Acórdão do Tribunal da Relação de Lisboa

Processo: 451/24.5T8LSB.L1-2
Relator: INÊS MOURA
Descritores: OPERAÇÕES BANCÁRIAS ON LINE
SEGURANÇA
FRAUDE
NEGLIGÊNCIA GROSSEIRA
Nº do Documento: RL
Data do Acordão: 11-09-2025
Votação: UNANIMIDADE
Texto Integral: S
Texto Parcial: N
Meio Processual: APELAÇÃO
Decisão: IMPROCEDENTE

Sumário:

(art.º 663.º n.º 7 do CPC)

1. O Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica aprovado pelo DL 91/2018 de 12 de novembro que veio transpor para a nossa ordem jurídica a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015, regulando o acesso à atividade das instituições de pagamento e a prestação de serviços de pagamento, bem como o acesso à atividade das instituições de moeda eletrónica e a prestação de serviços de emissão de moeda eletrónica, vem atribuir ambas as partes – prestador de serviços e cliente - responsabilidades no cumprimento de diversos deveres associados à utilização de meios de pagamento digitais, de forma a potenciar a sua segurança.

2. No âmbito das operações bancárias *on line* compete ao prestador do serviço bancário garantir a segurança do sistema eletrónico que permite a realização de tais operações, correndo por sua conta o risco da falha ou deficiente funcionamento do sistema eletrónico, o que também resulta do disposto no art.º 796.º n.º 1 do C.Civil, competindo-lhe alegar e provar que a operação de pagamento realizada não foi decorrente de avaria ou deficiência de segurança do sistema, e/ou que houve culpa do cliente na obtenção dos elementos de segurança necessários à instrução de pagamento realizada de forma fraudulenta.

3. O legislador revelou uma preocupação em conferir uma maior proteção ao utilizador beneficiário do serviço, também evidenciada no n.º 4 do art.º 115.º do DL 91/2018, ao estabelecer que a responsabilidade deste pelas perdas resultantes de operação de pagamento não autorizada apenas ocorre, se a mesma tiver resultado de um comportamento culposo do utilizador do serviço, não apenas negligente, mas antes grosseiramente negligente, cabendo ao prestador do serviço o ónus da prova dos factos que o revelam.

4. Tem vindo a ser entendido de forma pacífica pela nossa jurisprudência e também pela doutrina, que o conceito de negligência grosseira a que alude o art.º 115.º n.º 4 do DL 91/2018 deve ser equiparado ao conceito de culpa grave no Direito Civil, podendo recorrer-se ao art.º 487.º n.º 2 do C.Civil que estabelece

que a culpa é apreciada, na falta de outro critério legal, pela diligência de um bom pai de família.
5. A culpa enquanto juízo de reprovação de uma conduta pela omissão de um dever de diligência, não pode deixar de ter em conta as circunstâncias do caso concreto, quer as que se reportam às condições do seu agente, quer aquelas que despoletaram o seu comportamento que determinou a ocorrência do dano, só assim podendo avaliar-se qual a diligência que no caso era exigível ao agente.
6. O facto do cliente do Banco receber uma SMS que surge na sequência de outras SMS emitidas pelo seu Banco, corresponde a um elemento que aponta para a circunstância de se tratar de uma mensagem fidedigna e não obstante existam erros de português, crê-se que os mesmos só por si podem não constituir um alerta para a generalidade das pessoas, na medida em que representam a ausência/erro de artigos definidos, o que pode não ser de estranhar em face da natureza abreviada das mensagens, pelo que pela a forma como foi apresentado a SMS em questão, só uma pessoa especialmente atenta ou diligente desconfiaria da sua origem.
7. O mesmo já não pode dizer-se quanto ao conteúdo da SMS, que se afigura que não podia deixar de constituir um evidente alerta para o A. por duas razões: a primeira porque dele consta: "Para voltar utilizar o APP CLIQUE: https:// novobancoapp.link? n=... Prazo 24 horas", quando o A. nunca tinha utilizado a aplicação móvel "App Novo Banco" e não a tinha instalada no seu telemóvel; a segunda porque pedia ao utilizador para clicar num *link,* quando o Banco alerta e havia alertado os seus clientes para possíveis fraudes, com a menção específica de nunca enviar aos seus clientes SMS com links com reativação de acessos.
8. Quanto à situação do A. ao clicar em tal *link* ter sido dirigido para uma página contrafeita e não para a página do Banco, afigura-se que pelo facto dessa página ter uma aparência idêntica à página oficial do Banco, não é exigível que desconfiasse de tal realidade, sendo que naquelas circunstâncias uma pessoa medianamente sagaz ou cuidadosa podia disso não se aperceber.
9. Já assim não se considera quando na suposta página de *homebanking* do seu Banco, a que o A. acedeu através do *link* que recebeu por SMS, e não pretendendo realizar qualquer operação de pagamento bancária, digita não só o seu código de segurança, bem como por duas vezes fornece 3 dígitos do seu cartão matriz, na sequência de tal lhe ser solicitado em nova SMS, afigurando-se-se que a generalidade das pessoas minimamente informadas e normalmente diligentes, não cederia o código de segurança e os dados do seu cartão matriz se não pretendesse utilizar a plataforma como instrumento de pagamento para a realização de alguma operação.

10. O A. tem um comportamento precipitado e gravemente descuidado, revelador de uma manifesta imprudência, ao clicar num *link* no sentido de reativar a utilização de uma aplicação que não tem e que não utiliza e ao fornecer as suas credenciais de segurança quando não pretendia realizar qualquer operação de pagamento, afigurando-se que uma pessoa medianamente atenta e diligente não o faria, abstendo-se pelo menos de prosseguir a operação quando tais elementos de segurança lhe são solicitados, já que não sendo assim estamos perante a desconsideração dos mais elementares deveres de cuidado e diligência.
11. O facto de nada ter chamado a atenção do A., fazendo-o duvidar que pudesse tratar-se de uma fraude e levando-o pelo menos a contactar previamente o seu Banco de modo a assegurar-se que assim não era, leva-nos a dizer que o seu comportamento foi precipitado e não minimamente ponderado e atento, o que configura uma grave violação do dever de cuidado que lhe era exigível, reveladora do incumprimento dos deveres legais e contratuais assumidos quando da sua adesão ao *homebanking*, salientando-se ainda a desconsideração das exigências de segurança e do alerta para as possíveis situações de fraude que, como é do conhecimento comum, os Bancos regularmente enviam aos seus clientes procurando preveni-las, o que no caso o Banco R. também fez.
12. O A. é licenciado em direito, exerce a advocacia e as funções de liquidatário judicial e tinha aderido há largos anos aos serviços digitais disponibilizado pelo Banco, assumindo um conjunto de deveres, designadamente relacionados com procedimentos de segurança, movimentando diversas contas bancárias e utilizando os canais digitais de *homebanking* com de forma muito assídua, pelo que não pode deixar de considerar-se que lhe era exigível um outro comportamento mais atento e cuidadoso nas circunstâncias que se apuraram, não podendo deixar de qualificar-se a sua conduta como grosseiramente negligente, que desresponsabiliza o Banco de o ressarcir os danos sofridos.

Decisão Texto Parcial:

Decisão Texto Integral:

Acordam na 2ª secção do Tribunal da Relação de Lisboa

I. Relatório

Vem AA, instaurar a presente ação declarativa de condenação sob a forma de processo comum contra o Novo Banco, S.A, pedindo a condenação deste no pagamento da quantia de €20.008,44 a título de indemnização por danos patrimoniais, acrescida de juros vencidos e vincendos desde a citação até efetivo e integral pagamento e de €10.000 de indemnização por danos não patrimoniais.
Alega, em síntese, para fundamentar o seu pedido que abriu duas contas bancárias de depósitos à ordem junto do R. e que é utilizador dos serviços de *homebanking* do R. Refere que terceiros de identidade desconhecida procederam em 20.11.2021 e 22.11.2021 a duas operações de transferência, respetivamente de

€9.998,44 de uma daquelas contas e de € 10.000,00 da outra conta, e adiantamento ("cash-advance") de € 10,00 a crédito da sua conta, operações realizadas sem a sua autorização. Alega que não ocorreu qualquer negligência grosseira da sua parte, encontran-se a R. obrigada ao pagamento das quantias peticionadas a título de danos patrimoniais. Mais refere que tal evento afetou de forma negativa a sua saúde mental e emocional, uma vez que na sequência do mesmo se viu privado de cerca de 20% das suas poupanças de mais de trinta anos de vida profissional, o que lhe provocou sofrimento psíquico, angústia e insónias. Indica ainda que se sentiu desgostoso, desanimado e desalentado, por ter a seu único cargo um filho e por as quantias acima mencionadas estarem destinadas a proporcionar ao filho a melhor educação possível e ainda porque teve de abdicar da semana de férias com a família no estrangeiro prevista para entre 27 de dezembro de 2021 e 3 de janeiro de 2022.
Devidamente citado, o R. veio contestar, concluindo pela improcedência da ação. Defende-se por impugnação e por exceção, alegando que o A. incumpriu as mais elementares regras de segurança na utilização dos seus canais digitais, ao clicar no link e fornecer os seus números de adesão, o PIN e o código da matriz, referindo que o A. sabia que a disponibilização, por qualquer meio do código PIN recebido, era suscetível de "Ativar autorizações" e que o código PIN não podia ser fornecido por meio de SMS. Alega também que os movimentos a débito indicados pelo A. ocorreram de forma regular e foram devidamente executados, uma vez que foram feitos com recurso a métodos de autenticação forte do cliente. Mais refere que alerta exaustivamente os seus clientes com medidas de segurança que os mesmos devem tomar para prevenir a ocorrência de práticas fraudulentas e que, por esse motivo, o A. não cumpriu as mais elementares regras de cuidado e zelo na utilização dos seus dispositivos móveis e informáticos e dos canais digitais, conforme era sua obrigação.
O A. veio responder no sentido da improcedência das exceções.
Foi proferido despacho saneador que afirmou a validade e regularidade da lide.
Realizou-se a audiência de julgamento e foi proferida sentença que julgou a ação totalmente improcedente, absolvendo o R. do pedido contra ele formulado.
É com esta decisão que o A. não se conforma e dela vem interpor recurso, concluindo pela sua revogação e substituição por outra que condene o R. no pedido, apresentando para o efeito as seguintes conclusões, que se reproduzem:
1ª – Na decisão colocada em crise há concretos pontos de facto que se consideram incorretamente julgados, por erro na apreciação da prova produzida, elencando-se os três factos provados que devem ser aditados ou alterados:
Facto Provado 9 - Ademais, os limites máximos de pagamento por serviço encontravam-se situados em € 500,00, desta forma impedindo o Autor de fazer pagamentos de valor superior a 500 através das referidas contas.
Facto Provado 10 - Nessa sequência, o Autor reclamou, em data anterior ao dia 19 de Novembro de 2021, do limite de pagamento acima mencionado junto do seu gerente, BB, através de e-mail e telefone, tendo-lhe sido comunicado que a R. iria proceder ao aumento do limite de pagamento, que o Autor iria ser contactado a tal propósito e que este contacto não seria feito através de mensagem.
Facto Provado 11 - Em 19 de Novembro de 2021, pelas 16h51m, o Autor recebeu, no seu telemóvel, um "SMS" do número identificado como "novobanco", enviada por terceiros não identificados e com o seguinte conteúdo: "NovoBanco: SEUS

ACESSOS FORAM BLOQUEADOS. Para voltar utilizar o APP CLIQUE: https://novobancoapp.link?n=.. Prazo 24 horas".
2ª - A matéria de facto dada por provada pelo Tribunal recorrido deve ser modificada com base nos elementos de prova indicados pelo ora Recorrente nas Alegações antecedentes e, nessa conformidade, passar a considerar-se provado que:
Facto Provado 9 - Ademais, os limites máximos de pagamento por serviço encontravam-se situados em € 500,00, redução essa introduzida pelo R., em Novembro de 2021, em virtude de estar a ser alvo de ataques cibernéticos, desta forma impedindo o Autor de fazer pagamentos de valor superior a € 500,00 através das referidas contas, não tendo este sido informado desses ataques.
Facto Provado 10 - Nessa sequência, o Autor reclamou, em data anterior ao dia 19 de Novembro de 2021, do limite de pagamento acima mencionado junto do seu gerente, BB, através de e-mail e telefone.
Facto Provado 11 - Em 19 de Novembro de 2021, pelas 16h51m, o Autor recebeu, no seu telemóvel, um "SMS" do número identificado como "novobanco", enviada por terceiros não identificados e com o seguinte conteúdo: "NovoBanco: SEUS ACESSOS FORAM BLOQUEADOS. Para voltar utilizar o APP CLIQUE: https://novobancoapp.link?n=.. Prazo 24 horas", a qual se encontra agregada de forma sequencial e é proveniente da mesma entidade emissora da "SMS" que a antecede e da "SMS" subsequente ambas remetidas pelo R..
3ª – Há ainda outro ponto de facto incorrectamente apreciado, o qual respeita ao Facto Provado 53 da decisão impugnada, neste caso, o mesmo deve considerar-se Não Provado com fundamento nos meios probatórios invocados nas Alegações sendo certo que foi redigido do seguinte modo:
- O Autor conhece com pormenor o funcionamento do sistema bancário e dos canais de acesso directo aos bancos, pelas funções profissionais acima mencionadas que desempenha e já desempenhou.
4ª – Tal Facto Provado 53 deve dar-se sem efeito por, entre outros motivos invocados nas Alegações, se encontrar em contradição insanável com o Facto Provado 51, revelando-se inconciliável a coexistência de ambos, porquanto se mostra incompatível considerar demonstrado que, no âmbito das funções profissionais, o A. tratava dos assuntos bancários via "e-mail" e que, "ex vi" das mesmas, conhecia com pormenor os canais de acesso directo aos bancos;
5ª – Em consequência da alteração da factualidade supra referida, têm que ser retiradas as respectivas ilações jurídicas, isto é, que no caso "sub judice" não houve qualquer comportamento indiciador de negligência grosseira por parte do A., poupando-se, em sede de conclusões, desenvolvimentos a propósito do enquadramento legal e a transcrição de Acórdãos sobre os quais versa a parte III desta peça processual.
6ª – Sem prejuízo do Recorrente entender que deve ser operada modificação na matéria de facto, verifica-se – sem conceder - que, mesmo que tal não ocorresse, a sentença recorrida não podia transitar em julgado visto se basear em argumentos que são contrariados quer pelos documentos juntos aos autos, quer pela prova produzida em audiência de julgamento.
7ª – O Doc. 1 da p.i. trata-se de Certificado Notarial, logo, documento autêntico, conforme preceituado pelos artigos 363º, nº 2 e 369º, ambos do Código Civil (C.C.), pelo que faz prova plena sobre a verdade dos factos, tal como resulta do

artigo 371º, nº 1, do C.C., devendo o penúltimo parágrafo desse documento ter sido levado em consideração, desde logo, na elaboração do Facto Provado 11;
8ª – O que se infere de tal documento autêntico é que o A. agiu em consonância com sms`s endereçadas para o seu número de telefone, as quais se encontram agregadas, de forma sequencial e nada podia fazer crer que não fossem provenientes do R. dado terem sido veiculadas pelo mesmo canal emissor do qual tinha recebido centenas de outras sms´s do R. pelo que não existia motivo algum para desconfiar que na origem das mesmas não estivesse esse Banco.
9ª – Apenas foi possível ter sido perpetrado o crime cibernético que vitimou o A. porque quando os terceiros ("hacker´s") enviaram, no dia 19 de Novembro de 2021, às 16,51 h., sms para o telefone do A. já tinham conseguido, em momento prévio, piratear o próprio canal emissor utilizado pelo R. para remeter mensagens a esse cliente.
10ª – Tal fragilidade demonstra que os dispositivos de segurança relacionados com o "homebanking" do R. são vulneráveis, o qual, aliás, confessou impotência para contrariar tal vulnerabilidade uma vez que no artigo 3º do requerimento que ofereceu aos autos, em 14 de Novembro de 2024, admite que: "Ora, relativamente à mensagem SMS recebida pelo A. em 19.11.2021, pelas 16h51, a mesma trata-se de uma técnica de spoofing que o R. não tem forma de impedir."
11ª – A leitura da captura de ecran do telemóvel do A. que constitui o Doc. 2 da p.i., permite que nos apercebamos da similitude entre a forma de redacção da sms fraudulenta e da imediatamente subsequente, remetida pelo R., fidedigna.
12ª - Não são evidentes erros de português na mensagem dos "hacker`s" apenas nela se tendo eliminado, na construção da frase, artigos definidos como "os" e "a" ou, caso se interprete como erro ortográfico essa supressão, então, tem forçosamente de se retirar idêntica conclusão da sms seguinte, do R., uma vez que também nela este se absteve de colocar artigos definidos, nomeadamente, "as" entre os dois vocábulos "Ativar autorizações".
13ª - Acresce que tal sms do R. utiliza – na esteira da sms fraudulenta – o português falado no Brasil na medida em que o verbo "activar" foi escrito sem a letra "c".
14ª - Ambas as mensagens usam maiúsculas pelo que, também por aí, se revelam difíceis de distinguir sendo certo que – o que é relevantíssimo – têm as duas o mesmo "I.D." (número) de origem que é aquele que o R. utiliza para, no âmbito do "homebanking", comunicar com o A..
15ª – O que se destaca na sms enviada pelo R. ao A., às 17,21 h, do dia 19 de Novembro de 2021, é que foi redigida de forma "… pouco explícita sobre o risco real em que incorre o cliente …", tal como se deixou exarado no Parecer Técnico (cfr. Ponto 3.2 do mesmo) que o A. ofereceu aos autos, em 31 de Outubro de 2024, elaborado por especialista em cibersegurança a quem o Tribunal "a quo" deu especial credibilidade, como deixou consignado no final da página 15 da sentença recorrida.
16ª – O texto dessa sms enviada pelo R., após a sms fraudulenta, padece de manifesta deficiência dado que, por um lado, nem sequer é iniciada pela indicação do remetente "Novobanco", contrariamente ao que era comum e, por outro, não transmite ao A, de forma cristalina, a gravidade daquilo que está a acontecer, isto é, que se encontra alguém com outro número de telefone, a instalar a "App", a obter/activar autorizações para modificar a autenticação do

"homebanking" e, acto contínuo, a fazer duas transferências dos montantes máximos permitidos (€ 10.000,00).
17ª - A data em que a fraude ocorreu coincidiu, cronologicamente, com período de, além de mudança da imagem do R., alteração da respectiva plataforma digital que iria levar a que o A. ficasse privado da realização de pagamentos de serviços de montantes superiores a € 500,00 no "e-banking", situação que o mesmo pretendia ver revertida e que o induziu na convicção que as sms`s que recebeu, em 19 de Novembro de 2021, se enquadravam nesse âmbito razão pela qual seguiu as correspondentes instruções.
18ª – Os meios probatórios que sustentam a alteração, bem como o aditamento, do Facto Provado 9, nomeadamente, os excertos dos depoimentos das testemunhas BB e CC citados nas Alegações, constituem demonstração cabal da existência dum facto conexo, decorrente da discussão da causa, que se prende com violação do dever de informação por parte do R. em relação ao A. dado se ter abstido de lhe comunicar, em Novembro de 2021, quando decidiu limitar o valor máximo do pagamento de serviços no "homebanking", que tal medida era consequência de actos de pirataria digital que estavam a atingir as plataformas electrónicas do R..
19ª - A informação que o R. optou por sonegar leva a que lhe seja assacada responsabilidade civil pelos danos causados ao A., por via contratual e extracontratual, uma vez que o relacionamento entre partes tem de se pautar pelo princípio da boa-fé devendo estas agir entre si com lealdade, lisura e transparência, tal como preceituam os artigos 227º, nº 1 e 762º, nº 2, ambos do C.C..
20ª – Há nexo de causalidade entre a violação do dever de informação e o dano causado já que é plausível que, caso o A. estivesse inteirado do período crítico que se atravessava no que concerne a ataques cibernéticos aos clientes do R. através do "homebanking" deste, a sms fraudulenta que recebeu poderia ter gerado desconfiança sem prejuízo da mesma provir do número de contacto do Banco.
21ª – Como ficou exarado nos artigos 4º e 5º da queixa-crime entregue, na Polícia Judiciária, a qual constitui o Doc. 10 da p.i., logo no dia imediatamente seguinte (23 de Novembro de 2021) à data em que tomou conhecimento da fraude que sofreu (22 de Novembro de 2021), é indubitável que o A. se encontrava a aguardar uma resposta do R. sobre a resolução do condicionalismo criado por este.
22ª – Acontece também que a página da "internet" para a qual o A. foi encaminhado era semelhante àquela a que regularmente acedia no "homebanking" do R., o que, também por aí, impossibilitou qualquer juízo de estranheza sobre a regularidade da operação solicitada.
23ª – Escutado o depoimento das testemunhas que lidaram profissionalmente com o A. não se infere que este seja pessoa incauta ou distraída pelo que, caso não tivesse sido previamente pirateado o canal emissor do R., a fraude electrónica não teria ocorrido por não ser expectável que alguém com tal perfil trate, negligentemente, um assunto desta natureza.
24ª – O ataque cibernético que o A. sofreu não constituiu caso isolado na medida em que, à data (final de 2021), se registou um elevado número de fraudes idênticas que vitimaram os clientes do R., como decorre, entre outros, do Doc. 13 e do Doc. 16 da p.i., além dos depoimentos das testemunhas BB, DD e CC.

25ª - Não se pode imputar ao A. uma conduta gravemente culposa perante as circunstâncias em que se desenvolveu o "caso subjudice" já que, se um número significativo de pessoas utilizador dum concreto sistema informático é induzido à prática de certos actos que resultam em prejuízo para os mesmos, tais condutas não
podem ser qualificadas como de negligência grosseira dado que o "homem médio" não as enjeita.
26ª – O A. foi empregado bancário na área comercial, durante nove meses, mas há mais de 33 anos, ou seja, em tempos em que os meios tecnológicos eram incipientes e os contactos que, desde então, estabelece com Bancos, na vida pessoal ou por motivos profissionais, são efectuados através de "e-mail" ou por telefone e não por meio de quaisquer outros sistemas de informação mais sofisticados.
27ª - Tendo o A. conhecimentos genéricos sobre a actividade bancária não dispõe de especiais competências digitais, nem acumulou qualquer experiência a lidar com canais de comunicação electrónica dos Bancos, excepto no que tange ao "e-banking" do R., do qual é cliente desde Maio de 2005, não tendo ocorrido nenhuma situação anómala durante mais de 16 anos, mas que, contudo, foi insuficiente para o colocar a salvo do crime cibernético que o vitimou em Novembro de 2021.
28ª – Assim, de acordo com o critério vertido no Considerando 72, da Directiva (U.E.) 2015/2366, que determina a necessidade de atender a todas as circunstâncias do caso para avaliar a eventual negligência da conduta do utilizador dos serviços, não se pode, mesmo admitindo que o A. facultou informações confidenciais àquele que julgava ser o R., concluir que se esteja perante uma situação de negligência grave ou grosseira cometida por aquele.
29ª – A responsabilidade pelo sucedido não pode deixar de recair sobre o R. por ter sido impotente para evitar o acesso de "hacker´s" ao canal que usa para comunicar com o A., fragilidade essa também evidente na clonagem da própria página de "homebanking", além de ter enviado mensagem pouco explícita que impediu o A. de se inteirar, guiando-se pelo critério do "homem médio", da gravidade daquilo que lhe estava a acontecer na tarde do dia 19 de Novembro de 2021.
30ª – Atento o sentido da decisão do Acórdão, do Tribunal da Relação do Porto, de 16 de Maio de 2023, que constitui o Doc. 17 junto à p.i., proferido em acção com idêntico objecto, pedido e causa de pedir aos destes autos, com o mesmo R. e com outro autor, mas que partilha com o A. a qualidade de cliente do R., é de toda a conveniência, para salvaguarda dos princípios de certeza e segurança jurídica e a fim de evitar divergências entre Arestos de Tribunais da Relação, no domínio da mesma legislação e sobre a mesma questão de direito, que a jurisprudência se mantenha uniforme pelo que o R. deve ser condenado no pedido.
O R. veio responder ao recurso, pugnando pela sua improcedência e manutenção da decisão proferida.
II. Questões a decidir:
São as seguintes as questões a decidir, tendo em conta o objeto do recurso delimitado pelo Recorrente nas suas conclusões- art.º 635.º n.º 4 e 639.º n.º 1 do CPC- salvo questões de conhecimento oficioso- art.º 608.º nº 2 *in fine*:

- da impugnação da decisão da matéria de facto;
- da (ir)responsabilidade do R. pelos danos causados por (in)existência de negligência grave ou grosseira por parte do A.
III. Fundamentos de Facto
São os seguintes os factos que resultaram provados com interesse para a decisão da causa, com as alterações resultantes da parcial procedência da impugnação da decisão da matéria de facto, quanto aos pontos 10,11 e 53, que se assinalam:
1. A Ré é uma instituição bancária e tem como objeto o exercício da atividade bancária, incluindo todas as operações acessórias, conexas ou similares compatíveis com essa atividade e permitidas por lei.
2. O Autor é, desde há mais de 20 anos, cliente da Ré, sendo titular de duas contas bancárias de depósitos à ordem, identificadas pelos números de contrato ... e ... e abertas no balcão da Avenida de Berna, em Lisboa.
3. Em 9 de maio de 2005, o Autor aderiu aos serviços digitais disponibilizados pela Ré, adesão esta à qual foi atribuído o número 6435188 e que ficou associado o número de telemóvel para segurança adicional ..., pertencente ao Autor, tendo, em consequência, sido providenciados ao Autor o número de adesão e as chaves de acesso necessárias para a utilização desse serviço digital (PIN e cartão matriz) e o código SMS, elementos estes pessoais e intransmissíveis.
4. Entre 9 de maio de 2005 e 22 de novembro de 2021, o Autor utilizou os canais digitais de *homebanking* da Ré (Novobanco online-NB Net), tendo, entre estas duas datas, concretizado mais de 8.150 logins.
5. Os serviços digitais acima mencionados concedem ao Autor a capacidade de realizar, por meio de dispositivos como computadores, *tablets* ou telefones com acesso à internet, diversas operações bancárias online relativas à sua conta, incluindo, mas não se limitando apenas a transferências e pagamentos de serviços.
6. Desde 2005 até novembro de 2021, o número identificado como "novobanco" foi o contacto utilizado pelos serviços da Ré para comunicar com o Autor, especialmente durante operações que exigiram códigos de validação.
7. Em novembro de 2021, o Autor tinha ativado o sistema de autenticação forte, através de código remetido pelo segundo, via sms, constituído por seis algarismos, sistema este do qual dependia a realização de qualquer transferência bancária com origem nas contas ... e ... e efetuada através dos canais digitais da Ré.
8. Em novembro de 2021, em data anterior ao dia 19, a Ré encontrava-se a ser alvo de alterações no logotipo e na cor dominante da marca, mudanças essas que também afetaram a plataforma digital da Ré.
9. Ademais, os limites máximos de pagamento por serviço encontravam-se situados em €500, desta forma impedindo o Autor de fazer pagamentos de valor superior a 500 através das referidas contas.
10. Nessa sequência, o Autor reclamou, em data anterior ao dia 19 de novembro de 2021, do limite de pagamento acima mencionado junto do seu gerente, BB, através de *e-mail* e telefone, tendo-lhe sido comunicado que a Ré iria diligenciar no sentido de procurar aumentar o limite de pagamento e que o Autor iria ser contactado a tal propósito. (alterado)
11. Em 19 de novembro de 2021, pelas 16h51m, o Autor recebeu, no seu telemóvel, um "SMS" do número identificado como "novobanco", enviada por terceiros não identificados e com o seguinte conteúdo: "NovoBanco: SEUS

ACESSOS FORAM BLOQUEADOS. Para voltar utilizar o APP CLIQUE: https://novobancoapp.link? n=... Prazo 24 horas", a qual se encontra agregada de forma sequencial com a SMS que a antecede e a SMS subsequente, ambas remetidas pelo R. (alterado)
12. O Autor seguiu a hiperligação constante do SMS acima mencionado, tendo sido direcionado para uma página de Internet contrafeita por terceiros com o intuito de capturar ou comprometer as credenciais de acesso a instrumentos de pagamento do *homebanking* e que possuía uma aparência idêntica à página oficial de *homebanking* da Ré, onde lhe foi pedido que colocasse o seu número de utilizador e a palavra passe.
13. O Autor colocou o nome de utilizador e a palavra passe na referida página.
14. De seguida, no dia 19 de novembro de 2021, pelas 17:15, terceiros não identificados, na posse do nome do utilizador e da palavra passe do Autor, instalaram a referida aplicação móvel da Ré "App novo banco" em telemóvel desconhecido e iniciaram sessão na mesma, através da colocação do número de utilizador e da palavra passe do Autor.
15. De seguida, pelas 17h21m, o Autor recebeu outra mensagem no seu telemóvel, enviada pela Ré e surgida como remetida pelo contacto "novobanco", com o seguinte conteúdo: "(ATENCAO – ALERTA DE FRAUDES): NÃO DIVULGUE este código por via de SMS COM LINKS nem através de CHAMADAS TELEFONICAS. Ativar autorizações. Codigo 620621".
16. Confiando na legitimidade desta mensagem, e por tal lho ter sido solicitado, o Autor digitou na página contrafeita, entre as 17h21 e as 17h24, o código de segurança 620621 e 3 códigos do seu cartão matriz.
17. Nessa sequência, pelas 17h24, os terceiros ativam a funcionalidade "Deixar cartão matriz em casa", que permite aos clientes, num só equipamento, prescindir a seu pedido da utilização do elemento adicional de segurança que o "Cartão Matriz" assegura, substituindo-o pelo PIN ou biometria.
18. De seguida, e por tal lho ter sido solicitado, o Autor digitou na página contrafeita, pelas 17h24, mais 3 códigos do cartão matriz.
19. Após, os terceiros ficaram com acesso total às contas do Autor junto da Ré, incluindo o mecanismo da autenticação forte.
20. Nessa sequência, no dia 20 de novembro de 2021, terceiros não identificados efetuaram login na "App Novo Banco", com o nome de utilizador e a palavra passe do Autor, com o número de adesão pertencente àquele (...) e o respetivo código secreto de 6 dígitos, tendo procedido à seguinte operação sem a autorização deste último: pelas 11h20m, transferência interna da quantia de € 9.998,44, da conta nº ... para EE.
21. Por sua vez, no dia 22 de novembro de 2021, terceiros não identificados efetuaram login na "App Novo Banco"", com o número de adesão pertencente ao Autor (...) e o respetivo código secreto de 6 dígitos, tendo procedido às seguintes operações sem a autorização deste último: adiantamento ("cash-advance") de € 10,00 a crédito da conta nº ... (pelas 11h15m) e transferência interna de € 10.000,00, da conta nº ... em benefício de FF (11h21m).
22. Até ao momento, as referidas quantias não voltaram a estar disponíveis nas contas do Autor.
23. O Autor apercebeu-se da realização das operações acima mencionadas apenas no dia 22 de novembro de 2021, 2ª feira, ao consultar as suas contas na sua área

pessoal do Novobanco online.
24. Em 22 de novembro de 2021, o Autor enviou *um e-mail* a BB a dar conhecimento da realização das transferências acima mencionadas sem a sua autorização, a solicitar o imediato cancelamento da movimentação das duas contas através da Internet e a solicitar o envio de comprovativo relativo a tais transferências, com o fim de as reportar às autoridades policiais.
25. No mesmo dia, o Autor efetuou o pedido de anulação dos canais diretos junto da Ré, cancelamento esse realizado de imediato pela Ré, no mesmo dia.
26. Em 29 de novembro de 2021, BB enviou ao Autor um *e-mail* a informar que o limite máximo para pagamentos de serviço era de €1.000.
27. No dia 23 de novembro de 2021, o Autor apresentou participação junto da Polícia Judiciária, reportando as operações acima mencionadas, participação esta que foi registada e deu origem ao Inquérito n.º 1110/21.6JGLSB, atualmente em investigação na Procuradoria da República da Comarca de Lisboa - DIAP - 3ª Secção.
28. Nesse mesmo dia, o Autor deu conhecimento à Ré, por *e-mail*, da apresentação da participação acima mencionada.
29. Em 7 de dezembro de 2021, o Autor enviou um *e-mail* a BB, solicitando à Ré a transmissão da sua posição sobre o pedido de reposição dos montantes acima mencionados em 10 dias.
30. No final do ano de 2021, clientes da Ré foram alvo de ataques informáticos nas respetivas contas bancárias, incluindo através do envio de mensagens com links que reencaminham para páginas falsas a solicitar as posições do cartão matriz, do aparecimento de *pop-ups* em páginas falsas semelhantes à página da Ré a solicitar fotografias do cartão matriz (*phishing*) e da realização de chamadas falsas onde terceiros se fazem passar por trabalhadores da Ré ou por funcionários de empresas de software informático (*vishing*).
31. Nessa sequência, no dia 23 de dezembro de 2021, foi publicada, no Jornal "Expresso", uma notícia com o título "Ataques informáticos: Clientes do Novo Banco ficam com as contas a zero", onde eram relatados os ataques informáticos acima mencionados e era reforçado que a Ré nunca enviava aos seus clientes *e-mails* com links e nunca pedia aos clientes mais do que 3 posições nem a fotografia do cartão matriz, sendo fraudulentas as atuações em que tal acontecesse.
32. Em tal notícia, era referido também que a Ré solicitava aos seus clientes que, em caso de dúvida, contactassem o gestor, o balcão ou outro canal oficial da mesma e que a Ré sensibilizava os seus clientes para as melhores práticas de segurança na utilização dos canais digitais e divulgava recomendações de segurança e alertas sobre os ataques informáticos mais recentes.
33. De tal notícia constava ainda a circunstância de a Ré ter comunicado as mensagens fraudulentas ao Centro Nacional de Cibersegurança, aos operadores de telecomunicações e aos prestadores de serviços de Internet onde estão alojados os sites de *phishing*.
34. Por carta registada com aviso de receção datada de 28 de julho de 2022, o Autor interpelou formalmente a Ré, concedeu-lhe o prazo de 30 dias para creditar nas contas ... e ... as quantias monetárias acima mencionadas, carta esta que foi recebida.
35. Por carta datada de 20 de setembro de 2022, a Ré declinou qualquer

responsabilidade pela reposição das referidas quantias monetárias, alegando que as operações reclamadas foram devidamente autorizadas pelo Autor e registadas e contabilizadas com padrões de segurança adequados e através dos dados de segurança pessoais e intransmissíveis (número de adesão, palavra passe e código), não tendo sido detetada qualquer falha nos canais digitais da Ré.
36. O "Jornal de Notícias" ("JN"), em 28 de novembro de 2022, publicou, na primeira página, a condenação da Ré pelo Juízo Local Cível de Penafiel, em processo instaurado por um cliente desse Banco, que foi lesado por sms fraudulento, GG, a indemnizar o lesado pela quantia de €9.400 que havia sido transferida para terceiros sem a sua autorização- Processo 659/22.8T8PNF.P1.
37. De tal notícia constava a circunstância de terceiros terem, no dia 16 de novembro de 2021, enviado o sms fraudulento através do qual a Ré contactava habitualmente o lesado e de este último ter, por tal motivo, confiando de que o mesmo provinha da Ré, ter clicado no link constante da referida mensagem, ter sido direcionado para uma página semelhante à página da Ré, onde lhe foi solicitado o número de adesão e a palavra passe, tendo, de seguida, constatado que tinham sido retirados €9.400 da sua conta sem a sua autorização.
38. Por acórdão datado de 16 de maio de 2023, a 2ª Secção do Tribunal da Relação do Porto confirmou a decisão da 1ª instância, exceto no que respeita ao pagamento de juros de mora.
39. Com a perda das quantias acima mencionadas nos dias 20 e 22 de novembro de 2021, o Autor ficou privado de cerca de 20% das poupanças que conseguiu amealhar, fruto do seu trabalho, ao longo de mais de trinta anos de vida profissional.
40. O Autor tem um filho menor de idade, de nome HH, nascido em 18 de abril de 2008 e à data, com 13 anos de idade, que vive consigo e por cujas despesas de alimentação, vestuário, saúde e educação é o Autor responsável.
41. Parte das quantias monetárias acima mencionadas seriam utilizadas pelo Autor para suportar as despesas de educação do filho HH.
42. Nessa sequência, o Autor sentiu sofrimento psíquico, angústia, insónias, desgosto profundo, desânimo e desalento com a perda e a não reposição das quantias monetárias nas suas duas contas.
43. O Autor tinha previsto passar uma semana de férias com a família, no estrangeiro, entre os dias 27 de dezembro de 2021 e o dia 3 de janeiro de 2022, plano do qual se viu forçado a abdicar em virtude do abalo, psíquico e financeiro que este episódio lhe provocou.
44. O Autor foi empregado bancário, no "Banco de Comércio e Indústria", entre 1 de abril e 31 de dezembro de 1991, tendo assumido funções de "Gestor de Particulares" nos balcões dessa instituição de crédito, no Restelo e na Avenida 1, ambos em Lisboa.
45. O Autor é licenciado em Direito e, desde 7 de agosto de 1992 até à presente data, exerce advocacia, de forma ininterrupta, sendo titular da Cédula da Ordem dos Advogados com o nº 9936 L.
46. Desde 1997 até à atualidade, o Autor trabalha também como liquidatário judicial.
47. O Autor exerce também o cargo de Administrador Judicial em processos de insolvência desde há mais de 25 anos, sendo portador do correspondente cartão e mantendo-se inscrito nas Listas de Administradores Judiciais das 23 Comarcas

do País.
48. Desde 2006 até 29 de novembro de 2023, o Autor movimentou 393 contas no "EUROBIC", na qualidade de administrador judicial.
49. Realizou também diligências junto dos Banco "EUROBIC" nos últimos 17 anos, tal como, antes, no "B.I.C. – Banco Internacional de Crédito", no "B.E.S. - Banco Espírito Santo, SA." ou no "B.P.N. – Banco Português de Negócios, SA, incluindo cancelamento de garantias bancárias prestadas a massas insolventes, abertura de contas, ordens para transferências ou pagamentos, remessa de extratos com saldos, entre outros movimentos.
50. O Autor nunca utilizou a aplicação móvel "App Novo Banco" e sabia, em novembro de 2021, que não a tinha instalada no telemóvel nem a usava.
51. No exercício das suas funções profissionais, o Autor sempre se revelou rigoroso nos pedidos que fazia aos bancos, quanto a transferências e pagamentos, sendo os procedimentos a este propósito relativos ao "Eurobic" tratados à distância, por *e-mail* entre os colaboradores do referido banco e o Autor.
52. O Autor é atento a todas as operações bancárias que ordena enquanto administrador judicial e, sempre que deteta algum erro, comunica aos funcionários do "Eurobic", solicitando que os corrijam.
53. ~~O Autor conhece com pormenor o funcionamento do sistema bancário e dos canais de acesso direto dos bancos, pelas funções profissionais acima mencionadas que desempenha e já desempenhou~~. (eliminado)
54. Das Condições Gerais de Canais Direitos da Ré é estabelecido que "Os Canais Diretos do Banco para Clientes particulares são o Novobanco Online, as suas aplicações para smartphone ou tablet ("apps") e a sua linha de atendimento telefónico, designada por Linha Direta" (Cláusula 1.1.).
55. Deste documento consta também que, para aceder aos Canais Diretos, o Cliente tem de se identificar perante o Banco, que a pedido do Cliente, emitirá os seguintes «Códigos de Segurança»: 1- Um Cartão de Acesso aos Canais Diretos, pessoal, único e intransmissível, do qual constam o número de adesão e uma chave alfanumérica constituída por 192 dígitos distribuídos em 64 posições; 2- Um Código Secreto (PIN), pessoal, único, e intransmissível, composto por 6 dígitos numéricos, que só poderá ser alterado por iniciativa do Cliente ou a solicitação do Banco, por razões de segurança e que pode ser substituída por impressão digital, imagem facial ou outro dado biométrico nas Apps para telemóvel e 3- um Código de Validação de operação, que constitui a Segurança Adicional por SMS, composto por seis dígitos, enviado por SMS, ou, alternativamente, por chamada de voz, para o número de telemóvel previamente fornecido pelo Cliente, código este que será pedido ao Cliente sempre que este efetue determinadas operações no Novobanco Online, nas Apps para telemóvel ou tablet ou por Linha Direta, indicando as mensagens SMS ou "push notification" com códigos numéricos enviadas pelo Banco, no seu texto, os detalhes da operação a autorizar (Cláusula 1.2 a 1.5).
56. Do referido documento consta também que a Ré nunca solicitará ao Cliente que introduza mais do que 3 dígitos da sua chave alfanumérica e que, caso essa informação lhe seja solicitada, verbalmente, por escrito, através da Internet ou por qualquer outra via, o Cliente se compromete-se a contactar de imediato o Banco, através do Linha Direta para o número ..., disponível 24 horas por dia (com serviço de atendimento personalizado, disponível nos horários divulgados

no site www.novobanco.pt). (Cláusula 1.6).
57. Das referidas condições consta também que "Para a iniciação e execução de instruções nos Canais Diretos do Banco, o Cliente deverá identificar-se no serviço, com os dados de acesso que lhe forem solicitados e que são explicitados nestas Condições Gerais, o Cliente consente e autoriza expressamente a execução das operações bancárias disponíveis nos Canais Diretos do Banco e que tiver selecionado, só sendo consideradas como tendo sido efetivamente recebidas e submetidas, instruções para as quais o Cliente tenha fornecido todos os dados solicitados e, posteriormente, lhe tenha sido apresentada mensagem de confirmação da correta receção e processamento da instrução" (Cláusula 7.1).
58. Ademais, a Ré reserva-se o direito de não executar operações bancárias e de não contratar serviços e/ou produtos ordenados pelo Cliente sempre que: a) A conta sobre a qual se pretende que a operação bancária solicitada seja efetuada apresente saldo insuficiente para o efetivo cumprimento da mesma, não podendo a referida conta ficar devedora, salvo se existir um Descoberto Contratado; b) Existirem dúvidas razoáveis sobre a identificação do Cliente ou sobre o seu efetivo conhecimento e consentimento relativo ao teor das instruções recebidas pelo banco; e/ou c) Esteja em causa a segurança das comunicações ou do sistema (Cláusulas 7.4 e 7.5).
59. Por outro lado, das referidas condições decorre ainda que, para evitar o uso fraudulento dos Canais Diretos do Banco, o Cliente deverá tomar as seguintes medidas preventivas: Garantir a segurança do Cartão de Acesso aos Canais Diretos, bem como do respetivo número de adesão e da chave alfanumérica; Manter o PIN secreto; Não introduzir os seus dados pessoais e Códigos de Segurança em qualquer página da Internet, com exceção das páginas ou aplicações do Banco, ou das de um prestador de Serviços de Pagamento devidamente autorizado para o exercício dessa atividade no contexto do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, estabelecido no Decreto-Lei n.º 91/2018 de 12 de novembro; Não introduzir em qualquer página da Internet, incluindo na do Banco, nem enviar por *e-mail* ou guardar de forma eletrónica mais do que três dígitos da chave alfanumérica de 192 posições, constante do seu Cartão de Acesso aos Canais Diretos; Verificar cuidadosamente o teor do SMS ou "push notification" da Segurança Adicional, só o devendo introduzir no Novobanco Online, nas Apps para telemóvel ou tablet ou por Linha Direta caso esteja seguro da autenticidade da mensagem (Cláusulas 9.1 a 9.14).
60. Destas condições consta ainda que a Ré não será, em caso algum, responsável pelos prejuízos derivados de erros de transmissão, deficiências técnicas, interferências ou desconexões ocorridas por via e no âmbito dos sistemas de comunicação utilizados para o acesso aos Canais Diretos, a menos que a ocorrência do facto danoso seja imputável a um ato seu ou a uma sua omissão culposa" (Cláusula 15.1).
61. Tais condições são do conhecimento do Autor e foram-lhe disponibilizadas pela Ré aquando da adesão aos canais diretos.
62. A Ré emite avisos e alertas de segurança acerca de mensagens fraudulentas, quer disponibilizando-os no seu sítio da internet www.novobanco.pt, quer enviando-os por *e-mail* para os seus clientes, quer através de notificações push aquando do *login* no *homebanking*.
63. Na página da Ré, https://www.novobanco.pt/, surge um separador

"Segurança Online", que diz "A sua segurança é importante. Consulte já as recomendações de segurança e os alertas de fraude".
64. Das recomendações de segurança da Ré consta a seguinte recomendação: "Atenção aos links recebidos por SMS ou *e-mail* com origem num contacto desconhecido: Evite fazer clique em mensagens, imagens ou outros conteúdos publicitários de aspeto ou origem duvidosa. Elimine a mensagem e bloqueie o remetente, ou, caso seja de uma entidade fidedigna, sugerimos que confirme a veracidade do conteúdo contactando a mesma, antes de aceder ao link. Tenha também cuidado se o SMS lhe pedir uma resposta com os seus dados pessoais. Pode não se tratar de software malicioso, mas uma forma de angariar contactos para campanhas de SPAM.".
65. Das recomendações de segurança da Ré consta ainda a seguinte. "Cuidados que deve ter com os seus dados no banco online: Desconfie de alterações na imagem gráfica do novobanco Online ou nos procedimentos de acesso a que está habituado. Por exemplo, se lhe pedirem mais dados de acesso do que o habitual, ou se a página de introdução dos dados abrir numa janela distinta. Na dúvida, contacte o Linha Direta. Desconfie se lhe forem apresentados, nas páginas, textos com erros gramaticais ou gralhas, ou se a linguagem utilizada indiciar que foram escritos por estrangeiros ou pessoas que não dominem a linguagem e os termos habitualmente utilizados no novobanco Online".
66. Dos alertas de fraude constam a circunstância de a Ré nunca enviar aos seus clientes SMS com links com reativação de acessos e os alertas emitidos pela Ré em 25 de março de 2021 e março de 2022, relativos à circunstância de a Ré nunca enviar aos seus clientes SMS com links acerca do bloqueio de acessos e a solicitação de que os clientes desconfiem, sempre de mensagens que implicam uma "ação imediata" ou "ameaças de bloqueios/suspensão de contas/acessos".
67. O jornal "Expresso" noticiou, em 9 de março de 2023, que, em 2022, a Ré obteve lucros no montante de €561.000.000,00.
68. No dia 17 de julho de 2024, a Procuradoria-Geral da República emitiu um alerta de cibercrime para uma campanha de *phishing* dirigida a clientes da Ré, em que os agentes utilizavam *e-mails* que surgem como provenientes da Ré, com dados autênticos das vítimas para simulações de páginas do banco, e que visavam a obtenção dos seus dados bancários,, referindo este alerta que, anteriormente, tinham sido enviadas mensagens SMS e de *Whatsapp* fraudulentas para clientes da Ré também surgidas como provenientes desta última e com o mesmo propósito.
69. A publicação de tal alerta foi noticiada no dia 18 de julho de 2024 pelo Jornal de Notícias.
Factos Não Provados:
A) Sempre que qualquer cliente acede ao serviço "NBnet" – imediatamente após a introdução das credenciais de acesso e mesmo antes de conseguir aceder a qualquer menu – é confrontado com um alerta de segurança "Proteja-se do roubo", a solicitar aos clientes que, quando recebam uma mensagem da Ré, a leiam atentamente e confirmem os dados das operações descritas.
B) As recomendações de segurança surgem sempre que se encerra a sessão no "NBnet".
C) Em novembro de 2021, a Ré já tinha emitido alertas para a circunstância específica de existirem mensagens que, embora provindas de um número

designado "novobanco", eram fraudulentas e para a circunstância de terceiros conseguirem enviar mensagens aos clientes da Ré através do canal "novobanco", com o intuito de deles obterem as credenciais de acesso (técnica de *spoofing*).

- da impugnação da decisão da matéria de facto

Vem o Recorrente impugnar a decisão proferida sobre a matéria de facto, quanto aos pontos 9, 10, 11 e 53 dos factos provados.

Por terem sido cumpridos os requisitos previstos no art.º 640.º n.º 1 e n.º 2 al. a) do CPC procede-se à avaliação da impugnação apresentada.

- o ponto 9 dos factos provados, apresenta a seguinte redação:

9. Ademais, os limites máximos de pagamento por serviço encontravam-se situados em €500, desta forma impedindo o Autor de fazer pagamentos de valor superior a 500 através das referidas contas.

Entende o A. que deve ser dado como provado que:

9. Ademais, os limites máximos de pagamento por serviço encontravam-se situados em €500, redução essa introduzida pelo R., em novembro de 2021, em virtude de estar a ser alvo de ataques cibernéticos, desta forma impedindo o Autor de fazer pagamentos de valor superior a 500 através das referidas contas, não tendo este sido informado desses ataques.

Para fundamentar o aditamento pretendido invoca o depoimento da testemunha BB e CC, nos excertos de gravação que identifica.

O tribunal *a quo* fundamentou da seguinte forma resposta a esta matéria: *"Os factos 8, 9 e 10 resultaram das declarações de parte do Autor, às quais o Tribunal confere, de forma geral credibilidade, atenta a forma clara e objetiva como foram prestadas, tendo sido igualmente confirmados pelas testemunhas CC e BB, este último funcionário da Ré desde 2007 e gerente de conta do Autor em 2021."*

Salienta-se que esta matéria que o Recorrente pretende que seja aditada aos factos provados, não foi por ele alegada na p.i., não constituindo facto essencial que integre a causa de pedir apresentada nos termos do art.º 5.º n.º 1 do CPC, não tendo sido invocada a violação de qualquer dever de informação por parte do R., não assumindo relevância para a boa decisão da causa.

O que consta do ponto 9 dos factos provados pode relevar apenas no contexto que foi apurado, no sentido de que o A. estava à espera de uma comunicação do banco, por ter reclamado sobre o limite máximo que estava a ser autorizado para os pagamentos através dos canais digitais, o que os factos provados 10 e 26 já permitem inferir.

É irrelevante para o caso saber o que levou à fixação desse limite, ou a existência de alguma falta de informação ao A. sobre eventuais ataques cibernéticos de que o Banco pudesse ter sido alvo, questão que não está em discussão nos autos, não só porque não foi em tal situação que o A. fundamentou o seu pedido, mas também porque não foi na sequência de qualquer ataque ao sistema informático do Banco que foi retirado o dinheiro da conta do A.

Salienta-se que o A. na p.i. não veio invocar a violação de qualquer dever de informação por parte do R., apenas lhe fazendo referência agora em sede de recurso.

De qualquer modo, conforme consta da al. C) dos factos não provados, não resultou provado que o R. tenha emitido junto dos clientes em novembro de 2021, algum alerta para específico de existirem mensagens fraudulentas provindas de um número designado "novobanco".

Uma vez que o aditamento desta matéria não é relevante para a decisão de causa, atenta a causa de pedir configurada pelo A. na sua petição inicial, por a alteração pretendida não ser suscetível de interferir na mesma, é inútil a apreciação da impugnação da decisão de facto nesta parte, sendo que de acordo com o princípio da limitação dos atos, previsto no art.º 130.º do CPC não é sequer lícita a prática de atos inúteis no processo.
No sentido de constituir um ato manifestamente inútil analisar a impugnação da decisão da matéria de facto se os factos impugnados não tiverem qualquer relevância para a decisão, tem vindo a pronunciar-se a nossa jurisprudência, do que são exemplo, entre outros, o Acórdão do TRC de 12 de junho de 2012 no proc. 4541/08, o Acórdão do TRP de 7 de maio de 2012 no proc. 2317/09 ou o Acórdão do STJ de 17 de maio de 2017 no proc. 4111/13.4TBBRG.G1.S1 todos *in* www.dgsi.pt, referindo-se neste último: "*O princípio da limitação de actos, consagrado no artigo 130º do Código de Processo Civil para os actos processuais em geral, proíbe a sua prática no processo – pelo juiz, pela secretaria e pelas partes – desde que não se revelem úteis para este alcançar o seu termo. Trata-se de uma das manifestações do princípio da economia processual, também aflorado, entre outros, no artigo 611º, que consagra a atendibilidade dos factos jurídicos supervenientes, e no artigo 608º n.º 2, quando prescreve que, embora deva resolver todas as questões que as partes tenham submetido à sua apreciação, o juiz não apreciará aquelas cuja decisão esteja prejudicada pela solução dada a outras. Nada impede que também no âmbito do conhecimento da impugnação da decisão fáctica seja observado tal princípio, se a análise da situação concreta em apreciação 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. Com efeito, aos tribunais cabe dar resposta às questões que tenham, directa ou indirectamente, repercussão na decisão que aprecia a providência judiciária requerida pela(s) parte(s) e não a outras que, no contexto, se apresentem como irrelevantes e, nessa medida, inúteis.*"
Como se referiu, juridicamente não tem qualquer relevância o aditamento da matéria pretendida, por não ser suscetível de influenciar a decisão da causa, não se conhecendo a impugnação apresentada nesta parte.
- o ponto 10 dos factos provados, tem o seguinte teor:
10. Nessa sequência, o Autor reclamou, em data anterior ao dia 19 de novembro de 2021, do limite de pagamento acima mencionado junto do seu gerente, BB, através de *e-mail* e telefone, tendo-lhe sido comunicado que a Ré iria proceder ao aumento do limite de pagamento, que o Autor iria ser contactado a tal propósito e que este contacto não seria feito através de mensagem.
Quanto a este facto o que o Recorrente pretende é que o mesmo passe a ter a seguinte redação:
10. Nessa sequência, o Autor reclamou, em data anterior ao dia 19 de novembro de 2021, do limite de pagamento acima mencionado junto do seu gerente, BB, através de *e-mail* e telefone.
Tal traduz-se na exclusão do segundo segmento deste ponto, eliminando-se: "*tendo-lhe sido comunicado que a Ré iria proceder ao aumento do limite de pagamento, que o Autor iria ser contactado a tal propósito e que este contacto não seria feito através de mensagem*".
Invoca para o efeito o doc. 7 junto com a p.i., as declarações de parte do A. e o

depoimento das testemunhas BB e CC, nos excertos de gravação que indica.
O doc. 7 representa a cópia de um email enviado por BB ao A., datado de 29.11.2021, indicando como assunto "NB- Pag Serviços – valor limite p/ pagamentos on line", onde é referido que na sequência das conversas sob o assunto em subject, informa que o limite para pagamento de serviços é agora 1.000€.
O A. nas suas declarações afirma efetivamente que contactou aquele seu gestor no sentido de poder ser aumentado o valor máximo dos pagamentos por meios digitais, afirmando que aquele ficou de lhe dizer alguma coisa sobre o assunto, mas não lhe disse de que forma essa informação podia chegar.
A testemunha BB, gestor de conta do A. refere que não foi dito ao A. que o limite ia ser aumentado, nem que a questão ia ser resolvida por sms, confirmando, no entanto, conversas com o A. sobre tal assunto.
Já a testemunha CC diz que a indicação que era dada aos clientes era para o fazerem (os pagamentos superiores ao limite existente) no multibanco, não tendo o seu depoimento sobre esta matéria revelado nada de interesse, sendo situação na qual não teve intervenção em concreto.
Da conjugação do doc. 7, com as declarações de parte do A., que não obstante ser parte interessada no processo se apresentam como credíveis, tal como também o considerou o tribunal *a quo*, e com o depoimento da testemunha BB, o que se retira com segurança o é não só que "o Autor reclamou, em data anterior ao dia 19 de novembro de 2021, do limite de pagamento acima mencionado junto do seu gerente, BB, através de *e-mail* e telefone" como facto deste ter ficado de diligenciar no sentido de ver se a situação podia ser alterada, como efetivamente veio a ser, com o aumento para o dobro do valor dos pagamentos *on line*, como resulta do email que lhe enviou mais tarde.
Já quanto à forma como essa informação seria prestada, dá-se credibilidade ao alegado pelo A. quando diz que não lhe foi dito como lhe chegaria tal informação, afigurando-se plausível que tal não tenha sido matéria especificamente abordada no contexto, podendo os intervenientes partir do princípio de que a comunicação do gerente de conta ao A. seria feita nos moldes habituais.
Regista-se ainda que o que a testemunha BB refere, é que nunca foi dito ao A. que a questão iria ser resolvida por SMS, o que é diferente de afirmar, como consta no facto provado 10, que a R. comunicou ao A. que o contacto não seria feito através de SMS.
Assim, em razão dos elementos de prova analisados, verifica-se que a última parte deste facto provado 10 carece de suporte probatório e deve ser eliminado, procedendo parcialmente a impugnação apresentada, na sequência do que se altera a sua redação que passa a ser a seguinte:
10. Nessa sequência, o Autor reclamou, em data anterior ao dia 19 de novembro de 2021, do limite de pagamento acima mencionado junto do seu gerente, BB, através de *e-mail* e telefone, tendo-lhe sido comunicado que a Ré iria diligenciar no sentido de procurar aumentar o limite de pagamento e que o Autor iria ser contactado a tal propósito.
- o ponto11 dos factos provados, tem a seguinte redação:
11. Em 19 de novembro de 2021, pelas 16h51m, o Autor recebeu, no seu telemóvel, um "SMS" do número identificado como "novobanco", enviada por terceiros não identificados e com o seguinte conteúdo: "NovoBanco: SEUS

ACESSOS FORAM BLOQUEADOS. Para voltar utilizar o APP CLIQUE: https://novobancoapp.link? n=... Prazo 24 horas".
Não questionando a matéria provada que consta deste ponto, o que o Recorrente pretende é que lhe seja aditado o seguinte: *"a qual se encontra agregada de forma sequencial e é proveniente da mesma entidade emissora da "SMS" que a antecede e da "SMS" subsequente, ambas remetidas pelo R."*
Invoca para o efeito o doc. 1 junto à p.i., o parecer técnico que juntou aos autos a 31.10.2024 e as declarações da testemunha II.
O Recorrido vem opor-se ao aditamento requerido, alegando que não pode dizer-se que os SMS são provenientes da mesma entidade emissora, apenas podendo concluir-se que a mensagem em questão se encontra agregada de forma sequencial na mesma corrente/cadeia/histórico de mensagens do remetente "NOVOBANCO", não pertencendo a entidade emissora ao Banco, o que terá sido resultado de uma técnica de *spoofing* que o Banco não tem forma de impedir, apenas podendo ser controlada pela operadora de telecomunicações.
Invoca o parecer técnico que juntou em 14.11.2024 em resposta ao apresentado pelo A. e o depoimento das testemunhas II e DD, nos excertos de gravação que indica.
O tribunal *a quo* fundamentou da seguinte forma a resposta dada a esta matéria: *"Os factos 11 a 21 e a concreta circunstância de terem sido terceiros, e não o Autor, a instalar a aplicação móvel do Novo Banco e a usá-la entre 19 e 22 de novembro de 2021 para fazer as operações acima mencionadas resultam da conjugação das declarações de parte do Autor com o teor do print junto pela Ré em 21 de outubro de 2024 (Referência Citius40791454, de 21.10.2024), resultando igualmente a dinâmica do evento do parecer junto em 31 de outubro de 2024 aos presentes autos (Referência Citius 40911762, de 31.10.2024), ao qual o Tribunal confere especial credibilidade, uma vez que foi elaborado pelo Engenheiro II, que, ademais de Licenciado em Engenharia Eletrotécnica e Sistemas de Computadores, é especialista na área da Segurança de Informação e na Cibersegurança e na análise forense da prova digital, incluindo sistemas informáticos. Ademais, tais factos foram igualmente relatados e confirmados pelo próprio autor do parecer, II, aquando da sua inquirição, assim como pelas testemunhas CC, BB, DD e JJ (amigo do Autor e especialista em Engenharia de Software)."*
O doc. 1 junto com a p.i. corresponde a uma certificação feita por notário da existência e conteúdo de mensagens recebidas no telemóvel do A., sendo uma a SMS a que alude este facto provado, bem como a que lhe antecede e precede, do remetente identificado como NovoBanco, permitindo perceber que nestes dois no início da mensagem vem referido: "Novobanco on line", enquanto que na SMS em questão vem referido "NovoBanco".
Para melhor perceção desta questão, transcreve-se o teor de tal documento na parte que releva:

--- Mensagem enviada pelo "NovoBanco" para o número no dia dezoito de Novembro de dois mil e vinte e um, às doze horas e quatro minutos : "Novobanco Online. Transferencia Nacional/SEPA. ATENCAO: Nao divulgue este codigo a terceiros, nem atraves de chamadas telefonicas. Valor: 81,00 EUR para o IBAN PT[illegible] . Acum. Dia: 139,40 EUR Cod. Valid. 487468" ;----------

--- Mensagem enviada pelo "NovoBanco" para o número no dia dezanove de Novembro de dois mil e vinte e um, às dezasseis horas e cinquenta e um minutos :"NovoBanco: SEUS ACESSOS FORAM BLOQUEADOS. Para voltar a utilizar o APP CLIQUE: https://novobancoapp.link?n= Prazo 24 horas."; ----------

--- "[ATENCAO – ALERTA DE FRAUDES]: NAO DIVULGUE este codigo por via de SMS COM LINKS nem atraves de CHAMADAS TELEFONICAS. Ativar autorizacoes. Codigo SMS 620621"; ----------

--- Mensagem enviada pelo "NovoBanco" para o número no dia vinte e sete de Janeiro de dois mil e vinte e dois, às treze horas e trinta e oito minutos: "Novobanco Online. Login com Autenticacao Forte. Codigo de Validacao: 638380" .----------

O denominado parecer técnico junto pelo A. a 31.10.2024 encontra-se assinado por II, também ouvido como testemunha, ali sendo feita a análise da matéria alegada nos autos pelo A.

Contrariamente ao que refere o Recorrente, dele não é possível retirar, sem mais, que a SMS em questão *é proveniente da mesma entidade emissora da "SMS" que a antecede e da "SMS" subsequente, ambas remetidas pelo R.",* já que se se atentar no ponto 1 da pág. 5 de tal relatório, verifica-se que é aberta a possibilidade de ter existido um imitação do número de origem usado pelo banco, numa técnica denominada de *spoofing*.

Isso mesmo resulta também das declarações da testemunha II sobre a matéria, quando refere que há uma sequência de mensagens que vêm todas com o mesmo número de origem, concluindo que o atacante terá enviado uma mensagem com I.D. de origem igual ao número que o Novo Banco costuma utilizar, salientando-se que o conhecimento que o mesmo mostra ter é o que lhe advém da consulta do presente processo, depondo o mesmo não tanto como testemunha, mas como perito.

Os elementos probatórios indicados pelo Recorrido apontam no mesmo sentido, sendo que o depoimento da testemunha DD, Inspetor da Polícia Judiciária, que de igual modo faz declarações sobre os factos enquanto técnico ou perito, esclarecendo no que consiste a técnica de *spoofing*, centra o problema no âmbito

das redes de comunicação dos operadores, que permitem a personificação de qualquer número com recurso a técnicas ou meios ilícitos, e não no sistema informático da entidade bancária, referindo que é da responsabilidade daquelas juntamente com as entidades reguladores precaverem-no.
O que decorre do conjunto destes elementos de prova, é que as mensagens em questão vêm com a indicação do mesmo número de origem, que pode ter sido imitado pelo atacante, e não que tiveram a mesma origem, ou seja, não permitem concluir, como pretende o A., que foram todas emitidas pelo R.
Em face do exposto, a impugnação apresentada a este facto procede apenas em parte, de modo a refletir o facto da mensagem em questão se apresentar no telemóvel do A. sequencialmente com outras provenientes do R., não podendo, no entanto, dizer-se que foi proveniente da mesma entidade emissora – o R., na sequência do que se altera a redação deste facto provado, que passa a ser a seguinte:
11. Em 19 de novembro de 2021, pelas 16h51m, o Autor recebeu, no seu telemóvel, um "SMS" do número identificado como "novobanco", enviada por terceiros não identificados e com o seguinte conteúdo: "NovoBanco: SEUS ACESSOS FORAM BLOQUEADOS. Para voltar utilizar o APP CLIQUE: https://novobancoapp.link? n=... Prazo 24 horas", a qual se encontra agregada de forma sequencial com a "SMS" que a antecede e a "SMS" subsequente, ambas remetidas pelo R."
- o ponto 53 dos factos provados tem o seguinte teor:
53. O Autor conhece com pormenor o funcionamento do sistema bancário e dos canais de acesso direto dos bancos, pelas funções profissionais acima mencionadas que desempenha e já desempenhou.
Entende o Recorrente que esta matéria deve ser tida como não provada.
O tribunal *a quo* fundamentou da seguinte forma a resposta a esta matéria:
"Os factos 51 a 53 foram relatados, de forma coincidente, pelas testemunhas KK e LL, que demonstraram o rigor com que o Autor exercia a sua função, a forma como este lida e trabalha enquanto administrador de insolvência e liquidatário judicial com os colaboradores do Eurobic e o grau da experiência e do conhecimento do Autor sobre o funcionamento do sistema bancário."
Refere o Recorrente que esta matéria é incompatível com o ponto 51 dos factos provados que mostra que o A. tratava dos assuntos bancários via email; invoca o doc. 19 junto com a p.i. que mostra que o A. foi empregado bancário durante nove meses; os doc. 28, 29, 30 e 31 que mostram que as instruções remetidas pelo A. ao Eurobic eram enviadas por email; o depoimento da testemunha LL que refere que os pedidos de movimentos ao Eurobic pelo A. eram feitos pelo A. por email e confirmados telefonicamente; o depoimento da testemunha MM.
Responde o Recorrido que o depoimento das testemunhas KK e as declarações do próprio A. mostram que o mesmo é conhecedor das regras relativas à utilização dos serviços de *homebanking*.
Quanto a esta questão oferece-nos apenas dizer o seguinte:
- não se vislumbra a existência de qualquer incompatibilidade entre este facto provado e o ponto 51 dos factos provados que tem o seguinte teor: "51. No exercício das suas funções profissionais, o Autor sempre se revelou rigoroso nos pedidos que fazia aos bancos, quanto a transferências e pagamentos, sendo os procedimentos a este propósito relativos ao "Eurobic" tratados à distância, por *e-*

mail entre os colaboradores do referido banco e o Autor."
- as funções profissionais que o A. desempenha ou desempenhou já constam como assentes nos pontos 44 a 47 dos factos provados;
- os pontos 48 a 52 dos factos provados referem-se a atividade ou comportamentos do A. no seu relacionamento com entidades bancárias;
- o teor do ponto 53 impugnado ao atestar que em virtude das suas funções profissionais o A. conhece com pormenor o funcionamento do sistema bancário e "dos canais de acesso direto dos bancos", não corresponde a um facto a que deva ser dada resposta em sede de decisão de matéria de facto, mas antes a uma conclusão a retirar (ou não) em sede de apreciação jurídica da causa em função da avaliação que se faça dos factos provados.
A decisão sobre a matéria de facto só deve ser integrada por factos, o que decorre do art.º 607.º n.º 4 do CPC, devendo ficar afastados da mesma os juízos meramente conclusivos ou os conceitos de direito.
Os contornos entre o que é facto e o que é direito são muitas vezes ténues, ensinando-nos Anselmo de Castro, _in_ Direito Processual Civil Declaratório, Vol. III, pág. 269: "_a linha divisória entre facto e direito não tem carácter fixo, dependendo em considerável medida não só da estrutura da norma, como dos termos da causa; o que é facto ou juízo de facto num caso, poderá ser direito ou juízo de direito noutro. Os limites entre um e outro são flutuantes"_.
Nem sempre é fácil distinguir um facto de uma conclusão ou distinguir matéria de facto de matéria de direito. Diz-nos o Acórdão do TRP de 7 outubro 2013, no proc. 488/08.1TBVPA.P1, _in_ www.dgsi.pt: "_Pode afirmar-se, em sentido muito simplificador, que uma conclusão implica um juízo sobre factos e estes, quando em si mesmos considerados, revelam uma realidade, compreensível e detetável sem necessidade de qualquer acréscimo dedutivo._"
A jurisprudência tem vindo a considerar, do que é exemplo o Acórdão do STJ de 7 de maio de 2014, no proc. 39/12.3T4AGD.C1.S1, _in_ www.dgsi.pt que: _"são de afastar expressões de conteúdo puramente valorativo ou conclusivo, destituídas de qualquer suporte factual, que sejam suscetíveis de influenciar o sentido da solução do litígio, ou seja, na expressão do Ac. de 09-12-2010 deste Supremo Tribunal, que invadam o domínio de uma questão de direito essencial."_
À luz destas considerações e revertendo para o caso em presença, sem grande dificuldade se percebe que a expressão "conhecer em pormenor" tem uma natureza conclusiva e valorativa, quando não se densifica neste ponto impugnado o âmbito do conhecimento do A. sobre o funcionamento do sistema bancário e sobre os canais de acesso direto dos bancos, o que só o recurso a outros factos concretos pode revelar.
Aquela expressão implica uma avaliação conclusiva sobre factos e não um facto em si, por não ser suscetível de ser apreendido por qualquer meio de prova enquanto realidade objetiva.
Tal não determina, porém, que esta matéria seja tida como não provada, como pretende o Recorrente, mas tão só a eliminação deste ponto 53 da decisão de facto, destinando-se a qualificação do conhecimento do A. sobre o sistema bancário e os canais digitais a ser feita, se for caso disso, em sede de avaliação jurídica da causa, em razão dos factos que resultaram provados.
Em conformidade com o exposto, elimina-se o ponto 53 dos factos provados.
IV. Razões de Direito

- da (ir)responsabilidade da R. pelos danos causados por (in)existência de negligência grave ou grosseira por parte do A.

Alega o Recorrente, em síntese, que não pode qualificar-se o seu comportamento como grosseiramente negligente, em face das circunstâncias concretas que resultam dos factos provados que analisa, invocando a responsabilidade do R. por não ter evitado o acesso de *hacker's* ao canal que usa para comunicar com os clientes e a clonagem da sua página de *homebanking*.

O Recorrido defende que o A. agiu com negligência grosseira, clicando num *link*, sem desconfiar de uma mensagem que apresentava erros de português e que fazia menção a "voltar a utilizar o App", quando não utilizava a App Novo Banco, fazendo-o sem contactar previamente o Banco e fornecendo as suas credenciais de segurança pessoais.

A sentença sob recurso invocou a legislação aplicável ao caso e procedeu à subsunção dos factos ao direito, concluindo que para efeitos do disposto no art.º 115.º n.º 4 do DL 91/2018 o A. teve um comportamento grosseiramente negligente, na sequência do que absolveu o R. do pedido.

No que respeita à indicação da legislação relevante e normas aplicáveis ao caso em presença, o Recorrente não veio manifestar discordância com a sentença, designadamente quando a mesma situa o relacionamento das partes no âmbito da responsabilidade contratual e convoca o regime do DL 91/2028 de 12 de novembro – Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica - que veio transpor para o nosso ordenamento jurídico a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 15 de novembro de 2015.

A atividade bancária e as suas características impõem a necessidade de um conjunto de regras de conduta, não só por razões de política económica e salvaguarda do sistema financeiro, mas também por razões de tutela dos direitos e dos interesses dos clientes.

No âmbito do exercício da atividade bancária o RGIC- Regime Geral das Instituições de Crédito e Sociedades Financeiras, aprovado pelo DL 298/92 de 31 dezembro, vem integrar um conjunto de normas relativas às regras de conduta do banqueiro, sendo que em particular quanto às relações com o cliente, destaca-se o art.º 74.º do RGIC que dispõe sobre o dever de adoção por parte da instituição bancária, de deveres de diligência, neutralidade, lealdade e discrição e respeito consciencioso dos interesses que lhe estão confiados e o art.º 77.º que dispõe sobre o dever de informação e assistência.

Estas especificações acabam por mais não ser do que uma decorrência do princípio geral da boa fé que deve estar sempre presente quer na negociação e formação dos contratos, nos termos do art.º 227.º n.º 1 do C.Civil, quer na sua execução, conforme dispõe o art.º 762.º n.º 2 do C.Civil, sendo que a relação bancária tem origem contratual e assenta numa relação de confiança entre as partes.

A operação de abertura de conta bancária traduz-se num ato nuclear, o qual dá origem a uma relação tendencialmente duradoura entre a entidade bancária e o cliente e que assume a função de servir de base para outros diversos atos bancários praticados no âmbito da mesma conta. Trata-se de um contrato, na medida em que supõe uma declaração de vontade manifestada com um conteúdo específico, não se confundindo com o contrato de depósito, ainda que na maioria dos casos a abertura de conta surja associada a um contrato de depósito e este

suponha uma conta bancária aberta.
A respeito da abertura de conta bancária diz-nos L. Miguel Pestana de Vasconcelos, *in* Direito Bancário, pág. 74 e 75: *"A abertura da conta, mesmo em si, isoladamente considerada, tem um significado constitutivo, porque estabelece a base, o suporte, de todas as outras operações entre o banco e o cliente.(…) Para além disso, está previsto um conteúdo de um conjunto bastante amplo de negócios que as partes podem – mas não têm que – vir a celebrar (embora não possa haver uma recusa de celebração do banco que não seja justificada. Banco e cliente, decidindo concluir esses negócios (p. ex. cheques, cartões de crédito), fazem-no por referência a esse contrato inicial, eventualmente completando o seu conteúdo com alguns aspetos que depois venham a acordar.)*
Fala-se por vezes de uma relação bancária complexa, que visa exprimir sequências de atos e negócios jurídicos celebrados entre o banqueiro e o seu cliente, mas que não dispensa o estudo do seu conteúdo de forma individualizada. Apenas em concreto se poderá dizer se determinada relação bancária compreende uma ou várias obrigações e qual o seu teor- neste sentido, *vd.* Menezes Cordeiro, *in* Banca, Bolsa e Crédito, Estudos de Direito Comercial e de Direito da Economia, I Vol., pág. 50.
O art.º 362.º do C.Comercial qualifica as operações bancárias como operações comerciais, estipulando o art.º 363.º que estas se regem pelas *"disposições especiais respetivas aos contratos que representarem, ou em que afinal se resolverem."*
Nesta medida, quando estamos perante contratos que não disponham de um regime especial estabelecido, aplicam-se as regras do Código Civil e, quando seja, o caso do Código Comercial- *vd.* neste sentido, L. Miguel Pestana de Vasconcelos, *in* ob. cit. pág. 46.
No âmbito das relações bancárias que se estabelecem entre o Banco e os particulares, destaca-se o depósito bancário.
O depósito bancário vem expressamente previsto no art.º 407.º do C.Com. que dispõe: "*Os depósitos feitos em bancos ou em sociedades reger-se-ão pelos respetivos estatutos em tudo o que não se ache prevenido neste capítulo e demais disposições aplicáveis."*
O DL 430/91 de 2 de novembro veio regular a constituição de depósitos bancário no ordenamento jurídico português, estabelecendo no seu art.º 1º n.º 1 as modalidades de depósito.
O contrato de depósito vem previsto no art.º 1185.º do C.Civil, que nos dá a sua noção como "*o contrato pelo qual uma das partes entrega à outra uma coisa fungível, móvel ou imóvel, para que a guarde, e a restitua quando for exigida.",* prevendo o art.º 1187.º as obrigações do depositário, da qual se destaca a obrigação de restituir a coisa com os seus frutos, restituição regulamentada nos art.º 1192.º ss. do C.Civil.
Por seu turno, o art.º 1205.º do C.Civil qualifica como depósito irregular aquele que tem por objeto coisas fungíveis, remetendo o art.º 1206.º para as normas relativas ao contrato de mútuo, na medida do possível.
O depósito bancário consistindo no essencial na entrega de uma determinada quantia monetária a um banco, para que ele a guarde e restitua mais tarde outro tanto do mesmo género ou qualidade, tem por objeto uma coisa fungível, admitindo a restituição do equivalente em lugar da própria coisa entregue, tendo

vindo a ser entendido quer pela doutrina, quer pela jurisprudência, que se integra na noção de "depósito irregular".
Pela sua clareza e síntese do que vem sendo defendido sobre a qualificação do depósito bancário e seu regime jurídico, sufragando entendimento com o qual nos identificamos, temos como útil transcrever aqui excertos do Acórdão do STJ de 16-09-2014 no proc. 333/09.0TVLSB.L2.S1 *in* www.dgsi.pt onde se refere: *"O contrato de depósito bancário é geralmente definido como aquele "pelo qual uma pessoa entrega uma determinada quantidade de dinheiro a um banco, que adquire a respectiva propriedade e se obriga a restitui-lo no fim do prazo convencionado ou a pedido do depositante, mediante solicitação do depositante, nas condições previamente acordadas (Alberto Luís, Direito Bancário, ed. 1985, p. 165; João Melo Franco e Herlander Antunes Martins, Dicionário de Conceitos e Princípios Jurídicos, Coimbra, 1995, p. 309). Desta noção poderemos desde logo concluir que o contrato de depósito bancário é um contrato real, "quoad constitutionem", porque a sua constituição exige a entrega de dinheiro, ou seja, a transferência da propriedade do dinheiro do depositante para o banco. Em resumo, o contrato de depósito bancário é um contrato real, cuja perfeição só se alcança através da prática material da entrega de dinheiro (artigos 1185.º, 1205.º e 1206.º do Código Civil). O contrato de depósito bancário é um negócio jurídico bilateral, com a natureza de depósito irregular, quando tenha por objecto o depósito de fundos, com interesses quer do cliente quer do banco (PAULA PONCES CAMANHO, Do contrato de depósito bancário, p. 146/210). Embora seja este o entendimento maioritário, há também quem o considere como contrato atípico e inominado, devendo, por isso, aplicar-se-lhe, na medida do possível, as normas relativas ao contrato de mútuo (vide, entre outros, os acórdãos deste Tribunal de 19.07.79 e de 21.05.96, in, respectivamente, BMJ n.º 289, p. 345 e n.º 457, p. 343). Do contrato de depósito resulta, grosso modo, a obrigação para o depositário de guardar a quantia depositada e de a restituir (outro tanto em género e qualidade) quando for pedida. (PAULA PONCES CAMANHO, op. cit., p 176). Por outro lado, a utilização pelo banco dos montantes depositados, legalmente permitida e constitutiva da própria noção do depósito bancário, deve pautar-se pelas normas de utilização dos depósitos e pelas respectivas normas estatutárias ou usos bancários a que alude o art. 407º do C.Comercial, não podendo o banco, sem expressa anuência do depositante, dar-lhe outro fim diferente daqueles. "Sendo certo que existem diversas teses no que tange à qualificação e regime jurídico do depósito bancário, adere-se ao entendimento de acordo com o qual o depósito bancário constitui uma operação que interessa ao depositário, ao depositante e à própria organização social enquanto entidade produtora de riqueza e bem-estar. Em tal operação figura, como intermediário activo e directamente interessado, o depositário que, por isso, tem que fornecer ao depositante a necessária imagem de confiança sem a qual o depositante não lhe faculta os seus capitais. E um dos aspectos mais relevantes dessa imagem de confiança é a certeza de que o depositário assegura ao depositante a restituição do capital e acrescido, nos termos do depósito contratado." (…) O banco que recebe os valores fica obrigado à restituição do saldo existente, (quando solicitado e de acordo com as cláusulas contratuais acordadas) e obrigado à guarda e manutenção da integralidade dos fundos."*
Tal como acontece relativamente a qualquer outro contrato, se o Banco não cumpre as obrigações que para ele resultam do contrato de depósito celebrado, é

responsável pelos prejuízos que causa ao depositante, nos termos gerais previstos nos art.º 798.º e 800.º do C.Civil presumindo-se a sua culpa de acordo com o disposto no art.º 799.º n.º 1 do C.Civil, competindo-lhe por isso ilidir tal presunção, com a alegação e prova de factos que revelem que o incumprimento não resulta de culpa sua.
Diz-se com toda a propriedade na sentença sob recurso, em termos que não são contestados pelas partes: *"Quanto à natureza jurídica do contrato de depósito bancário, a doutrina e jurisprudência têm entendido que o mesmo é um depósito irregular, na aceção do artigo 1205.º do Código Civil, o que significa que são-lhe aplicáveis, por força do disposto no artigo 1206.º, do mesmo Código, na medida do possível, as regras do mútuo, nomeadamente os artigos 1142.º e 1144.º, do mesmo diploma legal (Neste sentido, Acórdão do Supremo Tribunal de Justiça de 14-12-2016, Processo n.º 1063/12.1TVLSB.L1.S1, Pinto de Almeida, disponível em www.dgsi.pt). Como tal, nos termos do disposto do artigo 1144.º, do Código Civil, com tal contrato, o banqueiro adquire a titularidade do dinheiro que lhe é entregue, sendo o cliente um credor. Assim sendo, o risco do que possa acontecer na conta do cliente recai sobre o banqueiro, a não ser que exista culpa do cliente (CORDEIRO, António Menezes, ob. cit., p. 623). Não ilidindo a instituição bancária a presunção de culpa que sobre ela impende, mantém-se a obrigação de restituição a seu cargo, nos termos das disposições conjugadas dos artigos 540.º, do n.º 1 do artigo 796.º, do n.º 1 do artigo 799.º e do artigo 1144.º, todos do Código Civil (Acórdão do Tribunal da Relação de Coimbra, de 25-06-2013, processo n.º 374/10.5 TBMGR.C1, Maria Domingas Simões, disponível em www.dgsi.pt.). O facto de o depósito bancário poder ser movimento através do serviço de homebanking não altera a sua natureza (BARREIRA, Carolina França, Homebanking: A Repartição dos prejuízos decorrentes de fraude informática, in Revista Electrónica de Direito, Outubro 2015, n.º 3, p. 7, disponível em https://www.cije.up.pt › download-file)."
O *homebanking* surge no âmbito da relação estabelecida entre o Banco e o cliente, como um contrato acessório ao contrato de depósito, que permite ao cliente efetuar uma série de operações bancárias *on line*, que o Acórdão do TRL de 13-03-2025 no proc. 11019/23.3T8SNT.L1.2 *in* www.dgsi.pt bem caracteriza, nos seguintes termos: *"O homebanking – também designado por online banking, internet banking, e-banking, banca ao domicílio, banca eletrónica, banco online – consiste num sistema de canais digitais disponibilizado pelo banco via Internet que permite aos clientes obter informações sobre a sua conta bancária, efetuar transferências e pagamentos, entre outras operações bancárias, e que tradicionalmente apenas eram feitas "ao balcão", nos espaços físicos de agências e sucursais. O contrato de homebanking é um contrato acessório do de conta bancária e que regula os direitos e deveres das partes no acesso e movimentação da(s) conta(s) bancária(s) pelo cliente bancário através de canais digitais disponibilizados pelo banco. Apesar de a lei não lhe atribuir um nome nem um conjunto concentrado de regras que o visem em exclusivo, é já um tipo social bem reconhecido na comunidade jurídica, e na sociedade em geral, por força da sua frequente e generalizada repetição na prática bancária, e pelo sequente tratamento que tem na doutrina – v.g., além dos textos supra citados, Calvão da Silva, «Conta corrente bancária, operação não autorizada e responsabilidade civil, STJ, Acórdão de 18 de dezembro de 2013», Revista de Legislação e de Jurisprudência, Ano 144, n.º 3991 (mar.-abr. 2015), pp. 290-326, Bruno Silva Palhão, «Os serviços de

pagamento e as operações não autorizadas», Cadernos de Direito Privado, n.º 65 (jan.-mar. 2019), pp. 3-17, Hugo Luz dos Santos, «Plaidoyer por uma "distribuição dinâmica do ónus da prova" e pela "teoria das esferas de risco" à luz do recente Acórdão do Supremo Tribunal de Justiça, de 18/12/2013 , o (admirável) "mundo novo" no homebanking?», O Direito, Ano 147, n.º 3 (2015), pp.715-743 –, e na jurisprudência (v.g., Ac. STJ de 23/01/2024, proc. 379/21.0T8FAR.E1.S1, Cons. Nelson Borges Carneiro).”

O progresso tecnológico que agora permite que o cliente do banco possa realizar operações bancárias que anteriormente só podia fazer se se deslocasse ao balcão do Banco ou a uma caixa ATM, não é apenas um fator de comodidade para o cliente, apresentando-se também como muito favorável para os bancos, na medida em que a implementação destes serviços lhes permitiu fazer uma reorganização dos seus trabalhadores e instalações, reduzindo de forma relevante os seus custos e consequentemente aumentar os seus lucros.

Esta situação veio exigir não só a implementação pelos Bancos de regras de segurança, como forma de obviar a ataques às suas plataformas informáticas que atualmente e cada vez mais acontecem, perpetradas com o objetivo de conseguir o acesso a contas bancárias de clientes de modo a delas serem retirados fundos, mas também impor que os próprios clientes adotem comportamentos seguros que não facilitem ou permitam o acesso às suas contas bancárias por terceiros

Na regulação desta realidade e com o fim de reduzir os riscos associados à utilização dos meios digitais, importa ter em conta o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica aprovado pelo DL 91/2018 de 12 de novembro que veio transpor para a nossa ordem jurídica a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015, regulando o acesso à atividade das instituições de pagamento e a prestação de serviços de pagamento, bem como o acesso à atividade das instituições de moeda eletrónica e a prestação de serviços de emissão de moeda eletrónica.

Para o caso que nos interessa, importa particularmente ter em conta as normas que integram o capítulo III deste Decreto Lei, que se reporta aos “Direitos e obrigações relativamente à prestação e utilização de serviços de pagamento”, destacando-se os art.º 110.º a 114.º do mesmo.

O art.º 110.º com a epígrafe “Obrigações do utilizador de serviços de pagamento associadas aos instrumentos de pagamento” estabelece:

“1- O utilizador de serviços de pagamento com direito a utilizar um instrumento de pagamento deve:

a)Utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, as quais têm de ser objetivas, não discriminatórias e proporcionais; e

b) Comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento ou à entidade designada por este último, a perda, o furto, 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 logo que receber um instrumento de pagamento, para preservar a segurança das suas credenciais de segurança personalizadas.”

Por seu turno, o art.º 111.º reporta-se às obrigações do prestador de serviços, de

pagamento associadas aos instrumentos de pagamento, prevendo que:
"1- O prestador de serviços de pagamento que emite um instrumento de pagamento deve:
a. ***Assegurar que as credenciais de segurança personalizadas do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento, sem prejuízo das obrigações do utilizador do serviço de pagamento estabelecidas no artigo anterior;***
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 comunicação prevista na alínea b) do n.º 1 do artigo 110.º ou solicitar o desbloqueio nos termos do n.º 4 do artigo 108.º;***
d. ***Facultar ao utilizador do serviço de pagamento, a pedido deste, os meios necessários para fazer prova, durante 18 meses após a comunicação prevista na alínea b) do n.º 1 do artigo 110.º, de que efetuou essa comunicação ou solicitou o desbloqueio nos termos do n.º 4 do artigo 108.º;***
e. ***Impedir qualquer utilização do instrumento de pagamento logo que a comunicação prevista na alínea b) do n.º 1 do artigo 110.º tenha sido efetuada.***
2 - O prestador de serviços de pagamento assegura que a comunicação a que se refere a alínea c) do n.º 1 é efetuada a título gratuito, cobrando apenas, e se for caso disso, os custos diretamente imputáveis à substituição do instrumento de pagamento.
3 - O risco do envio ao utilizador de serviços de pagamento de um instrumento de pagamento ou das respetivas credenciais de segurança personalizadas corre por conta do prestador do serviço de pagamento."
Conforme consta do preâmbulo deste diploma: ***"Salienta-se ainda a exigência de uma autenticação forte do cliente, prevendo que sejam adotadas as medidas de segurança suficientes para proteger a confidencialidade e integridade das credenciais de segurança personalizadas dos utilizadores de serviços de pagamento. Os serviços de pagamento fornecidos através da Internet ou de outros canais à distância, cujo funcionamento não depende do local onde estão fisicamente situados o dispositivo utilizado para iniciar a operação de pagamento ou o instrumento de pagamento utilizado, devem incluir a autenticação do utilizador que inclua elementos que associem de forma dinâmica a operação a um montante e beneficiário específicos, de modo que o utilizador esteja sempre informado do que está a autorizar. No que respeita à responsabilidade do ordenante por operações de pagamento não autorizadas, e a fim de incentivar a notificação do prestador de serviços de pagamento de qualquer furto ou perda de um instrumento de pagamento, reduzindo assim o risco de operações de pagamento não autorizadas, o presente decreto-lei vem reduzir o montante máximo pelo qual o ordenante é responsável, limitando igualmente essa responsabilidade ao saldo disponível ou ao limite da linha de crédito associada à conta ou ao instrumento de pagamento, salvo em caso de atuação fraudulenta ou de negligência grosseira da sua parte. Os prestadores de serviço de pagamento, por sua vez, não terão de reembolsar imediatamente os ordenantes por operações de pagamento não autorizadas se suspeitarem de que o ordenante agiu fraudulentamente e procederem à respetiva comunicação às autoridades competentes."***

Por seu turno o art.º 113.º aludindo à prova da autenticação e execução de instruções de pagamento, dispõe:

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

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

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

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

Finalmente os art.º 114.º e 115.º contemplam as situações em que há responsabilidade, respetivamente do prestador de serviços de pagamento e do ordenante, em caso de operação de pagamento não autorizada.

De acordo com o art.º 114.º em caso de responsabilidade do prestador de serviços, este fica obrigado a reembolsar e/ou indemnizar o cliente nos termos estabelecidos neste artigo que, designadamente, no seu n.º 9 prevê: *"Nos casos a que é aplicável o disposto no n.º 2 do artigo 113.º, recai sobre o prestador de serviços de iniciação do pagamento o ónus de provar que, no âmbito da sua esfera de competência, a operação de pagamento foi autenticada e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento por si prestado."*

Já o art.º 115.º prevê as situações em que o ordenante é obrigado a suportar as perdas resultantes de operação de pagamento não autorizada, destacando-se, pelo interesse que têm para o caso em avaliação, os n.º 3 a 6 deste artigo, que dispõem:

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

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

5 - Se o prestador de serviços de pagamento do ordenante não exigir a autenticação

forte do ordenante, este não deve suportar quaisquer perdas relativas a operação de pagamento não autorizada, salvo se tiver agido fraudulentamente.
6 - Caso o beneficiário ou o seu prestador de serviços de pagamento não aceite a autenticação forte do cliente, reembolsa os prejuízos financeiros causados ao prestador de serviços de pagamento do ordenante."
De acordo com este regime, compete ao prestador do serviço bancário garantir a segurança do sistema eletrónico que permite a realização das operações bancárias *on line*, correndo por sua conta o risco da falha ou deficiente funcionamento do sistema eletrónico, o que também resulta do disposto no art.º 796.º n.º 1 do C.Civil, competindo-lhe alegar e provar que a operação de pagamento realizada não foi decorrente de avaria ou deficiência de segurança do sistema, e/ou que houve culpa do cliente na obtenção dos elementos de segurança necessários à instrução de pagamento realizada de forma fraudulenta.
Este regime legal, vem atribuir ambas as partes – instituição financeira e cliente - responsabilidade no cumprimento de diversos deveres associados à utilização de meios de pagamento digitais, de forma a potenciar a sua segurança, revelando porém uma preocupação do legislador em conferir uma maior proteção ao utilizador beneficiário do serviço, também evidenciada no n.º 4 do art.º 115.º do DL 91/2018, ao estabelecer que a responsabilidade deste pelas perdas resultantes de operação de pagamento não autorizada apenas ocorre, se tiver resultado de um comportamento culposo do utilizador do serviço, não apenas negligente, mas antes grosseiramente negligente, cabendo ao prestador do serviço o ónus da prova dos factos que o revelam.
Como se refere no Acórdão do TRL de 22-02-2025 no proc. 7684/22.7T8LSB.L1-2 *in* www.dgsi.pt : *"O conceito de negligência grosseira deve ser encontrado na disciplina geral do direito civil, posto que não se mostra densificado no RJSPME, como salienta Carolina França Barreira (obra citada, p. 50).*
Tratando-se de violação de deveres contratuais, a negligência grosseira em referência deve ser aferida nos termos aplicáveis à responsabilidade civil, designadamente, à luz dos arts. 799º, n.º 2, e 487º, n.º 2 do Cód. Civil, com apelo à "comparação entre o comportamento concretamente adoptado pelo agente e o que seria observado nas mesmas circunstâncias de facto por um utilizador do serviço de pagamento normalmente informado, diligente e cuidadoso, pois este é o padrão referencial ou parâmetro de aferição a considerar para apurar do grau de reprovação ou censura de que é merecedor a conduta do utilizador (o grau de reprovação ou de censura será tanto maior quanto mais ampla for a possibilidade de a pessoa ter agido de outro modo), donde resulta que a culpa grosseira ocorrerá quando a omissão do dever de cuidado em que a negligência se traduz revelar que o comportamento observado se afastou do (contraria o) grau de diligência minimamente exigível e da observância de deveres de cuidado (resultantes da relação jurídica) ostensivamente evidentes, patentes e manifestos, traduzindo desconsideração do proceder expectável a qualquer comum utilizador do serviço de pagamento minimamente cuidadoso, apresentando-se como altamente reprovável à luz do mais elementar senso comum, revelando desconformidade com todos os padrões de referência" (acórdão do TRP de 18-04-2023, acima referido, que se segue de perto). Por ausência de outro critério legal, o padrão de conduta exigível ao utilizador do serviço deve ser definido tendo em conta o modelo de uma pessoa-tipo, um sujeito ideal, o tipo de homem médio ou normal, medianamente sagaz,

prudente avisado e cuidadoso (fazendo reportar estas qualidades ao do utilizador do serviço em causa) que utiliza tais serviços."

Tem vindo a ser entendido de forma pacífica pela nossa jurisprudência e também pela doutrina, que o conceito de negligência grosseira a que alude o art.º 115.º n.º 4 do DL 91/2018 deve ser equiparado ao conceito de culpa grave no Direito Civil, podendo recorrer-se ao art.º 487.º n.º 2 do C.Civil que estabelece que a culpa é apreciada, na falta de outro critério legal, pela diligência de um bom pai de família.

Refere-se no recente Acórdão do STJ de 17-06-2025 no proc. 25239/19.1T8LSB.L1.S1 *in* www.dgsi.pt : *"O DL 91/2018 não define o que é «negligência grosseira». Lê-se, porém, no considerando 72 da Directiva 2015/2366 que, «Para avaliar a eventual negligência ou negligência grosseira cometida pelo utilizador dos serviços de pagamento, deverão ser tidas em conta todas as circunstâncias. Os elementos de prova e o grau da alegada negligência deverão ser avaliados nos termos do direito nacional. Todavia, embora o conceito de negligência implique uma violação do dever de diligência, a negligência grosseira deverá significar mais do que mera negligência, envolvendo uma conduta que revela um grau significativo de imprudência; por exemplo, conservar as credenciais utilizadas para autorizar uma operação de pagamento juntamente com o instrumento de pagamento, num formato que seja aberto e facilmente detetável por terceiros. As modalidades e condições contratuais relativas ao fornecimento e à utilização de um instrumento de pagamento que tenham por efeito agravar o ónus da prova que recai sobre o consumidor ou atenuar o ónus da prova que recai sobre o emitente deverão ser consideradas nulas e sem efeito». Na nossa doutrina distingue-se entre culpa grave ou grosseira, consistente na inobservância da diligência mínima adoptada até pelos homens medianamente negligentes; culpa leve, substanciada no incumprimento dos deveres de diligência do homem normalmente diligente; e culpa levíssima, traduzida na inobservância da diligência adoptada pelos homens especialmente diligentes. Para Maria Raquel Guimarães «a actuação gravemente negligente do utilizador de um instrumento de pagamento pressupõe que este adopta um comportamento que um utilizador médio, razoavelmente informado e esclarecido, não adoptaria» («Na minha conta ou na tua?» Revisitação do regime aplicável às operações de pagamento fraudulentas à luz da nova Proposta de um Regulamento relativo aos serviços de pagamento no mercado interno, de 28 de Junho de 2023», A Revista, 4 (2023):84). Esta autora acrescenta, como tem vindo a ser defendido, entre outros, pelos acórdãos da Relação de Lisboa de 15.3.2016, da Relação de Coimbra de 15.1.2019 e da Relação do Porto de 27.6.2022, que «não se pode qualificar a conduta de quem fornece credenciais de segurança em resultado de uma prática fraudulenta como gravemente negligente quando «essas práticas fraudulentas são levadas a cabo porque um grande número de pessoas é ludibriado através delas e não apenas as extremamente descuidadas ou incautas; e para uma conduta poder ser qualificada como grosseiramente negligente ela não pode ser susceptível de ser levada a cabo por um número significativo de homens médios» (idem)."*

A culpa enquanto juízo de reprovação de uma conduta pela omissão de um dever de diligência, não pode deixar de ter em conta as circunstâncias do caso concreto, quer as que se reportam às condições do seu agente, quer aquelas que despoletaram o seu comportamento que determinou a ocorrência do dano, só

assim podendo avaliar-se qual a diligência que no caso era exigível ao agente. Como ensina Antunes Varela *in* Das Obrigações em Geral, pág. 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".* Vale a pena ter em conta sobre esta questão, o Acórdão do TRL de 13-10-2022 no proc. 344/21.8T8AGH.L1-2 *in* www.dgsi.pt fundamentado com citação de doutrina e jurisprudência, que avalia situações de fraude eletrónica, que a dada altura refere: "*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). 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"."

No caso em presença, os factos apurados revelam e as partes não contestam, que as operações bancárias em questão, através das quais foi retirado dinheiro da conta bancária do A. não foram por ele conscientemente queridas ou consentidas, antes tendo ocorrido na sequência de uma atuação fraudulenta de terceiros, habitualmente qualificada de *phishing*.

O atacante poderá ter enviado uma mensagem com I.D. de origem igual ao número telefónico que o Novo Banco costuma utilizar, clonando o seu número telefónico através de técnicas ilícitas, com o objetivo de obter acesso a informações ou sistemas protegidos, situando-se a fraude no âmbito das redes de comunicação dos operadores de telecomunicações e não no sistema informático do terceiro, no caso o Banco.

A respeito do conceito de *phishing*, pode ler-se no já citado Acórdão do TRL de 13-03-2025, com ampla indicação de doutrina para a qual se remete: *"Recorrendo a trechos do Ac. do TRL de 12/07/2018, proc. 2256/17.0T8LSB.L1-7, da ora relatora, acessível em www.dgsi.pt (como todos os demais citados), relativo a uma situação de phishing, «O phishing assemelha-se à pesca, mas em vez de tentar capturar peixes, tenta apropriar-se de informações pessoais. O autor do phishing envia e-mail que parece proveniente de outra entidade, nomeadamente bancária, referindo que a atualização ou validação de dados é necessária e pedindo para os introduzir, depois de o destinatário clicar num dado link contido no e-mail. Depois de clicar no link, o destinatário do e-mail de phishing entra num site falso, provavelmente de aspeto parecido ao da entidade pela qual o autor do phishing se quer fazer passar, e introduz os dados necessários para o login, como o username (no caso o número de cliente) e a password (no caso o pin de 6 dígitos), entre outros. Mesmo que o visitante da página falsa apenas introduza a sua identidade e palavra-passe, isso permite ao phisher aceder à conta verdadeira e aceder a muitos mais dados.*

O que importa então avaliar é se o comportamento do A. pode ser valorado como grosseiramente negligente, em face dos factos que resultaram provados, como entendeu a sentença sob recurso, já que a não ser assim, e de acordo com o regime legal que se expôs, caberá ao R. enquanto prestador do serviço assumir a responsabilidade pelos danos resultantes das operações bancárias em questão.

A sentença concluiu pela existência de incumprimento pelo A. das condições contratuais do serviço de *homebanking* e por negligência grosseira da sua parte, avaliando a questão da seguinte forma:

"Desde logo, ficou provado que a primeira mensagem que o Autor recebeu, embora

provinda do contacto "Novobanco", apresentava erros de português de Portugal, uma vez que: 1- omitia o determinante artigo definido plural "os", antes de seus acessos, referindo-se a "seus acessos", em vez de "os seus acessos", 2- omitia a palavra "a", depois de "voltar" e antes de "utilizar" ("voltar utilizar", em vez de "voltar a utilizar") e 3- referia-se à aplicação (app) no masculino, e não no feminino ("o app", em vez de "a app"). Resultou também provado que, em novembro de 2021, o Autor não utilizava a aplicação móvel "App Novo Banco" e sabia que não a utilizava. Ficou, ademais, provado que, não obstante se encontrar pendente a resolução do limite máximo de pagamento, tinha sido comunicado ao Autor pelo gerente BB que este assunto nunca seria resolvido por mensagem. Ficou também provado que a mensagem recebida pelo Autor no dia 19 de novembro de 2021, pelas 16h51m, apenas se referia a um bloqueio do acesso do Autor à app, não fazendo qualquer menção à circunstância de pretender resolver problemas relacionados com o limite máximo de pagamento nos canais diretos da Ré. Assim sendo, dizem-nos as regras da experiência comum que alguém que não utiliza a aplicação móvel do Novo Banco e que sabe que não a utiliza, quando seja confrontado com uma mensagem com erros de português, que indica que o seu acesso à app foi bloqueado e que nada refere acerca dos limites máximos de pagamento nos canais diretos da Ré, desconfie imediatamente da legitimidade desta mensagem e tente averiguar o que se passa junto do banco, antes de clicar no link dela constante. Contudo, não foi esta a reação do Autor: não só confiou na legitimidade da mensagem, não obstante os erros manifestos de português, a circunstância de se estar a referir tão-só e somente a um bloqueio de um acesso a uma aplicação da qual não era utilizador e o facto de tal mensagem não constar a circunstância de pretender aumentar o limite máximo de pagamento nos canais diretos da Ré, como não contactou o banco e clicou, de imediato, no link constante dessa mensagem. Cumpre também referir que, como ficou provado, o Autor, ademais de ser Licenciado em Direito, possui conhecimento sólido e pormenorizado quanto ao funcionamento do sistema bancário e dos sistemas eletrónicos de pagamento dos bancos, por lidar com o setor da banca desde 1991, primeiro enquanto funcionário no "Banco de Comércio e Indústria", entre 1 de abril e 31 de dezembro de 1991 e, desde agosto de 1992 até à atualidade, como advogado, administrador de insolvência e liquidatário judicial e responsável, desde 2006, pela movimentação de 393 contas no "Eurobic" e, desde 2007, pela realização de diligências, junto do Banco "EUROBIC" e antes no "B.I.C. – Banco Internacional de Crédito", no "B.E.S. - Banco Espírito Santo, SA." ou no "B.P.N. – Banco Português de Negócios, SA, relacionadas com o cancelamento de garantias bancárias prestadas a massas insolventes, abertura de contas, ordens para transferências ou pagamentos, remessa de extratos com saldos, entre outros movimentos. Por conseguinte, era exigível ao Autor um dever de cuidado superior ao exigível ao cidadão comum, quando confrontado com uma mensagem daquele teor, dever esse que não cumpriu, ao clicar imediatamente no link sem contactar o banco previamente e colocar o seu número de adesão e o seu cartão matriz, para voltar a reativar um acesso a uma aplicação que não utilizava e à qual sabia que não tinha aderido."

Os factos provados permitem destacar dois comportamentos diferentes do A.: o primeiro (factos 11 e 12) quando na sequência de um SMS que recebeu no seu telemóvel, provindo do número identificado "novobanco" seguiu a hiperligação

nele constante que o direcionou para uma página da internet contrafeita; o segundo (factos 15 a 18) quando na sequência de um novo SMS recebido no seu telemóvel , digitou na referida página contrafeita o seu código de segurança e 3 códigos do seu cartão matriz tendo, depois de lhe ter sido pedido novamente, digitado mais 3 códigos do seu cartão matriz.
No que se refere ao primeiro comportamento, vejamos se pode dizer-se, com razoabilidade, que era exigível ao A. que não clicasse no link que surgiu num SMS enviado para o seu telemóvel por terceiros não identificados, e que seria esse o comportamento que teira uma pessoa medianamente diligente, colocada nas circunstâncias do A.
Verifica-se que a SMS em questão provinha de um número identificado como "novobanco" surgindo de forma sequencial no telemóvel do A. com outras SMS que lhe haviam sido efetivamente enviados pelo R., e com o seguinte conteúdo: "NovoBanco: SEUS ACESSOS FORAM BLOQUEADOS. Para voltar utilizar o APP CLIQUE: https://novobancoapp.link? n=... Prazo 24 horas", a qual se encontra agregada de forma sequencial com a SMS que a antecede e a SMS subsequente, ambas remetidas pelo R.
O facto da SMS em questão surgir na sequência de outras SMS emitidas pelo Banco é um elemento que desde logo aponta para a circunstância de se tratar de uma mensagem fidedigna e não obstante existam os erros de português, evidenciados na sentença, crê-se que os mesmos só por si podem não constituir um alerta para a generalidade das pessoas, na medida em que representam a ausência de artigos definidos, o que pode não ser de estranhar em face da sua natureza abreviada, pelo que se afigura que quanto à forma como foi apresentada a SMS em questão, só uma pessoa especialmente atenta ou diligente desconfiaria da sua origem.
O mesmo já não pode dizer-se quanto ao conteúdo da SMS, que se afigura não poder deixar de constituir um evidente alerta para o A. por duas razões: a primeira porque dele consta: "Para voltar utilizar o APP CLIQUE: https://novobancoapp.link? n=... Prazo 24 horas", sendo certo que conforme resultou provado (ponto 50 dos factos provados) o A. nunca utilizou a aplicação móvel "App Novo Banco" e sabia, em novembro de 2021, que não a tinha instalado no seu telemóvel e não a usava; a segunda porque pedia ao utilizador para clicar num *link*, sendo que, como se apurou (facto provado 64 - *"dos alertas de fraude constam a circunstância de a R. nunca enviar aos seus clientes SMS com links com reativação de acessos e os alertas emitidos pela R. em 25 de março de 2021 e março de 2022, relativos à circunstância da R. nunca enviar aos seus clientes SMS com links acerca do bloqueio de acessos e a solicitação de que os clientes desconfiem, sempre de mensagens que implicam uma "ação imediata" ou "ameaças de bloqueios/suspensão de contas/acessos",*) corresponde a uma prática de alerta de fraudes que a generalidade dos Bancos e Novo Banco em concreto leva e levou a cabo junto dos seus clientes chamar a atenção para o facto do Banco nunca enviar aos seus clientes SMS com links de reativação de acessos, salientando-se ainda que o *link* em questão onde o A. clicou "novobancoapp.link", da forma como é identificado, apontava para uma situação de que ao aceder-se à página respetiva, era o acesso à App, que o A. nem sequer utilizava e não tinha instalada no seu telemóvel, que estava bloqueado e que podia ser resolvido.
Constata-se ainda que das recomendações de segurança da R. consta "*Atenção*

***aos links recebidos por SMS ou e-mail com origem num contacto desconhecido: Evite fazer clique em mensagens, imagens ou outros conteúdos publicitários de aspeto ou origem duvidosa. Elimine a mensagem e bloqueie o remetente, ou, caso seja de uma entidade fidedigna, sugerimos que confirme a veracidade do conteúdo contactando a mesma, antes de aceder ao link. Tenha também cuidado se o SMS lhe pedir uma resposta com os seus dados pessoais. Pode não se tratar de software malicioso, mas uma forma de angariar contactos para campanhas de SPAM*”, sugerindo o Banco que antes de aceder a um *link*, recebido por SMS, ainda que tenha sido enviado de uma entidade fidedigna, se contacte o Banco a fim de confirmar a veracidade do seu conteúdo.**

Como se diz no TRL de 22-05-2025 no proc. 7684/22.7T8LSB.L1- 2 *in* www.dgsi.pt : *“Por outro lado, sobre o utilizador do serviço impende um conjunto de deveres acessórios de conduta conexionados com a segurança do sistema. Assim, além de dever tomar as medidas razoáveis para preservar a eficácia dos mecanismos de segurança personalizados associados ao instrumento que utiliza (art. 110º, n.º 2, do RJSPME) e de comunicar ao banco prestador do serviço, sem atraso, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento (art. 110º, n.º1, al.b), do RJSPME), sobre o utilizador recaem deveres que respeitam à necessidade de se acautelar e proteger dos perigos de fraude para os quais seja alertado pelo banco, mormente por avisos, alertas e informações de segurança feitos no momento em que acede ao serviço na página do banco, logo depois de feito o registo inicial.”*

Considera-se assim, que um utilizador do serviço medianamente diligente e cuidadoso ficaria alerta e procuraria pelo menos contactar o Banco antes de clicar num *link* recebido através de uma SMS, ainda que a identifique com origem no seu Banco, quando aquela alude ao bloqueio dos acessos a uma App que o cliente não utiliza e nem tem instalada no telemóvel, pedindo para clicar num *link* para voltar a utilizar esse serviço, não obstante os alertas de fraude emitidos pelo Banco no sentido dos clientes não o fazerem, com a indicação de que nunca lhes envia SMS com *links* acerca de bloqueios de acessos.

Não se confere relevância ao facto do A. alegar, como veio a resultar apurado que se encontrava a aguardar um contacto do Banco sobre o aumento do valor do limite máximo de pagamentos por serviço de *homebanking*, que havia solicitado por email e telemóvel ao seu gerente de conta, na medida em que nada nos referidos SMS ou contactos fraudulentos aponta para que com razoabilidade o A. pudesse pensar que era a tal situação que os mesmos se referiam.

O segundo comportamento do A. tem a ver com a sua atuação após ter acedido à referida página da Internet contrafeita por terceiros, onde colocou não só o seu nome de utilizador e palavra passe, como também aí digitou o código de segurança que lhe foi enviado através de nova mensagem, fornecendo na sequência do que lhe foi pedido por duas vezes distintas, 3 códigos do seu cartão matriz.

Quanto à situação do A. não ter desconfiado que se encontrava numa página contrafeita e não na página do Banco, afigura-se que pelo facto de dessa página ter uma aparência idêntica à página oficial do Banco, tal não seria exigível, sendo que naquelas circunstâncias uma pessoa medianamente sagaz ou cuidadosa podia disso não se aperceber.

Já assim não se considera quando na suposta página de *homebanking* do seu

Banco, a que o utilizador acede através de um novo link que recebe por SMS, e não pretendendo realizar qualquer operação de pagamento bancária, digita não só o seu código de segurança, bem como por duas vezes fornece 3 dígitos do seu cartão matriz, na sequência de tal lhe ser solicitado em nova SMS, acreditando-se que a generalidade das pessoas normalmente diligentes, não cederia o código de segurança e os dados do seu cartão matriz se não pretendesse utilizar a plataforma como instrumento de pagamento para a realização de alguma operação.
Relembra-se que o A. era cliente do R., tendo aderido há largos anos (09-05-2005) aos serviços digitais por ele disponibilizados, assim assumindo um conjunto de deveres, designadamente relacionados com procedimentos de segurança, utilizando os canais digitais de *homebanking* (Novobanco online-NB Net), tendo desde aí até à data dos factos concretizado mais de 8.150 logins, o que revela uma utilização assídua de tal canal digital.
Como se refere no Acórdão do STJ de 12-12-2023 no proc. 9240720.5T8LSB.L1.S1 *in* www.dgsi.pt : *"Com importância para o utilizador, este deve observar a obrigação de utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização; comunicar, atempadamente, a perda, roubo ou apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento, impondo-se-lhe que tome todas as medidas razoáveis, para preservar a eficácia dos dispositivos de segurança personalizados do instrumento de pagamento."*
É certo, como se referiu, que o número telefónico identificado como "novobanco" vinha sendo utilizado para o Banco comunicar com o A., especialmente quando da realização de operações que exigiram códigos de validação, tendo o A. em novembro de 2021 ativado o sistema de autenticação forte, através do qual lhe era remetido pelo Banco via SMS, um código de seis algarismos, sistema este do qual dependia a realização de qualquer transferência bancária com origem nas contas do A. efetuada através dos canais da R.
O que é mais difícil de aceitar é que uma pessoa que não pretenda realizar qualquer operação de pagamento ou transferência bancária da sua conta e não tenha ficado com os acessos bloqueados a uma APP que não tem instalada no seu telemóvel e não usa, aceda a um *link* enviado por SMS e forneça o seu nome de utilizador e a palavra passe com o número de adesão e o respetivo código secreto de 6 dígitos, e ainda digite por duas vezes os códigos do seu cartão matriz, afigurando-se que uma pessoa medianamente diligente não o faria, abstendo-se pelo menos de prosseguir a operação quando tais elementos de segurança lhe são solicitados, já que não sendo assim estamos perante a desconsideração dos mais elementares deveres de cuidado e diligência.
O facto de nada disto chamar a atenção do utilizador, fazendo-o duvidar que pudesse tratar-se de uma fraude e levando-o pelo menos a contactar previamente o seu Banco de modo a assegurar-se que assim não era, leva-nos a dizer que o seu comportamento foi precipitado e não minimamente ponderado e atento, o que configura uma grave violação do dever de cuidado, reveladora do incumprimento dos deveres assumidos quando da adesão ao contrato de *homebanking*, salientando-se ainda a desconsideração das exigências de segurança e do alerta para as possíveis situações de fraude que, como é do conhecimento comum, os Bancos regularmente enviam aos seus clientes procurando preveni-las, o que no

caso o Banco R. também fez como decorre dos pontos 62 e 66 dos factos provados, designadamente emitindo avisos e alertas de segurança acerca de mensagens fraudulentas, quer disponibilizando-os no seu sítio da internet www.novobanco.pt, quer enviando-os por *e-mail* para os seus clientes, quer através de notificações push aquando do *login* no *homebanking*.
Regista-se ainda que, embora tenha resultado provado que no final do ano de 2021, clientes do R. foram alvo de ataques informáticos nas respetivas contas bancárias, incluindo através do envio de mensagens com *links* que reencaminham para páginas falsas a solicitar as posições do cartão matriz, a verdade é que os factos não permitem aferir o universo de pessoas que foi efetivamente ludibriada ao ser alvo de tais ataques, ou viu os mesmos serem concretizados com desfalque na sua conta bancária, nem tão pouco perceber se as circunstâncias em que os mesmos ocorreram são semelhantes àquelas que aqui se apuraram
Como se refere no já citado Acórdão do TRL de 13-03-2025 a respeito de uma situação de fraude por terceiros, também aqui: *"Do lado do banco a operação decorreu dentro da normalidade e regular funcionamento dos sistemas: a transferência (…) foi executada e validada com recurso a todas as credenciais de segurança (autenticação forte do cliente): i. PIN de acesso aos canais digitais, composto por seis dígitos; ii. 3 (três) posições aleatórias do Cartão Matriz; e, iii. código de seis dígitos enviado por SMS para o número de telemóvel da autora (… 27) – um código único e irrepetível, gerado automaticamente para cada transação. (…) Do ponto de vista do banco réu, de acordo com os seus sistemas operacionais e funcionais, tudo se passa como se todas as credenciais tivessem sido introduzidas pela mão da autora, pois apenas esta tinha acesso àquelas credenciais, estava obrigada a não as divulgar, e tinha contratualmente aceitado que, se o fizesse, se divulgasse as credenciais, quem as tivesse teria total acesso à conta (v. condições contratuais do acesso aos canais digitais)."*
No caso não pode ainda deixar de considerar-se que o A. é licenciado em Direito desde agosto de 1992; foi empregado bancário, ainda que durante poucos meses e numa altura em que não era possível a realização de operações bancárias por meios digitais; no presente exerce advocacia, de forma ininterrupta, trabalhando também como liquidatário judicial desde 1997 e exerce também o cargo de Administrador Judicial em processos de insolvência desde há mais de 25 anos, sendo que as suas funções, como também decorre dos factos provados, determinaram que tenha movimentado largas dezenas de contas bancárias, sempre se revelando rigoroso na concretização de tais operações a que é atento, o que torna mais difícil perceber como é que na situação em causa desconsiderou o que nos parecem ser elementares deveres de diligência e de cuidado nos comportamentos a adotar, na sequência da adesão aos serviços dos canais diretos do Banco, cujas condições lhe foram disponibilizadas pelo R. e que conhecia – ponto 61 dos factos provados.
Perante o Banco as transações em questão foram permitidas pelo A. que, tendo sido ludibriado, embora não o querendo de forma consciente, autorizou as transferências que foram realizadas a partir das suas credenciais de segurança, incluindo a chamada autenticação forte, que forneceu a terceiros, não tendo existido intromissão no sistema informático do Banco.
Em razão dos factos apurados, conclui-se que a conduta do A. que determinou a saída de fundos da sua conta bancária, se apresenta como precipitada, manifesta

e gravemente descuidada e grosseiramente imprevidente, quando na sequência de um SMS recebido como proveniente do Banco a indicar que os Acessos foram bloqueados e que para voltar a utilizar a App, que o A. não usava nem tinha instalada no seu telemóvel, clica num link que o direciona para uma página contrafeita, sem procurar antecipadamente esclarecer-se junto do seu Banco, que sempre emitia alertas no sentido de não enviar SMS com links aos clientes acerca de bloqueio de acessos.
Persistiu o A. num comportamento manifestamente descuidado, quando não pretendendo realizar qualquer operação de pagamento eletrónico não se abstém de prosseguir, fornecendo o código de segurança e os dígitos do seu cartão matriz, credenciais de segurança personalizadas, para o que não se vê qualquer justificação relevante, já que por si não tinha sido solicitada qualquer operação de pagamento *on line*.
Impunha-se ao A. um comportamento diferente, tendo o mesmo incumprido os mais elementares deveres de cuidado a que se vinculou com o Banco no âmbito dos serviços de *homebanking* que contratou, esquecendo também todos alertas de segurança por ele comunicados, facultando a terceiros os seus dados pessoais e intransmissíveis, no que se apresenta como um incumprimento dos seus deveres, designadamente do previsto no art.º 110.º n.º 1 al. a) e n.º 2 do DL 91/2018 de 12 de novembro, pelo que não pode deixar de qualificar-se a sua conduta como grosseiramente negligente, o que em razão do disposto no art.º 115.º n.º 4 do referido diploma leva a que as perdas que para si resultaram das operações de pagamento em questão não sejam da responsabilidade do Banco, devendo ser por si suportadas.

V. Decisão:
Em face do exposto, julga-se improcedente o recurso interposto pelo A., mantendo-se a sentença recorrida.
Custas pelo Recorrente por ter ficado vencido – art.º 527.º n.º 1 e 2 do CPC.
Notifique.
*****
Lisboa, 9 de setembro de 2025
Inês Moura
Rute Sobral
António Moreira