrido, fazendo-lhe crer que estava na página web verdadeira (…).

X – O risco subjacente a ataques informáticos, ao abrigo do contrato-quadro celebrado entre recorrente e recorrida corre por conta do banco recorrido, quer por força do disposto no art.º 796.º do CC, quer por força do disposto nos artigos 70.º e 71.º do RJPSME, na versão em vigor à data dos factos.

XI – Cabia ao banco recorrido provar que a conduta da recorrente, ao fornecer dados através da página em tudo idêntica à sua, era gravemente negligente o que, atentos os fundamentos supra aduzidos não logrou fazer.
XII – A recorrente tomou as precauções devidas ao usar o serviço de homebanking do banco recorrido, na medida em que dispunha de antivírus atualizado e acedeu à página pelos meios habituais, verificando o endereço respetivo, facto que se impunha dar como comprovado (…)".
A argumentação alinhada para tal efeito, pela recorrente, assenta, em suma, no seguinte:
- Que nada poderia fazer crer (ou desconfiar) ao representante legal da recorrente, que não se encontrava na página web do banco recorrido, nem mesmo quando, nesse preciso contexto, lhe foi solicitada uma atualização do cartão matriz;
- Que o representante legal não se encontrava, de momento, a realizar qualquer operação bancária;
- Que o alerta feito pelas instituições bancárias quanto à não divulgação de coordenadas do cartão matriz reporta-se, especificamente, à realização de operações bancárias;
- Que o fornecimento de tais elementos ocorreu após o Autor ter introduzido o seu username e PIN e ter visualizado o seu saldo bancário, sendo que, depois de introduzir tais elementos de segurança e estando visualmente perante o seu saldo bancário, ao qual apenas pode ter acesso quem dispõe também do username e do PIN, não era expectável que outra entidade aí pudesse intervir, que não o banco;
- Que à data da ocorrência dos factos (início de novembro de 2015), o representante legal utilizava o serviço há cerca de um ano e dez meses e a consciencialização para os riscos associados ao uso de serviços de homebanking não era, à data, tão intensa ou generalizada como é aos dias de hoje;
- Que os dados de acesso ao serviço de homebanking apenas foram fornecidos inadvertidamente, por recurso a um ardil que nunca seria possível ao representante legal da recorrente detetar, pela natureza e modo como ocorreram, nem poderia desconfiar de que se tratava de uma página falsa/forjada;
- Que, tendo presente o nível de sofisticação empregue no *pharming*, deveria o banco recorrido ter dotado o seu sistema informático de todos os meios de segurança ao seu dispor – em particular, o SMS token, sendo que, o representante legal da recorrente tinha antivírus ativado e atualizado no seu computador;
- Que não houve incumprimento de qualquer dever contratual por parte da recorrente, mormente o dever de guarda das credenciais pessoais; e
- Que inexistindo culpa por parte da recorrente, por não se ter logrado prova-lo, deveria o tribunal a quo ter aplicado o disposto

no art.º 796.º do CC e artigos 70.º e 71.º, ambos do RJSPME.
Vejamos:
Preliminarmente – e considerando ademais que não foi colocada qualquer questão a este respeito pela recorrente - a decisão recorrida não nos merece qualquer reparo quanto ao enquadramento jurídico levado a efeito relativamente à qualificação da relação jurídica estabelecida: No âmbito do contrato de abertura de conta ou de conta bancária, a autora e a ré outorgaram um denominado contrato de "homebanking", designado por "Montepio 24 – Empresas".
Efetivamente, conforme se sublinhou no Acórdão do Tribunal da Relação de Lisboa de 24 de maio de 2012 (Pº 192119/11.8YIPRT.L1-2, rel. EZAGÜY MARTINS), ***"o contrato de conta bancária - enquanto contrato nuclear instituinte do tronco comum sobre o qual repousarão todas as relações jurídicas entre banco e cliente, inclusive contratuais, possui um conteúdo negocial complexo do qual fazem parte, necessária ou usualmente, outras convenções acessórias embora autónomas: tal o caso do contrato de contacorrente bancária e do contrato de depósito."***
E, conforme evidencia (Inês Custódio Alves; Operações abusivas na banca eletrónica – A imputação de responsabilidades pelas perdas resultantes da movimentação não autorizada de fundos; FDUNL, 2019, p. 14), ***"[d]ecorrentes do fenómeno de evolução tecnológica, recrudesceram novas práticas no setor bancário, nomeadamente associadas à digitalização financeira, fenómeno que trouxe novos serviços financeiros de retalho caracterizados pela simplicidade e celeridade na utilização dos serviços de pagamento. Assim, assistimos ao acesso à distância de operações bancárias, assim como aos inúmeros serviços decorrentes da utilização de serviços de pagamento, cujo modus operandi decorre por via da Internet".***
Surge, assim, o serviço de ***"homebanking"*** **– do inglês banco em casa - que se revela, no plano jurídico, como uma 'teia' de contratos, a uma série de relações jurídicas complexas:** ***"o contrato de emissão ou de utilização não surge como uma "ilha", como um facto jurídico isolado, gerador de uma relação jurídica única entre determinados sujeitos jurídicos. Antes integra um conjunto mais complexo de relações que se estabelecem, por um lado, entre os mesmos sujeitos, e, por outro, entre estes e terceiros"*** **(cfr. Maria Raquel Guimarães; O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos; Coimbra, Wolters Kluwer/Coimbra Editora, 2011, pp.174-175 e 180).**
"O contrato de "homebanking" – que a lei também qualifica de "contrato-quadro" (art. 2.º, al. m), do Regime dos Sistemas de Pagamento (RSP), aprovado pelo DL n.º 317/2009, de 30-10) – celebrado entre autora e banco réu – é o acordo mediante o qual o cliente adere a um serviço prestado pelo banco, que consiste na possibilidade de manter relações via internet, de forma a: (i) aceder

a informações sobre produtos e serviços do banco; (ii) obter informações e realizar operações bancárias sobre contas de que a autora fosse titular; (iii) realizar pagamentos, cobranças e operações de compra, venda, subscrição ou resgate sobre produtos ou serviços disponibilizados pelo banco" **(assim, o Acórdão do Supremo Tribunal de Justiça de 14-12-2016, Pº 1063/12.1TVLSB.L1.S1, rel. PINTO DE ALMEIDA).**

O acordo de "homebanking", permite a simplificação de processos e operações disponibilizados pelo banco ao cliente, possibilitando-lhe um acesso mais continuado e rápido e, permitindo-lhe a realização de outras operações, bem como a obtenção de vários serviços, de forma em princípio mais cómoda e, simultaneamente, poupanças de escala, por parte do banco (cfr., neste sentido, o Acórdão do Tribunal da Relação de Guimarães de 30-05-2013, Pº 6479/09.8TBBRG.G1, rel. RITA ROMEIRA).

Conforme se referenciou no Acórdão do Supremo Tribunal de Justiça de 18-12-2013 (Pº 6479/09.8TBBRG.G1.S1, rel. ANA PAULA BOULAROT), caraterizando o serviço de "homebanking": ***"Entramos aqui no chamado «home banking», Banco internético (do inglês Internet banking), ebanking, banco online, online banking, às vezes também banco virtual, banco electrónico), concretizado pela possibilidade conferida pela entidade bancária aos seus clientes, mediante a aceitação de determinados condicionalismos, a utilizar toda uma panóplia de operações bancárias, online, relativamente às contas de que sejam titulares, utilizando para o efeito canais telemáticos que conjugam os meios informáticos com os meios de comunicação à distância (canais de telecomunicação), por meio de uma página segura do banco, o reveste de grande utilidade, especialmente para utilizar os serviços do banco fora do horário de atendimento ou de qualquer lugar onde haja acesso à Internet.".***

O enquadramento do ***"homebanking"*** **no seio da relação bancária inicia-se, assim, com a celebração do contrato de abertura de conta, entendido como um contrato bancário-matriz, no qual é constituído o quadro geral de regulação de negócio que venha a ser posteriormente celebrado pelas partes.**

Neste sentido, ***"a realização de operações de home banking – transferências electrónicas, pagamentos de serviços, entre outras – pressupõe um complexo de contratos que permite regular, de antemão, as relações entre o banco prestador do serviço e o seu cliente, utilizador do mesmo, simplificando os procedimentos a adoptar no momento em que essas operações são concretizadas"*** **(cfr. Maria Raquel Guimarães; O contrato-quadro no âmbito da utilização de meios de pagamento electrónicos; Coimbra, Wolters Kluwer/Coimbra Editora, 2011, p. 58).**

Assim, autónomo, mas interdependente em relação a outros contratos bancários, inserindo-se, normalmente, no âmbito de um

contrato-quadro de abertura de conta, da celebração do acordo de *"homebanking"* decorre uma complexidade de direitos e deveres que regulam a relação obrigacional, duradoura, entre as partes, relativamente ao utilizador e prestador de serviços de pagamento, constituindo uma das funcionalidades habituais desse acordo, a da possibilidade de o cliente bancário poder realizar e ordenar ao seu banco a realização de operações de pagamento.
Sobre a matéria dos deveres inerentes a cada uma das partes celebrantes do acordo respetivo regulava, à data dos factos, 2015, o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (abreviadamente RJSPME, aprovado pelo D.L. n.º 317/2009, de 30 de outubro, alterado pelo D.L. n.º 242/2012, de 7 de novembro e pelo D.L. n.º 157/2014, de 24 de outubro, que transpôs para a ordem jurídica portuguesa a Diretiva 2007/64/CE (regime jurídico este que, por força da transposição para a ordem jurídica portuguesa da Diretiva (UE) 2015/2366, do Parlamento Europeu e do Conselho, de23 de novembro de 2015, pelo D.L. n.º 91/2018, de 12 de novembro, veio a ser revogado ulteriormente, mas cujas disposições, atenta a data dos factos, não são aplicáveis à situação jurídica em apreço).
Nos termos desse regime jurídico constituíam "serviços de pagamento", a prestar pelas instituições previstas no artigo 7.º, entre os quais, as instituições de crédito e sociedades financeiras, as seguintes atividades:
"a) Serviços que permitam depositar numerário numa conta de pagamento, bem como todas as operações necessárias para a gestão dessa conta;
b) Serviços que permitam levantar numerário de uma conta de pagamento, bem como todas as operações necessárias para a gestão dessa conta;
c) 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, tais como:
i) A execução de débitos diretos, incluindo os de carácter pontual;
ii) A execução de operações de pagamento através de um cartão de pagamento ou de um dispositivo semelhante;
iii) A execução de transferências a crédito, incluindo ordens de domiciliação;
d) Execução de operações de pagamento no âmbito das quais os fundos são cobertos por uma linha de crédito concedida a um utilizador de serviços de pagamento, tais como:
i) A execução de débitos diretos, incluindo os de carácter pontual;
ii) A execução de operações de pagamento através de um cartão de pagamento ou de um dispositivo semelhante;
iii) A execução de transferências a crédito, incluindo ordens de domiciliação;
e) Emissão ou aquisição de instrumentos de pagamento;

f) Envio de fundos;
g) Execução de operações de pagamento em que o consentimento do ordenante para a execução da operação de pagamento é comunicado através de quaisquer dispositivos de telecomunicações, digitais ou informáticos, e o pagamento é efetuado ao operador da rede ou do sistema de telecomunicações ou informático, agindo exclusivamente como intermediário entre o utilizador do serviço de pagamento e o fornecedor dos bens e serviços" **(cfr. artigo 4.º)**
O RJSPME, na referida redação, estabelece diversas normas sobre o modo de autorização das operações de pagamento, dispondo, em particular, o seguinte:
"Artigo 65.º
Consentimento e retirada do consentimento
1 - Uma operação de pagamento ou um conjunto de operações de pagamento só se consideram autorizados se o ordenante consentir na sua execução.
2 - O consentimento deve ser dado previamente à execução da operação, salvo se for acordado entre o ordenante e o respetivo prestador do serviço de pagamento que o mesmo seja prestado em momento posterior.
3 - O consentimento referido nos números anteriores deve ser dado na forma acordada entre o ordenante e o respetivo prestador do serviço de pagamento, sendo que, em caso de inobservância da forma acordada, se considera que a operação de pagamento não foi autorizada.
4 - O consentimento pode ser retirado pelo ordenante em qualquer momento, mas nunca depois do momento de irrevogabilidade estabelecido nos termos do artigo 77.º
5 - O consentimento dado à execução de um conjunto de operações de pagamento pode igualmente ser retirado, daí resultando que qualquer operação de pagamento subsequente deva ser considerada não autorizada.
6 - Os procedimentos de comunicação e de retirada do consentimento são acordados entre o ordenante e o prestador do serviço de pagamento.
Artigo 66.º
Limites da utilização do instrumento de pagamento
1 - Nos casos em que é utilizado um instrumento específico de pagamento, para efeitos de comunicação do consentimento, o ordenante e o respetivo prestador do serviço de pagamento podem acordar em limites de despesas para as operações de pagamento executadas através do instrumento de pagamento em questão.
2 - Mediante estipulação expressa no contrato quadro, o prestador de serviços de pagamento pode reservar-se o direito de bloquear um instrumento de pagamento por motivos objetivamente fundamentados, que se relacionem com:
a) A segurança do instrumento de pagamento;
b) A suspeita de utilização não autorizada ou fraudulenta desse

instrumento; ou
c) O aumento significativo do risco de o ordenante não poder cumprir as suas responsabilidades de pagamento, caso se trate de um instrumento de pagamento com uma linha de crédito associada.
3 - Nos casos referidos no número anterior, o prestador do serviço de pagamento deve informar o ordenante do bloqueio do instrumento de pagamento e da respetiva justificação pela forma acordada, se possível antes de bloquear o instrumento de pagamento ou, o mais tardar, imediatamente após o bloqueio, salvo se tal informação não puder ser prestada por razões de segurança objetivamente fundamentadas ou se for proibida por outras disposições legais aplicáveis.
4 - Logo que deixem de se verificar os motivos que levaram ao bloqueio, o prestador do serviço de pagamento deve desbloquear o instrumento de pagamento ou substituí-lo por um novo.
Artigo 67.º
Obrigações do utilizador de serviços de pagamento associadas aos instrumentos de pagamento
1 - O utilizador de serviços de pagamento com direito a utilizar um instrumento de pagamento tem as seguintes obrigações:
a) Utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização; e
b) Comunicar, sem atrasos injustificados, ao prestador de serviços de pagamento ou à entidade designada por este último, logo que deles tenha conhecimento, a perda, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento.
2 - Para efeitos da alínea a) do número anterior, o utilizador de serviços de pagamento deve tomar todas as medidas razoáveis, em especial ao receber um instrumento de pagamento, para preservar a eficácia dos seus dispositivos de segurança personalizados.
Artigo 68.º
Obrigações do prestador de serviços de pagamento associadas aos instrumentos de pagamento
1 - O prestador de serviços de pagamento que emite um instrumento de pagamento tem as seguintes obrigações:
a) Assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento, sem prejuízo das obrigações do utilizador do serviço de pagamento estabelecidas no artigo anterior;
b) Abster-se de enviar instrumentos de pagamento não solicitados, salvo quando um instrumento deste tipo já entregue ao utilizador de serviços de pagamento deva ser substituído;
c) Garantir a disponibilidade, a todo o momento, de meios adequados para permitir ao utilizador de serviços de pagamento proceder à notificação prevista na alínea b) do n.º 1 do artigo anterior ou solicitar o desbloqueio nos termos do n.º 4 do artigo

66.º;
d) O prestador do serviço de pagamento deve facultar ao utilizador do serviço de pagamento, a pedido deste, os meios necessários para fazer prova, durante 18 meses após a notificação prevista na alínea b) do n.º 1 do artigo anterior, de que efetuou essa notificação; e
e) Impedir qualquer utilização do instrumento de pagamento logo que a notificação prevista na alínea b) do n.º 1 do artigo anterior tenha sido efetuada.
2 - O risco do envio ao ordenante de um instrumento de pagamento ou dos respetivos dispositivos de segurança personalizados corre por conta do prestador do serviço de pagamento.
Artigo 69.º
Comunicação de operações de pagamento não autorizadas ou incorretamente executadas e direito de retificação
1 - O utilizador do serviço de pagamento tem o direito de obter retificação, por parte do prestador do serviço de pagamento, se, após ter tomado conhecimento de uma operação de pagamento não autorizada ou incorretamente executada suscetível de originar uma reclamação, nomeadamente ao abrigo dos artigos 86.º e 87.º, comunicar o facto ao respetivo prestador do serviço de pagamento sem atraso injustificado e dentro de um prazo nunca superior a 13 meses a contar da data do débito.
2 - Sempre que, relativamente à operação de pagamento em causa, o prestador do serviço de pagamento não tenha prestado ou disponibilizado as informações a que está obrigado nos termos do capítulo i do presente título iii, não é aplicável a limitação de prazo referida no número anterior"
Conforme decorre da previsão dos citados artigos 67.º e 68.º relativamente aos serviços de pagamento, decorrem obrigações e deveres a observar, quer pelo utilizador desses serviços, quer pelo prestador de tais serviços.
Com efeito, como se assinalou ainda antes da vigência do RJSPME, a respeito da utilização de cartões bancários, mas cujas considerações são inteiramente atuais, *"o risco não tem que ser suportado apenas pelo banco, assim como não tem de o ser unicamente pelo titular do cartão. Se alguém tira proveito de uma coisa, sob tutela jurídica, justifica-se, por equitativo, que suporte os prejuízos que a sua utilização acarreta. Se é certo que só o banco está em condições de impedir o uso indevido do cartão após comunicação do seu titular, também é verdade que este até pode não ter tomado prévio conhecimento da sua utilização abusiva e nem ter qualquer responsabilidade nessa indevida utilização."*
(assim, o Acórdão do Supremo Tribunal de Justiça de 15-10-2009, Pº 29368/03.5TJLSB.S1, rel. ALBERTO SOBRINHO).
A entidade bancária confere aos seus clientes a possibilidade de utilização de um serviço de *homebanking* para movimentação dos fundos. Esta é a prestação principal do banco que confere aos utilizadores a possibilidade de usufruir de um serviço que lhes

permita a gestão e movimentação dos fundos disponíveis nas suas contas bancárias.
Assim, o utilizador tem os seguintes deveres:
- Utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, devendo tomar todas as medidas razoáveis, em especial ao receber um instrumento de pagamento, para preservar a eficácia dos seus dispositivos de segurança personalizados;
- Comunicar, sem atrasos injustificados, ao prestador de serviços de pagamento ou à entidade designada por este último, logo que deles tenha conhecimento, a perda, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento.
Conforme evidencia Carolina França Barreira (*"Home banking: A Repartição dos prejuízos decorrentes de fraude informática", in* Revista Electrónica de Direito; Outubro 2015, n.º 3, pp. 18-19), a respeito dos deveres do utilizador:
"No contrato de home banking, verificamos que são impostos expressamente deveres acessórios de conduta, sobretudo ao utilizador. Estes deveres são autónomos dos deveres principais e distintos dos deveres secundários, revelando-se essenciais ao correto processamento da relação contratual. 80 Os deveres acessórios de conduta podem derivar de uma cláusula contratual, de dispositivo da lei ad hoc ou do princípio da boa-fé (n.º 2 do artigo 762º do Código Civil, doravante, CC) que consagra genericamente esta categoria de deveres no âmbito das obrigações. O seu incumprimento, apesar de constituir a violação de deveres inscritos na relação obrigacional, não dá origem a uma ação judicial de cumprimento (artigo 817º do CC), podendo apenas gerar a obrigação de indemnizar os danos dela resultantes.
No caso do contrato de banca eletrónica, a positivação dos deveres acessórios de conduta no RSP e no clausulado do contrato deve-se ao seu carácter duradouro e à especial relação de confiança entre as partes. Assim, o utilizador do serviço tem a seu cargo um conjunto de deveres acessórios de conduta conexos com a segurança do sistema.
O primeiro a destacar é o dever de o utilizador tomar todas as medidas razoáveis para preservar a eficácia dos mecanismos de segurança personalizados associados ao instrumento de pagamento (n.º 2 do artigo 67º do RSP), no caso do home banking, os códigos de acesso a este serviço.
As chaves de acesso conferidas pela instituição bancária, usualmente inscritas num cartão matriz, constituem "dispositivos de segurança personalizados" tendo uma função de autenticação, de acordo com o disposto na alínea v) do artigo 2º do RSP. Assim, o conhecimento do conjunto de senhas confidenciais que, através da sua marcação no teclado do computador, permitem aceder ao serviço de home banking e realizar determinadas operações é o

meio utilizado para identificar e imputar as operações realizadas ao seu utilizador87. Face à essencialidade do conhecimento dos códigos de acesso para cumprir a função de autenticação, o utilizador fica, naturalmente, vinculado ao dever de garantir a segurança desses elementos, não facultando a sua utilização a terceiros (n.º 2 do artigo 67º do RSP). Este dever de confidencialidade quanto aos dados pessoais que permitem o acesso ao serviço de banca eletrónica é fundamental visto que é impossível realizar qualquer transferência através daquele serviço sem a introdução das chaves de acesso que constam do cartão matriz e que são aleatoriamente escolhidas pelo sistema informático, além de que uma vez digitada a chave correta, o sistema valida-a e presume que está perante o seu verdadeiro portador. Através destes códigos de acesso, o banco pretende verificar a coincidência entre a pessoa que pretende aceder ao serviço de home banking e o cliente que subscreveu o respetivo contrato, isto é, o credor do serviço eletrónico que a instituição bancária se obrigou a prestar. Este dever de não divulgação dos códigos de acesso costuma constar expressamente do contrato de banca eletrónica a que o cliente aderiu, assim como decorre das regras que, segundo um padrão de normalidade, o comum utilizador da internet sabe que devem ser observadas.

A este, acresce um outro dever acessório de conduta do utilizador, o dever de comunicação imediata ao banco da utilização abusiva do instrumento de pagamento. Este dever é, geralmente, imposto contratualmente mas, mesmo que assim não fosse, sempre decorria da especial relação de confiança entre o banco e o cliente (…)".

O cumprimento destes deveres do utilizador tem sido analisado em diversas situações. Por exemplo, concluiu-se já que, *"quem traz o PIN numa agenda acessível a qualquer pessoa que a leia infringe de forma grave um dever contratual, pelo que a imputação de culpa do titular nos parece incontroversa"* (assim, o Acórdão do Supremo Tribunal de Justiça de 02-03-2010, Pº 29371/03.5TJLSB.S1, rel. URBANO DIAS; e também, o Acórdão do Tribunal da Relação de Lisboa de 04-07-2013, Pº 103841/11.3YIPRT.L1-2, rel. ONDINA CARMO ALVES).

Por seu turno, constituem obrigações do prestador de serviços de pagamento associadas aos instrumentos de pagamento, as seguintes:

- Assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento (sem prejuízo das obrigações do utilizador do serviço de pagamento);

- Abster-se de enviar instrumentos de pagamento não solicitados, salvo quando um instrumento deste tipo já entregue ao utilizador de serviços de pagamento deva ser substituído;

- Garantir a disponibilidade, a todo o momento, de meios

adequados para permitir ao utilizador de serviços de pagamento proceder à notificação de comunicação de perda, roubo, apropriação abusiva ou utilização não autorizada do instrumento de pagamento ou de solicitação de desbloqueio nos termos do n.º 4 do artigo 66.º;
- Facultar ao utilizador do serviço de pagamento, a pedido deste, os meios necessários para fazer prova, durante 18 meses após a notificação de comunicação de perda, roubo, apropriação abusiva ou utilização não autorizada do instrumento de pagamento, de que efetuou essa notificação; e
- Impedir qualquer utilização do instrumento de pagamento logo que a notificação da mencionada comunicação tenha sido efetuada.
À entidade bancária cabe, a título principal, aceitar os sucessivos mandatos para pagamentos emitidos mediante a correta autenticação por parte do cliente, nos limites do saldo disponível da conta à ordem, ou na medida em que tenha sido previsto anteriormente a possibilidade de realizar operações a descoberto, ou do crédito concedido nos casos de abertura de crédito.
Como dever secundário acessório desta prestação principal, o banco deve entregar ao utilizador o cartão matriz e todos os códigos de acesso necessários à utilização do serviço de banca eletrónica, o que constitui um pressuposto essencial do acesso legítimo ao serviço uma vez que, sem os dispositivos de segurança personalizados na sua posse, o utilizador não consegue aceder ao serviço online.
A este propósito, reporta Carolina França Barreira (*"Home banking: A Repartição dos prejuízos decorrentes de fraude informática", in* Revista Electrónica de Direito; Outubro 2015, n.º 3, pp. 20-21) que:
"Sem prejuízo dos deveres que incumbem ao utilizador e tendo em conta que o funcionamento do sistema de home banking depende da utilização de meios informáticos que têm inerentes riscos próprios, o que pressupõe um comportamento diligente de ambas as partes95, ao banco cabe assegurar que os mecanismos de segurança personalizados associados ao instrumento de pagamento só sejam acessíveis ao utilizador a quem foi conferido o direito à sua utilização (alínea a) do n.º 1 do artigo 68º do RSP).
De forma a concretizar este dever acessório de conduta da entidade bancária, a lei acrescenta que cabe ao banco comunicar, como medida preventiva, "se for caso disso, uma descrição das medidas que o utilizador do serviço de pagamento deve tomar para preservar a segurança dos instrumentos de pagamento" (subalínea i) da alínea e) do artigo 53º do RSP). Assim, recai sobre a instituição bancária um reforçado dever de informação que consiste em elucidar o cliente quanto aos casos mais frequentes de fraude e aos perigos inerentes à utilização do serviço que se comprometeu a prestar, sempre tendo em consideração o tipo de utilizador e os seus

conhecimentos técnicos; não sendo, por isso, suficiente que o banco permita ao seu cliente aceder ao serviço de banca eletrónica, fornecendo-lhe as chaves de acesso. Assim, é frequente os bancos fazerem certas recomendações aos seus clientes a fim de os prevenirem relativamente à utilização do serviço de home banking, designadamente no sentido de não abrir mensagens de correio eletrónico cujo remetente seja desconhecido, não executar ficheiros não solicitados, ter sempre um antivírus atualizado no computador e não aceder à página do banco através de atalhos (não aceder por um link de uma mensagem de correio eletrónico, nem pelos "favoritos"), devendo digitar-se diretamente o site da entidade bancária na barra de pesquisa. É ainda aconselhado pelo banco utilizar computadores de confiança para aceder ao serviço de home banking, nunca fornecer senhas de acesso a contas bancárias a pedido do banco por correio eletrónico ou telefone e, em caso de dúvida, contactar a entidade bancária antes de fornecer quaisquer dados. Estes cuidados permitem evitar um ataque fraudulento, porém, mesmo que rigorosamente respeitados, não impedem intrusões por parte de piratas informáticos que põem o sistema permanentemente à prova (…). O referido dever justifica-se dada a complexidade do sistema informático que suporta o serviço de banca eletrónica e, principalmente, o risco de ocorrerem utilizações fraudulentas potenciadas pelo facto de as operações bancárias serem realizadas em "ambiente aberto", através da internet e não numa rede privativa do banco. Este é um dever acessório de conduta que decorre particularmente da especial relação de confiança entre a instituição bancária e o seu cliente, tendo a sua origem no contrato de abertura de conta. Desta forma, o banco procura alertar os seus clientes para o cumprimento dos deveres de segurança que devem ser observados na execução do contrato, de modo a que possam aceder às suas contas e movimentá-las em segurança, sem que terceiros desviem dinheiro das mesmas para outras.

Sendo a segurança do serviço uma das questões fundamentais do home banking, é essencial que o banco utilize uma tecnologia de encriptação (codificação) que garanta a confidencialidade das comunicações entre a entidade bancária e o seu cliente (…)".

Sintetizando, pode dizer-se que: *"A entidade bancária tem o dever de prestar um serviço eficaz e seguro e por sua vez, sobre o cliente/ utilizador impõe-se os deveres acessórios de conduta, como de utilização correta do serviço e de confidencialidade relativamente ao código de acesso pessoal à conta e aos dispositivos de segurança personalizados fornecidos pela entidade bancária, nomeadamente chaves de acesso, (v.g. inscritas num "cartão matriz") e que tem função de autenticação das operações, as quais são fundamentais para a realização de transferências"* (assim, o Acórdão do Tribunal da Relação do Porto de 04-06-2019, Pº 1482/17.7T8PRD.P2, rel. ALEXANDRA PELAYO).

Realizado o enquadramento da relação obrigacional inerente ao contrato de homebanking, certo é que, a banca eletrónica (prestação de serviços bancários com recurso a meios tecnológicos, através da Internet) se defronta com os riscos de utilização de esquemas fraudulentos inerentes à disponibilização de tais meios.
Os referidos meios – possibilitando a Internet, designadamente, o anonimato, a celeridade de transações e a possibilidade de atividades transfronteiriças – são, assim, frequentemente alvo de ataque, pelos vulgarmente designados *"hackers, com objetivo de se apropriarem, de forma ilícita, dos fundos existentes nas contas bancárias"* (assim, o Acórdão do Tribunal da Relação de Coimbra de 11-02-2020, Pº 8592/17.9T8CBR.C1, rel. ISAÍAS PÁDUA).
Entre esses esquemas fraudulentos contam-se os denominados, *"phishing"; "pharming", "spam", "SMiShing", "vishing", "skimming",* assim como, a utilização de software tipicamente classificado como *"malware"* (programas informáticos destinados a perturbar, alterar ou destruir todos, ou parte, dos módulos indispensáveis ao bom funcionamento de um sistema informático, como seja, os vírus, o *"trojan horse",* o mecanismo de *"keylogger"* ou o *"spyware"*).
No Acórdão do Supremo Tribunal de Justiça de 18-12-2013 (Pº 6479/09.8TBBRG.G1.S1, rel. ANA PAULA BOULAROT), distinguiu-se a figura do *"phishing"* e do *"pharming"* nos seguintes moldes: *"O phishing (do inglês fishing «pesca») pressupõe uma fraude electrónica caracterizada por tentativas de adquirir dados pessoais, através do envio de e-mails com uma pretensa proveniência da entidade bancária do receptor, por exemplo, a pedir determinados elementos confidenciais (número de conta, número de contrato, número de cartão de contribuinte ou qualquer outra informação pessoal), por forma a que este ao abri-los e ao fornecer as informações solicitadas e/ou ao clicar em links para outras páginas ou imagens, ou ao descarregar eventuais arquivos ali contidos, poderá estar a proporcionar o furto de informações bancárias e a sua utilização subsequente (…). A outra modalidade de fraude online é o pharming a qual consiste em suplantar o sistema de resolução dos nomes de domínio para conduzir o usuário a uma pagina Web falsa, clonada da página real, baseando-se o processo, sumariamente, em alterar o IP numérico de uma direcção no próprio navegador, através de programas que captam os códigos de pulsação do teclado (os ditos keyloggers), o que pode ser feito através da difusão de vírus via spam, o que leva o usuário a pensar que está a aceder a um determinado site – por exemplo o do seu banco – e está a entrar no IP de uma página Web falsa, sendo que ao indicar as suas chaves de acesso, estas serão depois utilizadas pelos crackers, para acederem à verdadeira página da instituição bancária e aí poderem efectuar as operações que entenderem, destinando-se ambas as*

técnicas (phishing e pharming) à obtenção fraudulenta de fundos".
**Semelhante distinção foi empreendida no Acórdão do Tribunal da Relação de Lisboa de 12-07-2018 (Pº 2256/17.0T8LSB.L1-7, rel. HIGINA CASTELO), nos termos seguintes: "*O phishing é uma atividade fraudulenta que se inicia com o envio de um e-mail que parece proveniente de outra entidade (nomeadamente bancária) e no qual é sugerido, sob pretextos vários, que o destinatário aceda à página Web (site) do suposto remetente através de uma hiperligação (link) contida no e-mail; depois de agir da solicitada forma, o destinatário do e-mail entra numa página falsa, provavelmente de aspeto parecido ao da entidade pela qual o autor do phishing se faz passar, e introduz os dados necessários para a entrada (login), como o seu nome de utilizador (username) e a palavra-passe, entre outros. As credenciais do destinatário do e-mail serão depois utilizadas pelo phisher para entrar no verdadeiro site da entidade (bancária ou outra) como se fosse o legítimo titular das credenciais, com vista à execução de ações ilícitas, nomeadamente apropriação de fundos alheios. No pharming o utilizador de internet é conduzido a uma página falsa na sequência (quase sempre) da instalação no seu computador de um programa malicioso destinado a redirecionar nomes de domínio (endereços de sites) por si pesquizados para sites fraudulentos. Para conseguir instalar nos computadores alheios esse programa viral, o pharmer envia e-mail de spam que o atingido abre e na sequência do qual toma uma determinada ação, nomeadamente clicando nalgum link do mesmo".*
A respeito do "*pharming*", dá nota Ana Helena França Azevedo (Burlas Informáticas: Modos de Manifestação, Universidade do Minho – Escola de Direito, Janeiro de 2016, em: https://repositorium.sdum.uminho.pt/bitstream/1822/44510/1/Ana%20Helena%20Fran%c3%a7a%20Azevedo.pdf, pp. 77-79):
"Uma outra variante de fraude online, mais aprimorada e perigosa, é o Pharming (farming conjugado com phishing). Esta técnica, para além de pressupor um processo técnico mais avançado, tem como finalidade o furto de dados sensíveis, nomeadamente números de cartão de crédito, dados de conta, senhas, entre outros. Diferentemente com o que sucede no phishing, o pharming pressupõe um controlo de um ponto de uma infraestrutura de comunicação. O ataque mais frequente, em sede de pharming é o comprometimento do router, melhor dizendo, todos aqueles utilizadores que utilizam aquela infraestrutura serão explorados simultaneamente porque o atacante consegue controlar parte da rede onde passa essa informação. Outra forma de ataque tem lugar quando o delinquente usa um processo denominado como "DNS cache poisoning" que consiste em suplantar o sistema de resolução dos nomes de domínio (DNS), alterando a configuração do servidor DNS do sistema, com vista a conduzir/redirecionar os utilizadores para uma página web falsa, clonada da real ou alterando o host file

no computador da vítima. Tanto o servidor DNS como o host file contêm direções dos IPs ou sequência numérica das direções URL das páginas visitadas. Assim o pharming muda as direções de IP contidas no servidor DNS ou no host file, conduzindo o utilizador a uma página em tudo idêntica à da pretendida. Não obstante, ressalvamos que a clonagem de páginas web falsas também tem lugar em sede de phishing, nomeadamente quando se recebe na caixa de correio eletrónico e-mails duvidosos, com links de supostamente entidades fidedignas. Em matéria de pharming, Pedro Verdelho pronunciou-se referindo-se à difusão de ficheiros ocultos que se auto-instalam nos computadores e uma vez alojados, alteram de forma oculta os arquivos do sistema., designadamente os ficheiros contendo os "favoritos" e o registo de cookies, de modo a que o utilizador quando aceder ao seus habitual site bancário é redirecionado para um outro site construído e disponibilizado em métodos idênticos ao do phishing, tornando muito difícil reconhecer uma fraude.

O processo do ataque de pharming funda-se em aceder ao servidor DNS e modificar as direções URL e de IP numérico no próprio browser reconduzindo as vítimas para um DNS controlado pelos delinquentes. A vítima escreve o URL correto, mas desconhece que a tradução daquele nome resulta de um endereço IP de um site que é uma cópia do site original, criado, gerido e desenhado por um atacante. Neste caso a vítima é ludibriada pelo servidor DNS que foi subvertido pelo atacante, criando desta forma a sua própria "quinta" (pharm(farm)) composta pelas vítimas. A vítima e o servidor desconhecem que estão a ser alvo de um ataque de pharming. Trata-se geralmente de cópias de sites de instituições bancárias. A vítima para «autenticar» a sua operação indica as suas chaves de acesso, sendo que as mesmas serão depois utilizadas pelos crackers, para acederem à verdadeira página da instituição bancária e aí poderem efetuar as operações que entenderem, e portanto, subtrair o património da vítima. Esta entrada na tabela de endereços IPs direcionada a uma página que se crê ser a página original, sendo a página maliciosa, é o elemento caracterizador do pharming.

Resumidamente:

1. o delinquente ataca o servidor DNS usado pela vítima, alterando o IP associado ao url «www.bank.com» para um outro IP ilegítimo de um servidor que contém uma réplica desse site;

2. A vítima introduz o endereço «www.bank.com»;

3. O computador questiona o servidor DNS para saber o IP do URL «www.bank.com»;

4. O servidor DNS devolve o IP usado pelo delinquente;

5. A vítima é direcionada para o site falso.

O ataque cache poisoning é, potencialmente, o ataque mais proeminente e perigoso em matéria de DNS. O protocolo DNS é intrinsecamente vulnerável ao ataque cache poisoning provocando

o comprometimento da integridade e segurança do sistema. Tanto a técnica de phishing como a de pharming visam a obtenção fraudulenta de quantias monetárias, logo os agentes criminosos estarão a consumir o crime de burla informática. A grande diferença entre o phishing e o pharming, é a pessoa que é atacada; No phishing a vítima é convidada a seguir links aparentemente genuínos, mas que não o são ao passo que no pharming recebe-se os links genuínos e a vítima é convidada a revelar os dados sensíveis, sendo que o elemento comprometido é o router (normalmente existe um DNS no router). Portanto, o phishing estará no "client-side", ao passo que o pharming no "server-side". Do ponto de vista do utilizador, deverá ter comportamentos preventivos na medida em que quando introduz dados sensíveis está a fazê-lo através de HTTPS e não de HTTP. Desta forma assegura que o homólogo de comunicação é genuíno através da utilização de protocolos de comunicação seguros" **(cfr., sobre a temática, para maiores desenvolvimentos, entre outros: M. Januário da Costa Gomes, Contratos Comerciais, 2013, Almedina, págs. 220 a 252, especialmente págs. 239-248; Ana Helena França Azevedo; Burlas Informáticas: Modos de Manifestação, Universidade do Minho – Escola de Direito, Janeiro de 2016; Carolina França Barreira; *"Home banking: A Repartição dos prejuízos decorrentes de fraude informática", in* Revista Electrónica de Direito; Outubro 2015, n.º 3, pp. 2-68; Pedro Verdelho; "*Phishing e outras formas de defraudação nas redes de comunicação", in* Direito da Sociedade da Informação (Oliveira Ascensão, coord.). Vol. VIII. Coimbra, Coimbra Editora, 2009, pp. 407-419; Maria Raquel Guimarães; *"A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica (home banking): anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09", in* Cadernos de Direito Privado, Braga, CEJUR. Nº 41, janeiro/março 2013, pp. 45-69; José Manuel Faria; *"Acesso a contas bancárias por terceiros no âmbito de operações de pagamento", in* Revista da Banca, Associação Portuguesa de Bancos. N.º 71, janeiro/junho 2011, pp. 25-39; Verónica Santos; As debilidades do serviço de homebanking, em especial quanto aos crimes de fraude informática de phishing e pharming. A questão da responsabilidade no âmbito das operações bancárias não autorizadas, UCP, 2018; Bruno Silva Palhão; Operações não autorizadas e repartição dos prejuízos: O homebanking na jurisprudência do RSP, UCP, Abril de 2008; Raquel Sofia Ribeiro de Lima; *"A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa", in* Revista Electrónica de Direito; Outubro 2016, n.º 3, pp. 2-62; Maria Teresa Resende Neiva Martins da Silva; A responsabilidade dos bancos em casos de phishing e pharming, FDUC, 2021; António Ramos Carvalho; *"O fenómeno do phishing", in* Cyberlaw, Edição n.º IX, Março 2020, FDUL -**

CIJIC, pp. 81-102; Soraia Armanda Oliveira da Silva; A responsabilidade civil no âmbito do contrato de homebanking; Univ. Minho, outubro de 2015; e Rui Elói Ferreira e Carolina Inverno Branco; Phishing: riscos e prevenção, disponível em: http://carlospintodeabreu.com/public/files/phishing_riscos_e_prevencao.pdf).

Conforme se referiu, em idênticos moldes, no Acórdão do Tribunal da Relação do Porto de 07-10-2014 (Pº 747/12.9TJPRT.P1, rel. ANA LUCINDA CABRAL): *"O phishing, numa primeira etapa, consiste na apropriação de informações de outra pessoa (como nome, informações de conta e senha bancária), para serem utilizadas fraudulentamente nas fases seguintes da trama (transferências de numerários de contas correntes e aplicações financeiras. O pharming é um ataque de phishing mais sofisticado sem o uso da "isca" (o e-mail com a mensagem enganosa). O vírus reescreve arquivos do PC que são utilizados para converter os endereços de Internet (URL´s) em números que formam os endereços IP (números decifráveis pelo computador. Assim, um computador com esses arquivos comprometidos leva o internauta para o site falso, mesmo que este digite corretamente o endereço do site intencionado. A mais sofisticada e perigosa forma de pharming é conhecida como "DNS (Domain Name System) poisoning" (traduzindo para o português, seria algo como "envenenamento do DNS"), por possibilitar um ataque em larga escala. Nessa modalidade, o ataque é dirigido a um servidor DNS, e não a um computador de um internauta isoladamente".*

Em suma: Estas duas 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 eletrónico, no *"pharming"*, modalidade mais perigosa que a anterior, por surgir de forma quase impercetível, 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.

Ora, nos termos do artigo 68.º, n.º 2, do RJSPME, o risco do envio ao ordenante de um instrumento de pagamento ou dos respetivos dispositivos de segurança personalizados corre por conta do prestador do serviço de pagamento.

Conforme se aludiu no Acórdão do Tribunal da Relação de Lisboa de 10-05-2018 (Pº 8903/15.1T8LSB.L1-2, rel. VAZ GOMES) sobre o sentido da previsão legal: *"Acordado um contrato de homebanking, é acordada a prestação de um serviço de banca electrónica ao domicílio por uma determinada entidade bancária a um seu cliente ambos partes no contrato, contratos que assentam num conjunto de cláusulas contratuais gerais definidas*

de forma unilateral pela entidade bancária e antecipadamente relativamente ao contrato tendo como destinatários os seus clientes aderentes do serviço; Trata-se de um sistema de prestação de serviços de pagamento ou transferência implementado pelo Banco, pelo que o risco de funcionamento deficiente ou inseguro do sistema de prestação de serviços de pagamento ou transferência localiza-se, portanto, na esfera do seu prestador, a quem incumbe a responsabilidade por operações não autorizadas pelo cliente nem devidas a causa imputável ao cliente. O contrato de pagamento ou transferência via electrónica é um contrato de prestação de serviços e o risco do incorreto pagamento ou transferência é ainda o risco contratual e não a responsabilidade pelo risco, e o risco em causa compreende-se ainda face à obrigações que sobre o depositário incidem de guardar e restituir a coisa com frutos (art.ºs 1187, alíneas a) e c) e 1205, 796 do CCiv)".

O tema da repartição dos prejuízos decorrentes de fraude informática encontra-se regulado no mencionado RJSPME, a ele se referindo, em particular, os artigos 70.º e ss., com a seguinte redação:

"Artigo 70.º

Prova de autenticação e execução das operações de pagamento

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

2 - 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, por si só, não é necessariamente suficiente para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 67.º

Artigo 71.º

Responsabilidade do prestador do serviço de pagamento por operações de pagamento não autorizadas

1 - Sem prejuízo do disposto no artigo 69.º, em relação a uma operação de pagamento não autorizada, o prestador de serviços de pagamento do ordenante deve reembolsá-lo imediatamente do montante da operação de pagamento não autorizada e, se for caso disso, repor a conta de pagamento debitada na situação em que estaria se a operação de pagamento não autorizada não tivesse sido executada.

2 - Sempre que o ordenante não seja imediatamente reembolsado pelo respetivo prestador de serviços de pagamento nos termos do

número anterior, são devidos juros moratórios, contados dia a dia desde a data em que o utilizador de serviços de pagamento haja negado ter autorizado a operação de pagamento executada, até à data do reembolso efetivo, calculados à taxa legal, fixada nos termos do Código Civil, acrescida de 10 pontos percentuais, sem prejuízo do direito à indemnização suplementar a que haja lugar.

Artigo 72.º

Responsabilidade do ordenante por operações de pagamento não autorizadas

1 - No caso de operações de pagamento não autorizadas resultantes de perda, de roubo ou da apropriação abusiva de instrumento de pagamento, com quebra da confidencialidade dos dispositivos de segurança personalizados imputável ao ordenante, este suporta as perdas relativas a essas operações dentro do limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, até ao máximo de (euro) 150.

2 - O ordenante suporta todas as perdas resultantes de operações de pagamento não autorizadas, se aquelas forem devidas a atuação fraudulenta ou ao incumprimento deliberado de uma ou mais das obrigações previstas no artigo 67.º, caso em que não são aplicáveis os limites referidos no n.º 1.

3 - Havendo negligência grave 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) 150, dependendo da natureza dos dispositivos de segurança personalizados do instrumento de pagamento e das circunstâncias da sua perda, roubo ou apropriação abusiva.

4 - Após ter procedido à notificação a que se refere a alínea b) do n.º 1 do artigo 67.º, o ordenante não suporta quaisquer consequências financeiras resultantes da utilização de um instrumento de pagamento perdido, roubado ou abusivamente apropriado, salvo em caso de atuação fraudulenta.

5 - Se o prestador de serviços de pagamento não fornecer meios apropriados que permitam a notificação, a qualquer momento, da perda, do roubo ou da apropriação abusiva de um instrumento de pagamento, conforme requerido pela alínea c) do n.º 1 do artigo 68.º, o ordenante não fica obrigado a suportar as consequências financeiras resultantes da utilização desse instrumento de pagamento, salvo nos casos em que tenha agido de modo fraudulento.

Artigo 73.º

Reembolso de operações de pagamento iniciadas pelo beneficiário ou através deste

1 - O ordenante tem direito ao reembolso, por parte do respetivo prestador do serviço de pagamento, de uma operação de pagamento autorizada, iniciada pelo beneficiário ou através deste, que já tenha sido executada, caso estejam reunidas as seguintes condições:

a) A autorização não especificar o montante exato da operação de pagamento no momento em que a autorização foi concedida; e
b) O montante da operação de pagamento exceder o montante que o ordenante poderia razoavelmente esperar com base no seu perfil de despesas anterior, nos termos do seu contrato quadro e nas circunstâncias específicas do caso.
2 - A pedido do prestador do serviço de pagamento, o ordenante fornece os elementos factuais referentes às condições especificadas no número anterior.
3 - O reembolso referido no n.º 1 corresponde ao montante integral da operação de pagamento executada.
4 - Em relação aos débitos diretos, o ordenante e o respetivo prestador de serviços de pagamento podem acordar, no contrato quadro, que o ordenante tenha direito ao reembolso por parte do respetivo prestador de serviços de pagamento mesmo que não se encontrem reunidas as condições de reembolso constantes do n.º 1.
5 - Contudo, para efeitos da alínea b) do n.º 1, o ordenante não pode basear-se em razões relacionadas com a taxa de câmbio se tiver sido aplicada a taxa de câmbio de referência acordada com o respetivo prestador de serviços de pagamento, nos termos da alínea d) do n.º 1 do artigo 48.º e da subalínea ii) da alínea c) do artigo 53.º
6 - Pode ser acordado, no contrato quadro, entre o ordenante e o respetivo prestador de serviços de pagamento, que o ordenante não tenha direito a reembolso caso tenha comunicado diretamente ao prestador do serviço de pagamento o seu consentimento à execução da operação de pagamento e, se for caso disso, que o referido prestador ou o beneficiário tenham prestado ou disponibilizado ao ordenante informações sobre a futura operação de pagamento, pela forma acordada, pelo menos, quatro semanas antes da data de execução.
Artigo 74.º
Pedidos de reembolso de operações de pagamento iniciadas pelo beneficiário ou através deste
1 - O ordenante tem direito a apresentar o pedido de reembolso, referido no artigo 73.º, de uma operação de pagamento autorizada, iniciada pelo beneficiário ou através deste, durante um prazo de oito semanas a contar da data em que os fundos tenham sido debitados.
2 - No prazo de 10 dias úteis a contar da data da receção de um pedido de reembolso, o prestador de serviços de pagamento reembolsa o montante integral da operação de pagamento, ou apresenta uma justificação para recusar o reembolso, indicando os organismos para os quais o ordenante pode remeter a questão, ao abrigo dos artigos 92.º e 93.º, se não aceitar a justificação apresentada.
3 - O direito do prestador do serviço de pagamento de recusar o reembolso nos termos do número anterior não é aplicável no caso a

que se refere a n.º 4 do artigo 73.º".
Conforme salienta, de forma certeira, Francisco Mendes Correia (*"Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Electrónica", in* Revista de Direito Civil, Vol. 2, n.º 3, 2017, p. 708), quando uma operação não tenha sido executada por parte do banco e o utilizador e titular da conta invoque que a mesma não foi previamente, por si, autorizada, podem isolar-se 4 constelações prototípicas de factos subjacentes: A operação foi realmente autorizada pelo utilizador (a) ou, pelo contrário, a operação não foi autorizada e a sua realização fica a dever-se a factos imputáveis a título de culpa ao banco (b), ao utilizador (c) ou a terceiro (d).
Ora, do modo como o regime jurídico se encontra configurado, apenas o banco, enquanto prestador do serviço de pagamentos *"pode assegurar a operacionalidade do complexo sistema informático utilizado e a regularidade do seu funcionamento, garantindo, também, a confidencialidade dos dispositivos de segurança que permitem aceder ao instrumento de pagamento. Por esta razão, recai sobre o banco prestador do serviço o risco das falhas e do deficiente funcionamento do sistema, impendendo ainda sobre o mesmo o ónus da prova de que a operação de pagamento não foi afectada por avaria técnica ou qualquer outra deficiência (cf. art.º 70.º do referido Regime dos Sistemas de Pagamento)"* (assim, o Acórdão do Supremo Tribunal de Justiça de 14-12-2016, Pº 1063/12.1TVLSB.L1.S1, rel. PINTO DE ALMEIDA).
De facto, de harmonia com o mencionado artigo 70.º do RJSPME, caso o utilizador do serviço "homebanking" negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada, *"incumbe ao respetivo prestador do serviço de pagamento fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência"* (n.º 1), sendo que, nessas condições, *"a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, por si só, não é necessariamente suficiente para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 67.º"* (cfr. n.º 2)
Assim, *"não se provando que o cliente agiu fraudulentamente, ou que não cumpriu intencionalmente ou com negligência grave a sua obrigação de utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, designadamente as respeitantes às chaves de acesso ao serviço de "homebanking", recai sobre o banco a responsabilidade pela movimentação fraudulenta da sua conta bancária, através da internet (art.ºs 67º, nº 1, a), 68º, nº 1, a), 70º, nº 1 e 2, e 72º, nº 1 a 3, do Regimento Jurídico dos Serviços de Pagamento e Moeda Electrónica (…)"*

(nestes termos, o Acórdão do Tribunal da Relação de Coimbra de 15-01-2019, Pº 5600/11.0TBLRA.C1, rel. MOREIRA DO CARMO).
Assim, dos artigos 70.º e 72.º do RJSPME resulta que se atribui ao prestador do serviço de pagamento o ónus de provar que as ordens de pagamento dadas pelo cliente foram devidamente autorizadas através da utilização efetiva dos mecanismos de autenticação disponibilizados, bem como foram corretamente registadas e contabilizadas, e que a sua execução foi isenta de qualquer avaria técnica ou devido a deficiência do serviço prestado pelo prestador de serviços de pagamento, tendo o ónus de provar a ocorrência de comportamento negligente, gravemente negligente ou doloso do utilizador (cfr., neste sentido, entre outros, os Acórdãos do Tribunal da Relação de Lisboa de 06-11-2018, Pº 1952/15.1T8SXL.L1-1, rel. ANA PESSOA e de 28-04-2022, Pº 17903/19.1T8LSB.L1-8, rel. LUÍS CORREIA DE MENDONÇA; o Acórdão do Tribunal da Relação do Porto de 04-06-2019, Pº 1482/17.7T8PRD.P2, rel. ALEXANDRA PELAYO e o Acórdão do Tribunal da Relação de Évora de 24-09-2020, Pº 26/19.0T8MRA.E1, rel. MANUEL BARGADO).
Se tal prova não for realizada pela instituição bancária, a mesma será responsável pelo imediato pagamento – que se não for efetuado terá as consequências a que se refere o n.º 2 do artigo 71.º do RJSPME – do montante da operação de pagamento não autorizada, repondo a conta na situação em que estaria se a operação de pagamento não autorizada, não tivesse sido executada (cfr. artigo 71.º, n.º 1, do RJSPME).
Se, ao invés, for apurada responsabilidade do ordenante por operações de pagamento não autorizadas, regerá o citado artigo 72.º do RJSPME:
- Se as operações de pagamento não autorizadas resultantes de perda, de roubo ou da apropriação abusiva de instrumento de pagamento, com quebra da confidencialidade dos dispositivos de segurança personalizados for imputável ao ordenante, este suporta as perdas relativas a essas operações dentro do limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, até ao máximo de (euro) 150;
- Se as perdas forem devidas a atuação fraudulenta ou ao incumprimento deliberado de uma ou mais obrigações previstas no artigo 67.º, o ordenante suporta todas as perdas resultantes de operações de pagamento não autorizadas (sem que seja aplicável o referido limite do saldo disponível ou da linha de crédito associada à conta/instrumento de pagamento);
- Se ocorrer negligência grave 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/ instrumento de pagamento, ainda que superiores a (euro) 150, dependendo da natureza dos dispositivos de segurança

personalizados do instrumento de pagamento e das circunstâncias da sua perda, roubo ou apropriação abusiva.
Assim, por exemplo, 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, rel. PEDRO MARTINS).
Em termos gerais, pode afirmar-se, como se decidiu no Acórdão do Tribunal da Relação de Guimarães de 23-12-2012 (Pº 305/09.5TBCBT.G1, rel. FILIPE CAROÇO) o seguinte: *"A complexidade dos sistemas bancários home banking, concebidos e controlados pelos Bancos, assim como a grande exigência dos mecanismos relacionados com a segurança das operações bancárias através deles realizadas, a par da propriedade do banco sobre os valores depositados pelos seus clientes, em ambiente contratual, justificam o funcionamento da regra da presunção de culpa prevista pelo art.º 799º, nº 1, do Código Civil, que recai sobre a entidade bancária na responsabilidade pela utilização fraudulenta daqueles meios. Em todo o caso, o banco pode elidir aquela presunção, afastando a sua culpa ou demonstrando mesmo a culpa do cliente pela deficiente utilização daqueles meios expeditos, designadamente, alegando e demonstrando que o cliente beneficiário violou o contrato, divulgando na internet dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de hackers. No primeiro caso, o Banco pode ainda ser responsabilizado pelo risco, enquanto na segunda hipótese a responsabilidade é do cliente".*
De harmonia com o disposto no artigo 487º do CC, *"a culpa é apreciada, na falta de outro critério legal pela diligência de um bom pai de família em face das circunstâncias de cada caso",* pelo que, o julgador terá que, perante o caso concreto, atender a todas as circunstâncias de facto, bem como às características pessoais do utilizador.
Conforme salienta Antunes Varela (Das Obrigações em Geral, vol. 1. 10ª edição, Almedina, Lisboa, 2000, p.574), *"o grau de reprovação ou de censura será tanto maior quanto mais ampla for a possibilidade de a pessoa ter agido de outro modo, e mais forte ou intenso o dever de o ter feito".*
A negligência grave pode definir-se como *"negligência grosseira, erro imperdoável, desatenção inexplicável, incúria indesculpável, vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes"* (assim, o Acórdão do Tribunal da Relação de Guimarães de 17-12-2014, Pº 1910/12.8TBVCT.G1, rel. FERNANDO FERNANDES FREITAS).

Diversas têm sido as situações caraterizadas como consubstanciando negligência grave do utilizador de instrumentos de pagamento bancários, quer pela doutrina, quer pela jurisprudência.

Assim, na doutrina, Inês Custódio Alves (Operações Abusivas na Banca Eletrónica – A imputação de responsabilidades pelas perdas resultantes da movimentação não autorizada de fundos; FDUNL, 2019, p. 42) conclui que: *"Consubstanciam situações de negligência grave não só aquelas em que o cliente forneceu os códigos de acesso e credenciais disponíveis no cartão matriz, como também nos casos em que, pese embora o correto funcionamento dos serviços do banco e do cumprimento do dever de informação ao cliente com a disponibilização de alertas de segurança na página de homebanking perfeitamente claros e elucidativos na detetação de interações fraudulentas, o mesmo procede com descuido e desatenção, conduta vista, aos olhos da jurisprudência, como censurável (…)".*

Na mesma linha, Raquel Sofia Ribeiro de Lima (*"A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa", in* Revista Electrónica de Direito; Outubro 2016, n.º 3, p. 48) explica 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]".*

Verónica Santos (As debilidades do serviço de homebanking, em especial quanto aos crimes de fraude informática de phishing e pharming. A questão da responsabilidade no âmbito das operações bancárias não autorizadas, UCP, 2018, p. 47) considera, do mesmo modo, que: *"Também ferido de negligência grave, será o comportamento do utilizador do instrumento de pagamento que deliberadamente incumpre os deveres que lhe são impostos por lei nomeadamente a prudência, diligência e deveres de cuidado, quando divulga a terceiros os códigos de acesso ao serviço de home banking violando o seu dever de segurança e confidencialidade sobre os seus dispositivos, bem como ultrapassa os avisos de segurança que vão surgindo mediante a abertura da ligação de acesso ao home banking, e que tem que ser por si fechados. Face a isto deverá ser o cliente a suportar todas as perdas originadas pelas operações de pagamento não autorizadas até à data da comunicação da ocorrência, art. 72º nº2 e 4 do RSP".*

Em semelhantes moldes, Maria Raquel Guimarães ("*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) enuncia um critério de aferição da negligência do utilizador dos instrumentos de

pagamento, dizendo que a conduta do mesmo só será passível de censura quando *"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…".*

E, na mesma linha, Bruno da Silva Palhão (Operações não autorizadas e repartição dos prejuízos: O homebanking na jurisprudência do RSP, UCP, 2018, p. 44) conclui 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".*

Na jurisprudência, a aferição da negligência grave do utilizador de serviços ou instrumentos de pagamento tem sido apreciada, de modo uniforme, em linha com os aludidos contributos doutrinais. Disso são exemplo as seguintes decisões (indicadas por ordem cronológica decrescente):

- Acórdão do Tribunal da Relação de Lisboa de 01-10-2020 (Pº 19530/17.9T8LSB.L-8, rel. MARIA AMÉLIA AMEIXOEIRA):
Tendo-se apurado que as transferências "sub judice" foram efectuadas fraudulentamente por terceiros, com recurso à técnica conhecida por phishing, logo se conclui que as mesmas não ocorreram por uma qualquer avaria ou deficiência do sistema informático da Ré/BANCO , como defende a Autora . E, Resultando provado que a utilização do serviço homebanking por banda da autora, se produziu com total desrespeito pela mesma das condições acordadas, maxime no que concerne às que se reportam à segurança , designadamente em sede de transmissão da totalidade dos dados do seu cartão matriz a terceiros, temos assim que , Acaba em última análise a Ré/BANCO por provar a culpa da Autora e o seu incumprimento do contrato de homebanking - por violação das mais elementares regras de segurança impostas pelo mesmo - , logrando ilidir a presunção de culpa prevista no art. 799º nº 1 do Código Civil, que sobre si impendia, pelo que não é responsável pela movimentação das contas bancárias de forma fraudulenta".

- Acórdão do Tribunal da Relação do Porto de 14-07-2020 (Pº 22158/17.0T8PRT.P1, rel. FERNANDO BAPTISTA):
"(…) VIII - Face ao princípio geral da boa fé, impõe-se, a quem pretende utilizar o home-banking, o dever de guarda dos dados que lhe permitem aceder ao sistema e realizar operações on-line e de preservação da confidencialidade dos mesmos, por forma a evitar a sua apropriação por terceiros, adoptando uma cultura de segurança

e rigor, face aos interesses envolvidos.
IX - As entidades bancárias têm (ou deverão ter) os meios para controlar a segurança da parte do sistema que se encontra do seu lado, ou seja, de fazer tudo o que está ao seu alcance para proteger os interesses dos seus clientes, dotando a sua organização empresarial com os meios humanos e materiais adequados a assegurar condições apropriadas de qualidade e eficiência. Mas não têm qualquer possibilidade de controlar a parte do sistema que se encontra do lado do cliente/utilizador (utilização que os clientes fazem dos seus computadores).
X - Apenas no caso de estarmos perante uma situação de negligência leve do utilizador do serviço é que o Banco terá de suportar os prejuízos excedentes que decorram de operações de pagamento não autorizadas, cabendo-lhe, nessa situação, suportar o risco do sistema informático que permitiu a intromissão de terceiros.
XI - Já tratando-se de negligência grave/grosseira ou dolo do utilizador do serviço, terá de ser esse utilizador a arcar com as consequências nefastas para si do desvio ilícito de fundos da sua conta, a ele, portanto, cabendo suportar os prejuízos que decorram de tais operações de pagamento não autorizadas.
XII - Sendo que a negligência grosseira constitui uma negligência temerária, qualificada, em que a culpa é agravada pelo elevado teor de imprevisão ou de falta de cuidados elementares, adoptando-se uma conduta de manifesta irreflexão ou ligeireza.
XIII - A conduta negligente grave do Autor (v.g., facultando a alguém qualquer dos três níveis de segurança – número de contrato, password e Cartão Matriz) não se pode consubstanciar como um risco inerente à actividade económica do Banco. A não se entender assim, o equilíbrio contratual – inerente ao sinalagma contratual – ficaria seriamente posto em causa, com aceitação duma postura leónica a todos os títulos inaceitável.
XIV - Estando provado que A autora transmitiu as credenciais de autenticação ao Pai que as disponibilizou online em site e por meio não apurado, incluindo os números das coordenadas do cartão matriz e que "foi através do uso dessas credenciais de acesso que um sujeito cuja identificação não foi possível apurar actuou da forma descrita nas alíneas …" (para além de se ter, ainda, provado que "O sistema informático do réu não foi alvo por essa ocasião de um ataque informático), só a essa postura gravemente negligente da Autora se devem atribuir as consequências danosas no seu património, que, como tal, terá de suportar.
XV - E sendo, embora, ao Banco Réu que cabe provar o comportamento negligente do titular da conta e a medida em que esse contribuiu para as operações não autorizadas, feita essa prova e bem assim que não houve qualquer ataque ao sistema do Banco Réu (por força do qual terceiros acedessem à conta da autora), ficará ilidida a presunção dos artigos 799º, nº1 do Código Civil e

mesmo afastada a aplicação do artigo 796º, nº1, do Código Civil, porquanto foi o alienante (a Autora/Cliente) que causou o perecimento da coisa, não sendo o Banco responsável pelo prejuízo causado ao credor (art. 798.º do Código Civil (…)";
- Acórdão do Tribunal da Relação de Guimarães de 09-06-2020 (Pº 51/18.9T8PRG.G1, rel. MARIA CRISTINA CERDEIRA): *"A complexidade dos sistemas bancários de homebanking, concebidos e controlados pelos Bancos, assim como a grande exigência dos mecanismos relacionados com a segurança das operações bancárias através deles realizadas, a par da propriedade do Banco sobre os valores depositados pelos seus clientes, em ambiente contratual, justificam o funcionamento da regra da presunção de culpa prevista no art.º 799º, nº. 1 do Código Civil, nos termos da qual recai sobre o Banco depositário o ónus da prova de que a falta de cumprimento ou o cumprimento defeituoso da obrigação (correspondente a avarias técnicas ou outras deficiências que levaram à utilização fraudulenta daqueles meios) não procede de culpa sua. Em todo o caso, avultando neste tipo de contratos de homebanking a obrigação de utilização correcta do serviço por parte do utente, o qual assenta em boa parte na não divulgação dos seus elementos de segurança e códigos de acesso, o Banco pode elidir aquela presunção, afastando a sua culpa ou demonstrando mesmo a culpa do cliente pela deficiente utilização daqueles meios expeditos, designadamente, alegando e provando que o cliente beneficiário violou o contrato, divulgando na internet dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de hackers. O comportamento da Autora ao abrir um email que lhe pareceu proveniente do Banco réu, com o pedido de activação do cartão matriz, sendo-lhe solicitado, para o efeito, que acedesse a um link e introduzisse todos os dígitos do seu cartão, o que ela fez, tendo fornecido a totalidade das coordenadas que se encontram inscritas no cartão matriz, apesar de se encontrar inscrito no cartão matriz que utilizou para inserir todas as coordenadas o seguinte aviso: "Atenção: Nunca indique mais do que dois dígitos deste cartão matriz", mostra-se adequado a viabilizar a realização por terceiros de operações de pagamento não autorizadas. Age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do Banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador. Ao divulgar na internet a totalidade das combinações de algarismos que compõem o seu cartão matriz – apesar dos vários avisos e alertas de segurança que constam do cartão matriz, da carta que a Ré enviou à Autora com o cartão, do site da Ré na internet e da página de login do sistema "Net..." – a Autora actuou ao arrepio do contrato de homebanking a que aderiu e em violação de regras básicas de segurança nele previstas para a utilização do serviço "Net...", regras essas acessíveis à Autora, o que permitiu que*

terceiros se apoderassem dos seus elementos de segurança e assim lograssem aceder às contas bancárias tituladas pelas Autoras e efectuar operações fraudulentas. A actuação da Autora, ao inserir a totalidade das coordenadas inscritas no cartão matriz em página electrónica semelhante à do serviço de homebanking da Ré, fazendo uma utilização imprudente e descuidada daquele serviço, violando as regras de segurança impostas pelo respectivo contrato, tendo sido este comportamento causa directa da movimentação das suas contas bancárias por terceiros, configura negligência grave, preenchendo a previsão do art.º 72º, n.º 3 do RSP, pelo que lhe cabe a responsabilidade pelas operações de pagamento não autorizadas executadas, até ao limite do saldo disponível. Por sua vez, a Ré, ao provar a culpa da Autora na transmissão da totalidade das coordenadas inscritas no cartão matriz a terceiros e, consequentemente, o seu incumprimento do contrato de homebanking por violação das mais elementares regras de segurança impostas pelo mesmo, ilidiu a presunção de culpa prevista no art.º 799º, nº. 1 do Código Civil que sobre si impendia, pelo que não é responsável pela movimentação das contas bancárias de forma fraudulenta";

- Acórdão do Tribunal da Relação de Lisboa de 12-07-2018 (Pº 2256/17.0T8LSB.L1-7, rel. HIGINA CASTELO): *"Tendo o banco comunicado ao cliente, em vários momentos, por vários meios e formas, o modo de corretamente utilizar as credenciais de acesso ao sistema de homebanking, a introdução pelo cliente dos códigos de acesso à conta bancária (identificação e palavra-passe) e dos números do cartão matriz (terceiro nível de verificação de identidade para certas operações bancárias) numa página Web com elementos (mais ou menos, muitos ou poucos) semelhantes à página do banco, mas à qual chega ao clicar numa hiperligação de um e-mail, constitui uma grave violação do dever de manter em segredo as credenciais em causa. O cliente do banco, parte no contrato de homebanking, suporta (até ao limite do saldo disponível ou da linha de crédito associada à conta) as perdas resultantes de operações de pagamento efetuadas em execução de ordens dadas através do sistema de homebanking por terceiros a quem, por atuação gravemente negligente, facultou os códigos e chaves necessários a que tais ordens fossem identificadas como tendo sido dadas por si";*

e

- Acórdão do Tribunal da Relação de Guimarães de 25-11-2013 (Pº 2869/11.4TBGMR.G1, rel. ESPINHEIRA BALTAR): *"Age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador".*

Neste último Acórdão, o Tribunal da Relação de Guimarães concluiu, no apontado sentido, assentando em que, *"para um utilizador informático minimamente diligente, cuidadoso, e*

minimamente informado no uso desta tecnologia, sabendo ou tendo o dever de saber dos perigos que assolavam o sistema (através da informação prestada pela ré sobre o assunto e colocada no site onde as pessoas eram logo alertadas e podiam informar-se melhor acedendo ao menu segurança) e a Web em geral, tinha que se questionar perante tal solicitação. E, perante esta dúvida, tinha um de dois caminhos a seguir, ou contactava rapidamente com a ré, via telefone, ou ignorava a solicitação e comunicava o acontecimento à ré. E só em face da solução que lhe fosse dada, é que continuaria a usar o programa. Tinha de ter a consciência que estava numa situação que não era normal e tinha de sanar a dúvida".

Revertendo estas considerações e aplicando-as ao caso dos autos, em termos de apuramento de responsabilidade, vemos que se apurou, em termos factuais, que, no início de novembro de 2015, a autora, através do seu sócio gerente, NC, quando acedeu à página do *homebanking* da Caixa Económica Montepio Geral, foi direcionando para uma página de Internet previamente forjada e em tudo idêntica à página oficial daquela instituição, solicitando a atualização do cartão matriz e a indicação de determinadas coordenadas do mesmo.

Nessa sequência, pessoa ou pessoas (hacker(s)) cuja(s) identidade(s) não foi apurada conseguiu, assim, que a autora, na qualidade de cliente da Caixa Económica Montepio Geral fornecesse os seus códigos de ativação do serviço homebanking, após o que a pessoa ou pessoas cuja identidade não foi possível apurar, hacker(s), munido(s) das respetivas credenciais de acesso, obtidas de forma fraudulenta, acederam à conta bancária da A. como se se tratasse do seu verdadeiro titular, tomou conhecimento dos saldos bancários daquela conta e movimentou-a determinando, através da Internet, diversas transferências de valores, tudo sem o conhecimento, contra a vontade e em prejuízo da autora.

Atuando desta forma, o indivíduo ou os indivíduos cuja identidade não foi possível apurar, hacker(s), com a intenção de obter vantagem patrimonial, conseguiram através do acesso ilegítimo, via internet, com utilização de meios informáticos, o acesso à conta bancária da A. e procederam a uma subsequente subtração de valores que aí se encontrassem, transferindo-os para contas bancárias, tituladas por si e por terceiros, sobre as quais mantivesse algum tipo de domínio.

Tal pessoa, ou pessoas, acedeu ou acederam, assim, através do serviço de homebanking, à conta bancária titulada pela A. com o número 2131.10.605744-2., domiciliada no Montepio Geral, agência de Angra do Heroísmo, sem o conhecimento e contra a vontade do seu titular efetuando no dia 13 de novembro de 2015 e no dia 15 de novembro de 2015, respetivamente, 4 e 13 acessos ilegítimos / levantamentos / transferências internacionais, de diversas quantias, totalizando 22.497,00€.

Mais se apurou que, ao sócio gerente da autora, foram atribuídos pela Ré, códigos de acesso/credenciais de utilização, que, à data dos factos funcionavam em 3 níveis de segurança: Número de utilizador; Password; Cartão matriz.
O número de utilizador correspondente ao número de cliente Montepio e pode ser personalizado. A password, composta por seis dígitos, que após o primeiro login, tem de ser obrigatoriamente alterada por uma da autoria e do exclusivo conhecimento do cliente. Por sua vez, o cartão matriz é composto por 72 posições, cada uma com 3 dígitos, para validação de operações passíveis de alterar o património detido pelos clientes, junto do Banco Montepio, cujo processo de produção é externo à Ré e não envolve qualquer atuação humana, uma vez que as coordenadas são geradas por computador, sendo remetido via CTT para o endereço dos clientes, e apenas passível de ser ativado mediante a validação de códigos de acesso ao Net24 (número de utilizador e password) adstrito ao cartão expedido.
Para a realização de uma operação com alterações patrimoniais, o utilizador teria de efetuar o login, na página da internet da Ré, colocar a sua password, selecionar a operação e colocar as duas coordenadas do seu cartão matriz, e só mediante a sua correta validação, é que se confere validade à ordem transmitida.
Ao sócio gerente da autora (que é utilizador frequente do sistema de pagamento homebanking) foram explicados todos os procedimentos de segurança e de utilização do referido serviço e a respetiva informação encontra-se disponível no site da Ré.
Finalmente, ficou provado que, os aludidos movimentos bancários, apenas foram possíveis porque, em cada um deles, foi introduzido o número de utilizador, a password – cuja 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 – e duas coordenadas do cartão matriz, que são sempre solicitadas de forma aleatória, pelo sistema e nunca repetidas.
Demonstrado ficou que o sistema da ré não foi alvo de qualquer intrusão ou ataque informático.
Todavia, apurou-se que o sócio gerente da autora - no início de novembro de 2015 e direcionado da forma acima referenciada para uma página da internet forjada idêntica à da página oficial da ré - preencheu 50% das coordenadas constantes do seu cartão matriz.
Em face da factualidade referenciada, sem dúvida – aspeto que não é posto em questão – que ocorreram diversas transferências bancárias de fundos, não autorizadas pela autora e efetuadas, de modo fraudulento, pela técnica do *"pharming"* acima descrita, levando a autora a crer que estaria no sítio institucional na Internet da ré, quando, todavia, estava numa página forjada – idêntica à institucional ou oficial – previamente elaborada para o

efeito fraudulento gizado e fornecendo as credenciais de acesso da conta titulada pela autora, bem como, procedeu a uma invocada atualização do cartão-matriz facultando cerca de 50% dos números desse cartão.

Conforme bem se refere na decisão recorrida, *"[m]esmo que o sócio gerente da Autora tivesse o site alegadamente "guardado" no seu computador, o malware na forma de vírus pode na mesma alterar o site, enviando aquele para um site que não o fidedigno. Mas apesar das parecenças, o facto de ser pedida uma atualização do cartão matriz, quando o mesmo refere expressamente que não deverá ser fornecido mais de dois dígitos, origina uma incongruência que deveria despertar desconfiança no sócio gerente"*, o que, todavia, não ocorreu.

Ora, se a primeira situação - o direcionamento do legal representante da autora, enquanto utilizador do serviço de pagamento fornecido pela ré, para uma página de internet forjada, um *site* não fidedigno - não se pode considerar revelador de alguma negligência, porque efetuado de forma não desejada ou involuntária (direcionamento esse que, como se viu, foi conseguido por intermédio de atuação fraudulenta de terceiro), já a segunda situação – a conduta do legal representante da autora, quando lhe é solicitada a atualização do cartão-matriz e o mesmo a efetua - revela um comportamento negligente, imprevidente e inconsiderado que a generalidade dos utilizadores de um tal serviço, não adotaria.

Na realidade, não só a atualização do cartão-matriz - do modo como ocorreu, se encontrava identificada no site institucional da ré com o aviso *"Exemplos de tentativas de Fraude"* (a par de outros avisos, como o de que, *"se lhe for solicitado que preencha o cartão completo ou qualquer outra combinação, deverá ser considerada como uma tentativa de fraude"*) podendo ser facilmente apreensível pelos clientes do banco – e especificamente pela autora - , como também, constava do próprio cartão-matriz disponibilizado pela ré, que o banco não solicitava mais do que 2 dígitos do referido cartão, aspeto que deveria ter levado a questionar o utilizador sobre porque razão, em contradição com tal afirmação de comportamento, na ocasião lhe era solicitada a inserção de mais de 2 dígitos do cartão matriz!

Assim, se bem que, na questão do direcionamento, a autora não pudesse contar com uma tal fraude, já no momento em que foi solicitada – no âmbito de uma suposta "atualização do cartão matriz" – a inserção de conteúdos do cartão matriz para além do limite no qual o banco referiu que o solicitaria, revela um comportamento não conforme com os mais elementares deveres de segurança do utilizador de serviços de pagamento financeiros e a inobservância, de forma clamorosa, dos deveres contratuais assumidos (cfr. cláusula 23.17 do acordo celebrado entre autora e ré, que não se pode dizer – ao contrário do pugnado pela

recorrente – apenas se reporte ao momento de realização de uma operação bancária – mas sim, claro está, uma pauta de conduta geral no cumprimento dos deveres de boa utilização do instrumento de pagamento disponibilizado à autora e cuja adesão tinha ocorrido vários anos antes – 18-11-2011 – e cuja ativação ocorrera em 06-02-2012 – cfr. facto provado n.º 18).
Neste ponto, ao invés – ou seja, na perspetiva da adequação de conduta da ré - a intensidade/generalidade dos avisos (que, segundo a autora, em 2015 não era tão intensa ou geral como atualmente sucede) não obvia à consideração da gravidade da falta de previdência da autora, pois, na realidade, face à instituição bancária em questão, os avisos de segurança encontravam-se implementados e eram difundidos, sendo que se afigura que tal implementação e difusão fossem hábeis para que a generalidade dos utilizadores do sistema da ré, pudessem considerar e tomar conhecimento do seu conteúdo, conformando o seu comportamento com o mesmo. A questão suscitada pela autora não tem, pois, neste sentido, algum relevo, no sentido de eximir a autora de responsabilidade.
Nos mesmos moldes, também a questão de a autora ter antivírus instalado e de a ré não ter, à data, implementado o *"SMS Code"* (Token) que veio a ser prescrito por força da Diretiva (UE) 2015/2366, do Parlamento Europeu e do Conselho, de 23 de novembro de 2015 (e pelo D.L. n.º 91/2018, de 12 de novembro) não permitem alterar as coordenadas do problema.
Vejamos:
A adopção do "SMS Code" (Token) – (ou seja, uma 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) se bem que se tenha destinado a incrementar a segurança nos pagamentos digitais - em linha com a Orientação 7 das Orientações da Autoridade Bancária (EBA) relativas à segurança dos pagamentos efetuados 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 Diretiva 2015/2366 e artigo 104.º do D.L. n.º 98/2018 – para determinados serviços de pagamento, não pode colocar em crise a validade e adequação dos procedimentos e dos pagamentos adotados na vigência do precedente sistema jurídico.
Na realidade, atualmente, em determinadas circunstâncias, os prestadores de serviços de pagamento aplicam a "autenticação forte" (*"uma autenticação baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a*

confidencialidade dos dados de autenticação;” **– cfr. artigo 2.º, d) do D.L. n.º 98/2018, associando, de forma dinâmica, elementos respeitantes à operação de um montante específico e a um beneficiário específico) do cliente, caso o ordenante de tais serviços, aceda em linha à sua conta de pagamento, inicie uma operação de pagamento eletrónico ou realize uma ação, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou de outros abusos.**

Concomitantemente, o n.º 2 do artigo 74.º da Diretiva 2015/2366 (e o artigo 115.º, nº 5, do D.L. n.º 98/2018) estabelece que, se o prestador não exigir este método de autenticação mais robusto, terá sempre de reembolsar o utilizador - que assim não será responsável - das perdas sofridas, exceto se este tiver atuado fraudulentamente.

Conforme explica Patrícia Alexandra Paiva Duarte (“Os serviços de iniciação de pagamento no novo RSP”, in Revista Electrónica de Direito, Vol. 25, Junho 2021, n.º 2, p. 65), a respeito da *“autenticação forte do utilizador”:*

“Uma das alterações fundamentais do RSP prende-se com a harmonização e reforço dos requisitos de segurança aplicáveis às operações de pagamento em todos os Estados-Membros.

De acordo com a al. c), do art.º 2.º, deverá entender-se por autenticação o procedimento que permite ao prestador verificar a identidade de um utilizador ou a validade da utilização de um instrumento, incluindo o próprio uso das credenciais de segurança personalizadas do utilizador, pelo que a exigência de uma autenticação forte do cliente impõe que o referido procedimento de verificação se baseie na utilização de “dois ou mais elementos pertences às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é)”. Em relação ao primeiro elemento, na recente opinião da EBA sobre os elementos que integram a autenticação forte do cliente [EUROPEAN BANKING AUTHORITY, Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, EBA-Op-2019-06, disponível em https://www.eba.europa.eu], faz-se referência de que poderá consistir numa palavra-passe, um código ou respostas baseadas em conhecimento que só o utilizador poderá ter, mas que já não preencherá o conceito o valor de verificação do cartão (CVV) e a sua data de validade, bem como a sua identificação de utilizador. No que toca ao elemento posse, a EBA considera que poderá estar em causa o telemóvel do utilizador ou um dispositivo de autenticação, sendo que a posse deverá ser confirmada através da criação ou receção de um elemento de validação dinâmica no dispositivo como o envio de uma senha ou código único. Já não será suficiente a posse de um cartão matriz comprovada com a introdução dos dados do cartão. Por fim, o elemento inerência que, certamente, melhor garante a correta verificação do utilizador,

basear-se-á, essencialmente, em características físicas e comportamentais do utilizador, ou seja, dados biométricos, como é o caso do reconhecimento facial, de voz e da impressão digital. A utilização dos referidos elementos tem de ser independente de modo a que a violação de um deles não comprometa a fiabilidade dos outros e a autenticação deverá ser realizada sempre de forma a proteger a confidencialidade dos dados de autenticação. Embora nada na letra da lei o impeça, pela sua razão de ser e de modo a cumprir o seu objetivo, os elementos utilizados na autenticação do utilizador têm de ser de natureza diferente".

Ora, no caso dos autos, reportando-se a situação em apreço a 2015, não é questionável, por um lado, a fiabilidade do sistema implementado pela ré, que não foi objeto de ataque ou intrusão, nem, por outro lado, é colocada em questão a compatibilidade de tal sistema de pagamentos da ré com o quadro legal então em vigor, observando o mesmo as prescrições que lhe estavam inerentes, satisfazendo as credenciais existentes (utilizador, password e cartão matriz) tais prescrições.

De todo o modo, independentemente destas considerações, não se alcança demonstrado algum nexo de causalidade adequada entre a ausência do sistema de autenticação do SMS Token e a defraudação ocorrida, no sentido de que, foi tenha sido tal ausência que tenha, de modo inexorável, viabilizado a fraude verificada.

É, que, na realidade, tendo presente a factualidade apurada, não se mostra possível concluir que, acaso estivesse a ré dotada, à data dos factos, de um tal sistema de autenticação, que o ocorrido, não viesse a suceder. Com efeito, a fraude na movimentação bancária atinente à saída de fundos, concretizada por terceiros, foi externa a qualquer dos sistemas implementados e disponibilizados pela ré e apenas foi proporcionada pelo fornecimento indevido e excessivo (por excedendo o limite de duas posições que o banco solicitava) de dados do cartão matriz que viabilizou as transações ulteriores, circunstância que, fosse outra a autenticação (designadamente, com o sistema SMS Token), não seria debelada.

Conclui-se, assim, em face de tudo o referido, 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 (a autora) 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 (2 posições de coordenadas, que respeita ao cartão matriz, aviso que o banco disponibilizava no seu site e que constava aposto no cartão matriz), mas que, ao

invés, divulga 50% das 72 coordenadas do cartão matriz.
Assim, não ocorrendo responsabilização da ré face aos factos ocorridos (tendo sido ilidida a presunção de culpa que sobre si, primariamente, impendia), conclui-se não merecer censura a decisão recorrida, que concluiu pela improcedência da pretensão da autora, absolvendo a ré do contra si peticionado por aquela.
*****
A apelação deduzida deverá, em conformidade com o exposto, improceder.
*****
De acordo com o estatuído no n.º 2 do art.º 527.º do CPC, o critério de distribuição da responsabilidade pelas custas assenta no princípio da causalidade e, apenas subsidiariamente, no da vantagem ou proveito processual.
Entende-se que dá causa às custas do processo a parte vencida, na proporção em que o for. *"Vencidos"* são todos os que não obtenham na causa satisfação total ou parcial dos seus interesses.
Conforme se escreveu no Acórdão do Supremo Tribunal de Justiça de 06-12-2017 (Pº 1509/13.1TVLSB.L1.S1, rel. TOMÉ GOMES), cujo entendimento se subscreve: *"O juízo de procedência ou improcedência da pretensão recursória não é aferível em função do decaimento ou vencimento parcelar respeitante a cada um dos seus fundamentos, mas da respetiva repercussão na solução jurídica dada em sede do dispositivo final sobre essa pretensão".*
Em conformidade com o exposto, a responsabilidade tributária inerente incidirá, *in totum*, sobre a autora/apelante, que decaiu, para este efeito, integralmente, na presente instância recursória – cfr. artigo 527.º, n.ºs. 1 e 2, do CPC.
*****
<u>5. Decisão:</u>
Pelos fundamentos expostos, acordam os Juízes que compõem o tribunal coletivo desta 2.ª Secção Cível, em julgar improcedente a apelação, mantendo a decisão recorrida.
Custas pela autora/apelante.
Notifique e registe.
*****
Lisboa, 13 de outubro de 2022.
Carlos Castelo Branco
Orlando dos Santos Nascimento
Maria José Mouro Marques da Silva