

Tribunal da Relação de Lisboa
Processo nº 5164/19.7T8FNC.L1-2

Relator: PEDRO MARTINS

Sessão: 15 Dezembro 2022

Número: RL

Votação: UNANIMIDADE

Meio Processual: RECURSO DE APELAÇÃO

Decisão: IMPROCEDENTE

REGIME DE SERVIÇOS DE PAGAMENTO

Sumário

O art. 70/1 do Regime dos Serviços de Pagamento (anexo I ao DL 317/2009) estabelece “uma presunção de ilicitude a favor do utilizador”, identificando “os factos que devem ser provados pelo prestador para a afastar: a correcta autenticação, registo e contabilização da ordem, bem como a inexistência de avaria técnica ou qualquer deficiência.” Depois, “como norma suplementar deste regime especial”, existe “o art. 70/2 do” RSP: “ainda que o prestador de serviços consiga demonstrar” tudo aquilo, “e, além disso, prove que foi utilizado o sistema de pagamento registado pelo utilizador, essa demonstração não é suficiente para dissipar a situação de incerteza quanto à factualidade subjacente à operação não autorizada. Nestes casos, a demonstração da utilização do instrumento de pagamento – e, com esta referência tem-se obviamente por incluídos todos os protocolos e dados de autenticação –, não é suficiente para ‘provar que a operação foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações.’”

Texto Integral

Acordam no Tribunal da Relação de Lisboa os juízes abaixo identificados:

M e marido e filhos (daqui para a frente utilizar-se-á a expressão autora só para designar a autora M) intentaram uma acção contra (i) a V-SA, e a (ii) Banco-SA, (daqui para a frente identificada apenas como Banco), pedindo que elas fossem condenadas solidariamente a pagar-lhes 9.899€ de capital, 391,62 € de juros vencidos e nos que se vencerem até completo reembolso do capital,

à taxa legal anual de 4%, e 2.000€ a título de indemnização por danos morais. A V e o Banco contestaram, impugnando os factos que apontavam para as suas responsabilidade e deduzindo excepções (a V, a da sua ilegitimidade processual, julgada entretanto improcedente, e da incompetência territorial do tribunal, julgada entretanto procedente; o Banco, excepções de direito material, embora sem qualificar uma única como tal).

Os autores responderam às excepções deduzidas pela V.

Depois de realizada a audiência final foi proferida sentença, condenando o Banco a reembolsar aos autores 7.949€ com juros de mora, à taxa de 4%, vencidos desde 26/10/2018 e vincendos até integral pagamento, e absolvendo-o do demais, tal como absolveu também a V dos pedidos.

O Banco interpôs recurso, impugnando parte da decisão da matéria de facto e a sua condenação parcial, defendendo que deve ser absolvido totalmente do pedido.

Os autores e a V contra-alegaram, defendendo a improcedência do recurso.

*

Questões a decidir: se a matéria de facto deve ser alterada e se o Banco não devia ter sido condenado.

*

Foram dados como provados os seguintes factos que importam para a decisão daquelas questões [os factos já têm as alterações decorrentes da decisão da impugnação da decisão da matéria de facto, assinaladas com sublinhados ou com rasuras]:

1. A autora é cliente da V desde o ano de 1997, tendo-lhe sido atribuída a conta n.º 111111111, ao abrigo do qual a V, entregou à autora um cartão denominado “SIM V”, que lhe permitia fazer as comunicações que entendesse mediante o pagamento das tarifas acordadas e através do telemóvel com o n.º 000000000.
2. Ficou acordado entre ambas que todas as comunicações a enviar para a cliente, ora autora, seriam enviadas para a sua morada em F, sendo certo que toda a correspondência da V desde o ano de 2001, tem sido enviada para esta morada.
3. No dia 06/10/2018, a autora recebeu no seu telemóvel, com o referido cartão “SIM V”, uma mensagem com o seguinte teor: “V. O seu pedido de troca de cartão encontra-se em curso. Para mais informações ligue 22222 (tarifa aplicável). Obrigada.”
4. Atendendo a que não havia feito nenhum pedido à V, a autora telefonou para o número indicado 22222 e comunicou que não havia feito qualquer pedido de troca de cartão, mostrando-se preocupada.
5. Do outro lado da linha foi dito que a segunda via do seu cartão iria ser

cancelada.

6. Posteriormente, no dia 25/10/2018, no final do dia, a autora pretendeu fazer um telefonema com o seu referido telemóvel, mas não conseguiu tendo pensado que estava a ocorrer uma situação pontual de falta de rede.

7. Os autores M e marido são clientes do Banco com uma conta de depósito nº 333333 e a autora ainda está autorizada a movimentar duas outras contas, no mesmo Banco, uma titulada pela filha e outra titulada pelo filho.

8. Sendo os filhos jovens, ele ainda estudante universitário e ela já em fase de estágio profissional, ambos vivendo na cidade de Lisboa, estas contas serviam para os pais lhes transferirem os valores necessários aos estudos e alimentos, o que é feito normalmente pela autora, através da utilização dos serviços de *homebanking*.

9. A autora há vários anos aderiu ao serviço de *homebanking* disponibilizado pelo Banco, designado por N24, tendo-lhe sido fornecidas as chaves de acesso que lhe permitiam a utilização desse serviço através da internet.

10. A autora utilizava esses códigos de acesso para movimentar a sua referida conta bancária.

11. 54. a 59. No dia 26/10/2018, de manhã, a autora acedeu à sua conta bancária através da internet e do N24, para fazer um pagamento e, depois de o ter feito, foi surpreendida com os seguintes movimentos que haviam sido feitos entre dia 25 e dia 26/10:

- TRF. Filha, no valor de 1.000€, realizada às 18:59 de 25/10/20218;
- TRF. DE D. PRAZO 040-15.098905-7 no valor de 7.200€, realizada às 08:11 do dia 26/10/2018;
- PAG SERV. 7238 no valor de 1.969,50€, realizado às 08:15 do dia 26/10/2018;
- PAG SERV. 7527 no valor de 1.969,50€, realizado às 08:19 do dia 26/10/2018;
- PAG SERV. 4527 no valor de 1.010€, realizado às 08:23 do dia 26/10/2018;
- PAG SERV. 7522 no valor de 12,50€, realizado pela autora às 08:26 do dia 20/10/2018.

11-A., e 60. a 62. Depois do movimento das 8:26 foram ainda feitos os seguintes movimentos, às horas que se seguem de 26/10/2018:

- PAG SERV. 8951 no valor de 2.000€, realizado às 08:32;
- TRF. Filho, no valor de 1.150€, realizada às 08:35;
- PAG SERV. 4179 no valor de 1.950€, realizado às 08:38;
- TRF Filha, no valor de 775€, realizada às 08:42;
- PAG SERV. 5250 no valor de 1.000€, realizado às 09:02.

12. A autora tentou contactar imediatamente o Banco, para declarar que tais movimentos [referindo-se aos realizados até às 08:38] não haviam sido feitos

ou autorizados por si, só à terceira tentativa tendo sido atendida, ocasião em que lhe foi dado um número de Lisboa, através do qual fez a chamada descrita nos factos 52 e 63, tendo então sido aconselhada a ir à PSP apresentar queixa-crime, por burla informática.

13. E assim fez – DOC. 8.

14. Como continuava a ter dificuldade em estabelecer ligações pelo seu telemóvel, dirigiu-se em seguida à V, agência na cidade F e aí foi então informada que a V havia recebido vários pedidos de 2.ª via do seu cartão “SIM”, estando registados no sistema os seguintes pedidos:

- 1.º Pedido solicitado em 06/10/2018 e enviado pela V para Queluz;
- 2.º Pedido solicitado em 18/10/2018 e enviado pela V para Rio Tinto;
- 3.º Pedido solicitado em 22/10/2018 e enviado pela V para Rio Tinto;

15. Ou seja, a V recepcionou três pedidos de segunda via do cartão SIM 000000000, no espaço de 20 dias, pedindo o envio dessa 2.ª via para diferentes moradas que eram indicadas telefonicamente.

16. O 1.º pedido foi anulado após o telefonema da autora, o 2.º pedido não chegou a ser executado; o 3.º pedido foi executado e a V enviou uma 2.ª via do referido cartão para a morada que lhe foi indicada telefonicamente; e, por razões que se desconhecem, a V enviou nesta mesma data – 22/10/018 – outro cartão para a morada da cliente, a autora.

17. Depois de duas tentativas falhadas de pedido de 2.ª via do referido cartão, bem como da informação por parte da cliente de que não havia feito qualquer pedido de novo cartão, no dia 22/10/2018, a V enviou duas 2.ªs vias desse cartão, uma para a morada que lhe foi indicada telefonicamente por terceiros que se desconhecem e outra para a morada da cliente, ora autora.

18. Na referida agência da V, foi explicado à autora que, por ter sido emitida 2.ª via do referido cartão, o anterior havia sido desactivado, razão por que não conseguia fazer telefonemas.

19. Os serviços bancários, nomeadamente ordens de transferência e pagamentos, estão condicionados a dois passos de segurança e validação: identificação do cartão-matriz e o SMS Code.

20. O envio da segunda via do cartão SIM 000000000 para desconhecidos permitiu a estes o acesso ao segundo passo de segurança e validação que consiste no envio de um SMS com a indicação de um código, pelo Banco, para o número do telefone do cliente.

21. E assim, esses terceiros, de posse do cartão SIM 0000000000, entraram na página do *homebanking* dos autores e efectuaram movimentos nas contas bancárias à ordem e a prazo de que os referidos autores são titulares no Banco.

22. Ainda no dia 25/10/2018, começou por ser dada e executada uma ordem

de transferência do valor de 1.000€ para a conta da autora filha.

23. Tendo sido bem-sucedidos, passaram à segunda operação: passaram uma conta a prazo para a ordem, no valor de 7.200€.

24. E logo de seguida, na mesma madrugada mas já no dia 26/10/2018, efectuaram os pagamentos que se seguiram:

- 7238 no valor de 1.969,50€
- 7527 no valor de 1.969,50€
- 4527 no valor de 1.010€
- 8951 no valor de 2.000€
- 4179 no valor de 1.950€
- 5250 no valor de 1.000€

25. E na mesma data e de seguida, transferiram das contas dos autores filhos, para a conta 333333, respectivamente os valores de 775€ e 1.150€, valores estes que foram utilizados nas compras que efectuaram.

26. No total, foram feitos pagamentos ordenados e a favor de terceiros que se desconhecem, no valor de 9.899€.

27. Quanto à 2.ª via do cartão que foi enviado para a autora, foi por ela recebido no dia 26, sendo que ela só a ele teve acesso no dia seguinte quando abriu a correspondência que o carteiro lhe havia deixado na sua caixa de correio.

28. Esta 2.ª via de cartão era acompanhada de uma carta que referia: “A respectiva activação pode ser feita de forma automática e simples, ligando para o número 22222 (tarifa aplicável) e indicando o número inscrito no mesmo.”

29. Esses terceiros conseguiram ainda aceder aos dados pessoais e bancários dos autores, através da sua página *homebanking* acima referida, disponibilizada aos autores pelo Banco.

30. No dia 23/08/2019, foi creditado na conta dos autores o valor de 1.950€, a título de reembolso efectuado pelo Banco de um dos referidos pagamentos – DOC 10.

30 e 71. Em 23/08/2019 foram, em virtude da actuação do Banco, creditados na conta dos autores 1.950€ relativamente a um dos movimentos denunciados.

31. O Banco remeteu-lhes uma carta, disponibilizando-se a prestar as informações que venham a ser necessárias, mas não a indemnizar os autores – DOC 11.

32. A autora ficou muito abalada com esta situação, perdendo toda a confiança nas facilidades de pagamento fornecidas pelo banco, bem como nos telemóveis, o que lhe causa muitos incómodos.

33. A autora ficou altamente afectada no seu sono, pois ainda hoje tem noites de grandes insónias, por não conseguir obter uma justificação para este facto

e o reembolso dos valores que lhe foram retirados da sua conta bancária.

34. O processo que foi instaurado na PSP foi remetido para a Polícia Judiciária, tendo a autora já prestado declarações há vários meses, mas estando ainda pendente em fase de averiguações.

35. O Banco é uma Banco cuja actividade se caracteriza pela prática de todos os actos, por lei, permitidos aos bancos.

36. Entre o Banco e os autores foram celebrados os seguintes contratos:

- Conta à ordem n.º 333333, titulada pela autora, onde figura o marido como autorizado;
- Conta a prazo n.º 444444, titulada pela autora, onde figura o marido como autorizado;
- Conta à ordem n.º 555555, titulada pela filha, e à data dos factos figurava como autorizada a autora;
- Conta à ordem n.º 666666, titulada pelo filho onde figuram como autorizados a autora e o marido.

37. A adesão da autora ao serviço N24 foi alvo de renovação, no dia 31/01/2013, conforme contrato que se junta como doc.1.

38. Serviço através do qual os clientes bancários têm a possibilidade de aceder a informação sobre produtos e serviços do Banco, realizar operações sobre todas as contas que titulam, co titulam, ou onde figurem como autorizados, realizar operações de compra e venda, subscrição ou resgate de produtos financeiros ou serviços, entre outros.

39. Para esse efeito, foram atribuídos à autora, pelo Banco, códigos de acesso/credenciais de utilização, pessoais e intransmissíveis.

40. À data dos factos funcionavam em 4 níveis de segurança, obrigatórios, designadamente:

- a) Número de utilizador;
- b) *Password*;
- c) Cartão matriz;
- d) SMS CODE.

41. O número de utilizador e a *password* são atribuídos presencialmente, no balcão, ao cliente no momento da subscrição do serviço.

42. A *password*, composta por seis dígitos, após o primeiro login, tem de ser obrigatoriamente alterada por uma da autoria e do exclusivo conhecimento do cliente.

43. Por sua vez, o cartão matriz é composto por 72 posições, cada uma com 3 dígitos, para validação de operações passíveis de alterar o património detido pelos clientes junto do Banco.

44. Cujo processo de produção é externo ao Banco e não envolve qualquer actuação humana, uma vez que as coordenadas são geradas por computador.

45. Sendo remetido via CTT para o endereço dos clientes, e apenas passível de ser activado mediante a validação de códigos de acesso ao N24 (numero de utilizador e *password*) adstrito ao cartão expedido.

46. Por sua vez, o sistema SMS CODE consiste em associar o número de telemóvel do cliente ao *homebanking* de forma a que no momento de realizar uma operação, em que resultem alterações patrimoniais, o sistema envia um código via SMS para o seu telemóvel.

47. Assim, para a realização de uma operação com alterações patrimoniais, o utilizador teria de efectuar o login, na página da internet do Banco, colocar a sua *password*, seleccionar a operação, colocar as duas coordenadas do seu cartão matriz e recorrer ao seu telemóvel para verificar o código, aleatório, e associado aquela operação em concreto, entretanto remetido, e só mediante a sua correta validação, é que se confere validade à ordem transmitida. Cfr. doc.2.

48. A partir do momento da adesão ao referido serviço de *homebanking*, os clientes autorizam o Banco a realizar as operações ordenadas através daquele meio electrónico.

49. Nos dias 25 e 26/10/2018, com recurso a este sistema de pagamentos, mediante a correta validação das credenciais pessoais da autora, foram ordenadas 10 operações, conforme doc.3.

50. Foram explicados à autora todos os procedimentos de segurança e de utilização do referido serviço. Informação que se encontra disponível no site da ré, conforme doc.4.

51. Os movimentos indicados, apenas foram possíveis porque, em cada um deles:

a) Foi introduzido o número de utilizador;

b) Foi introduzido a *password* – importando referir que a sua introdução se faz em teclado virtual, escolhido de forma aleatória, aparecendo os números sempre em local distinto, não permitindo a identificação do código, criado pelo cliente;

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

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

52. No dia 26/10/2018 no seguimento dos contactos com o Banco, a autora alegou existirem movimentos que não reconhecia como seus.

53. De encontro à declaração entregue no balcão do Banco, a autora esclarece que: “Hoje, cerca das 08:25 da manhã fiz uma transferência para a Santa Casa da Misericórdia para jogar no euro milhões e apercebi-me que a minha conta à

ordem e a prazo tinham sido movimentadas.” “Entrei imediatamente me contacto com o Banco (agência x) para alertar sobre esta situação. Depois de contactar a agência, contactei uma agência de Lisboa e fui informada como proceder”. Documento n.º 6.

[...]

63. O pedido de cancelamento, do acesso ao *homebanking*, foi registado às 9:24 [do dia 26/10/2018], tendo a chamada acabada de ser registada às 09:41. Conforme doc.18.

64. Para que os clientes do Banco possam usar o *homebanking* é necessário além do processo de contratação do serviço, que o utilizador declare o seu número de telemóvel.

65. Que é associado ao serviço, mediante a confirmação da identidade do cliente e a inserção de um código de 6 dígitos enviado para o telemóvel declarado, para efeitos de activação do serviço. Conforme doc.19.

66. Nessa medida, e à data dos factos, a autora tinha associado ao seu N24 o número de telemóvel 000000000, conforme doc.20.

67. Assim, as operações em causa só foram processadas pela indispensável utilização do telemóvel pessoal da autora.

68. Sem o qual, as operações não seriam concretizadas, por falta de um dos mecanismos de segurança e de autenticação forte da identidade do ordenante.

69. O Banco remeteu um código para o número que a autora lhe indicou e provou estar na sua posse, por referência ao procedimento já descrito.

70. O Banco, autorizado pela autora, diligenciou no sentido de recuperar as verbas que teriam sido retiradas da sua conta. Conforme docs.3 e 21.

71. Em virtude da actuação do Banco foi possível recuperar 1.950€ que foram reembolsados à autora Documento 10.

72. A autora conhece bem as normas de segurança.

*

Da impugnação da decisão da matéria de facto

O Banco entende que deviam ter sido dados como provadas as seguintes afirmações assinaladas com números romanos que vão ser vistas a seguir, sequencialmente:

I. O sistema do Banco não foi alvo de qualquer ataque informático;

Conclui nesse sentido conjugando (i) o que consta do facto 51 que sintetiza dizendo que os movimentos em causa foram ordenados, por terceiros,

conhecedores das credenciais de acesso da autora e na posse do seu cartão SIM, e (ii) o depoimento prestado pela testemunha P donde resultaria (em passagens devidamente assinaladas – aqui como a seguir), no essencial, que

(a) o sistema informático do Banco tem forma de obstar a intrusão de *hackers*,

(b) não tem registo, nos últimos anos, de nenhum incidente de segurança, (c) o doc.5, que é um documento retirado do sistema com os *logs homebanking*, não apresenta indícios de fraude (as coordenadas do cartão matriz foram sempre colocadas), pensando que (mas não conferiu/validou isso) todos os IP de acesso estariam localizados em Portugal, pelo que, (d) os movimentos em causa só podem ter resultado de um roubo de identidade ou da entrega intencional dos dados ao agente dos movimentos pelo próprio cliente; sendo que (e) o facto de o cliente ter um antivírus no computador não seria o bastante para obstar a que informaticamente se aceda ao seu telemóvel e ao próprio computador, através de um outro tipo de engenharia social que não passe pela instalação de *malware* dentro do computador. Tudo isto seria suficiente, segundo o Banco, para “provar cabalmente que o sistema do Banco não foi alvo de qualquer ataque informático e que os movimentos evidenciados foram processados por quem era detentor das credenciais indispensáveis para o efeito, o que caracteriza o aludido esquema de engenharia social.”

Os autores respondem que a testemunha invocada pelo Banco depôs com um discurso inseguro e sem estar munida de certezas sobre as circunstâncias do caso; não fez qualquer análise concreta da situação, limitando-se a referir que, em termos regulamentares, se fazem auditorias obrigatórias anuais e que em termos de ataques o Banco tem “toda a nossa segurança” e complementando com as validações – ou seja, declarou tão só aquilo que, de senso comum, qualquer cidadão normal poderia declarar, que uma plataforma de manipulação de valores *homebanking* terá estrutura de segurança e acreditação e que será, ademais, alvo de auditorias. A inexistência de registos, nos últimos anos, de incidentes de segurança, não só é inverosímil à luz da experiência comum, como vem desmentido pelos órgãos de comunicação social; os autores transcrevem um conjunto de notícias de jornais, dos últimos 3 anos, de condenações judiciais de indivíduos responsáveis de esquemas fraudulentos com os quais obtinham dinheiro das contas no Banco, num dos casos um gerente de um balcão do próprio Banco, bem como de condenações do Banco a pagar indemnizações aos clientes vítimas de esquemas de *phishing*. Por outro lado, dizem, a testemunha não explicou, nem se concebe, como poderia ver no doc.5 indícios de fraude, pois que, para que a fraude se concretize impõe-se que a operação se realize / que o *login* se faça. Ainda dizem que não se pode afirmar que não ocorreu qualquer ataque informático quando pende investigação criminal, há três anos, com apensação a processos com data anterior à data do crime de que a autora foi vítima. Não bastaria ao Banco limitar-se a declarar que não ter ocorrido qualquer ataque informático; teria de provar que não existiu tal ataque. Aceitando a testemunha em causa, responsável pelo departamento de segurança, que as operações estão

relacionadas com um esquema de engenharia social, tal corresponde a aceitar que a autora não teve qualquer intervenção. Teria de ser o Banco a provar que as operações não autorizadas não tiveram nada a ver com avaria técnica, fragilidade, exposição ainda que momentânea, ou com outra deficiência do sistema, uma vez que só o Banco pode assegurar que o complexo sistema informático (complexo e ininteligível quanto aos requisitos de segurança para o comum utilizador) funciona bem e garante a confidencialidade dos dados do utilizador. Por outro lado, face aos factos provados sob 1 a 11 e 14 e outros, os autores concluem que o sítio do Banco foi alvo de ataque, como se encontrava sob ataque, desde, pelo menos, 06/10/2018 até à data em que o agente criminoso logrou concretizar a burla e furtar os bens da autora, pois que se tivesse sido um crime gerado por perda de cartão matriz que tivesse habilitado o acesso ao mesmo por terceiros, não estaria pendente processo-crime de investigação por vários anos.

Apreciação:

Decorre dos factos provados não impugnados que os movimentos feitos no *homebanking* da autora se processaram com o conhecimento do seu n.º do contrato, da sua *password* e do seu cartão matriz, bem como com o cartão de telemóvel da autora usado noutro telemóvel (para acesso ao código fornecido por um SMS). Mas não se apurou a forma como é que aqueles dados e os dados que permitiram a aquisição do cartão foram parar às mãos de quem fez aqueles movimentos.

Perante isto, a afirmação de que “o sistema do Banco não foi alvo de qualquer ataque informático” pode ser vista a dois níveis, como o faz o Banco: (i) em termos gerais, referindo-se aos últimos anos, ou (ii) em concreto, para o caso dos autos. Quanto à afirmação genérica (i), que aliás é aquela que formalmente é feita e que não tem qualquer interesse para os autos, o simples depoimento, nesse sentido, de uma responsável da segurança do Banco, de resto muito pouco sugestivo, não convence minimamente. Quanto ao facto de os dados da autora não terem sido obtidos com um ataque informático ao Banco – mas note-se que a afirmação, nesses termos, nem sequer foi feita, ou seja, não é ela que está em causa - dir-se-ia que é possível que assim seja mas, como não se apurou, nos autos, como é que os dados foram obtidos, não se pode dizer que tal afirmação é verdadeira com base apenas no simples depoimento daquela testemunha do Banco no sentido de que o doc.5 com os *logs* do *homebanking* da autora não mostra indícios de um tal ataque informático. Para além disso, aquela afirmação não tem qualquer interesse para o caso: nada afasta a hipótese de outro tipo de actuação ilícita ter sido a fonte da obtenção dos dados.

Veja-se, por exemplo, a questão do cartão matriz: a tese do Banco, aplicada a

este cartão, seria a seguinte (imagina-se, já que o Banco não a expõe): o cartão matriz é produzido de forma externa ao Banco; o Banco não tem acesso ao mesmo. Logo, não é possível que as coordenadas do cartão matriz tenham sido obtidas através de um ataque informático ao Banco. Mas como não se sabe como é que tais coordenadas se tornaram acessíveis à pessoa que fez os movimentos bancários ilícitos, não é possível dizer que tais coordenadas não foram obtidas através de um acesso ilícito ao sistema informático do Banco (mesmo que sejam produzidas externamente nada indica que elas não passem pelo Banco ou não sejam acessíveis seja de que modo for ao Banco antes de serem entregues ao cliente). E de qualquer modo, também não seria possível dizer que, de outro modo, que não informático, ninguém conseguiria aceder a tais coordenadas. Não é ao tribunal, nem aos clientes dos Bancos, que cabe imaginar tudo aquilo que os agentes de actos ilícitos conseguem e sabem fazer para cometer os ilícitos que cometem. Também antes de se saber o que agora se sabe, os tribunais e os clientes dos Bancos provavelmente não saberiam que era tão simples obter segundas vias de cartões de telemóveis de terceiros.

Em suma: os elementos de prova invocados pelo Banco não convencem minimamente que as credenciais da autora não tenham sido obtidas através de um ataque/acesso ilícito (informático ou não) aos dados a que o Banco tem ou pode ter acesso.

Posto isto, não deixe de se acrescentar o seguinte:

Se se reparar, aquela afirmação que o Banco pretende dar como provada é apenas uma das várias – que serão vistas a seguir – com as quais o Banco tenta torcear as normas legais que lhe impõem o ónus de provar factos positivos que permitam a conclusão de que o cliente utilizou o *homebanking* de forma fraudulenta, deliberada ou gravemente negligente, não bastando pois provar que o sistema de segurança, utilizado regularmente, não permitia, em abstracto, a utilização que ocorreu. Ora, é isto mesmo que o Banco pretende. Se isto fosse possível, ou melhor, se isto fosse legítimo, então não faria qualquer sentido que a lei exigisse a prova de factos positivos da culpa do cliente. De resto, a construção do Banco é uma outra forma de dar uso a presunções consagradas em cláusulas contratuais gerais que têm sido declaradas nulas pelos tribunais.

A questão será vista melhor mais adiante, a propósito do Direito.

De qualquer modo, cite-se desde já, ainda, Maria Raquel Guimarães, na anotação ao acórdão do STJ de 18/12/2013, proc. 6479/09, publicada nos Cadernos de Direito Privado, Jan/Março de 2015, que diz, entre outras passagens que vão no mesmo sentido dos outros autores referidos mais à frente:

“No caso analisado pelo STJ, o banco prestador do serviço afirmou que ‘não detectara qualquer indício de falha de segurança no serviço de *homebanking*’. Note-se, porém, que, nos termos do n.º 2 do mesmo art. 70.º, ‘a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, por si só, não é necessariamente suficiente para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 67.º’.

Nesta medida, recaindo sobre o prestador do serviço de pagamento a prova da não ocorrência de qualquer avaria técnica e de que a operação foi autenticada e devidamente registada e contabilizada (art. 70.º, n.º1), não lhe deverá, ainda assim, ser suficiente fazer esta prova para imputar a operação ao seu cliente ou para criar a convicção de um comportamento faltoso da sua parte. Os registos informáticos do prestador do serviço deverão ser livremente apreciados pelo julgador, devendo a sua suposta infalibilidade ser provada pelo prestador do serviço de pagamento e não ser tida como um facto incontroverso [nota: Descrente desta suposta infalibilidade dos registos informáticos dos prestadores de serviços de pagamento e criticando os tribunais por não a questionarem, apresenta-se STEPHEN MASON [...]]. Como já assinalámos, prevê o art. 70.º, n.º2, do RSP que estes registos das operações apresentados pelo prestador de serviços de pagamento não são, por si sós, suficientes para estabelecer a relação necessária entre o utilizador do serviço e a operação ou para imputar a este um incumprimento grave do contrato. Deverá ser a entidade prestadora dos serviços de pagamento a provar este incumprimento ou imputar a operação ao titular do instrumento de pagamento, socorrendo-se, para tal, de meios de prova adicionais, para além dos seus registos informáticos. A fórmula utilizada pelo legislador – “a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, por si só, não é necessariamente suficiente” - não impede, em absoluto, que o tribunal se baste com esta prova, mas parece indicar que, em regra, este prestador de serviços de pagamento deverá fornecer outros meios de prova do incumprimento do contrato, negligente ou, sobretudo, deliberado ou fraudulento, imputável ao seu cliente. Esta prova, para além do normal registo das operações, é exigível, sem qualquer dúvida, estando em causa comportamentos fraudulentos do utilizador ou o incumprimento deliberado do contrato.

No caso concreto de operações de *homebanking* fraudulentas, o julgador poderá convencer-se da existência de negligência leve do utilizador sempre que haja apropriação abusiva dos instrumentos que permitem a realização das operações, mas já os casos de negligência grosseira ou de incumprimento

deliberado do contrato para não mencionar os casos de fraude) deverão ser provados pelo prestador do serviço com base em elementos adicionais, relativamente aos registos informáticos do banco.”

*

II. Os movimentos em causa ocorreram pela colaboração da autora e da V em um esquema de engenharia social.

Conclui nesse sentido com base, de novo, no depoimento da testemunha P, já referido, conjugado com a descrição do acesso em geral ao *homebanking* feita no facto 47, e com as declarações de parte da autora das quais resultaria que era a única conhecedora das credenciais de acesso ao *homebanking*, tal como conhece os passos necessários para esse acesso.

Os autores respondem que: é evidente que não existiu qualquer colaboração da autora, que foi, sim, vítima de falta de cuidado grosseiro no tratamento dos seus dados pela V e das falhas de segurança na gestão da plataforma *homebanking*. A autora desconhece e não pode conhecer como alguém se poderia ter apropriado dos seus dados de acesso, porém tal apuramento não incumbe à autora; incumbe às autoridades policiais - sendo que, nesse mesmo dia a autora apresentou queixa-crime a qual continua a correr termos - e ao Banco, este na qualidade de proprietário e controlador da plataforma de *homebanking* com autorização para a respectiva utilização.

Apreciação:

A qualificação dos factos provados como um esquema de engenharia social não tem qualquer interesse. A parte da sentença dedicada aos factos não se destina a discutir a qualificação desses factos.

Quanto à afirmação de ter havido colaboração da autora com a V ou é uma simples qualificação dos factos provados, e então considera-se que ela é abusiva e sem qualquer base, ou é uma afirmação conclusiva que teria de ter na sua base factos que não foram alegados nem provados, pois que o facto, já referido, de os movimentos bancários em causa terem sido feitos com os dados/credenciais da autora, não permite a conclusão de que tenha sido a autora a fornecê-los a quem fez tais movimentos. A própria testemunha que o Banco invocou anteriormente dá outra hipótese para tal ter acontecido: pode ter ocorrido aquilo a que ela chama um roubo e que melhor se pode dizer ser uma subtracção de dados da autora, relativamente à qual o Banco não aponta qualquer prova de que tenha havido qualquer colaboração da autora (não servindo para o efeito a parte das declarações de parte que o Banco transcreveu). Quanto à fotografia do cartão matriz, ver-se-á à frente que não há qualquer prova de a autora a ter feito alguma vez ou de a ter no telemóvel.

*

III. A autora era a única conhecedora das credenciais de acesso ao

homebanking. IV. O sistema do Banco apenas é capaz de verificar se as coordenadas inseridas estão, ou não, correctas.

O Banco conclui nesse sentido com base no seguinte:

As declarações de parte da autora além de sustentarem os factos provados 39 a 47, 50 e 51 provam que a autora era a única conhecedora da *password* composta por seis dígitos da sua autoria e das coordenadas do cartão matriz. Ora, se o sistema do Banco não foi alvo de ataque informático, se os mecanismos de identificação e autenticação foram correctamente inseridos sem erro e se a autora era a única conhecedora desses elementos, desde logo a *password* e o cartão matriz, então recorrendo a regras da experiência comum e à lógica, conclui-se que terá sido a autora a facultar essa mesma informação a terceiros. Pelo que resulta provado que a autora violou as instruções de segurança que lhe foram cabalmente transmitidas pelo Banco [instruções que constam do facto 50]. Que a autora era a única pessoa conhecedora das credenciais de acesso ao *homebanking*, resultaria do depoimento da testemunha S, onde esclarece que nem o Banco sabe as credências, apenas dispõe dos meios técnicos para aferir se os códigos introduzidos estão correctos ou não (o Banco transcreve passagens onde a testemunha diz o que é explicado no momento da contratação do serviço a nível de segurança e de funcionamento do sistema e depois de como é que é feito o acesso ao *homebanking* e, finalmente e apenas, uma resposta confirmativa (“exactamente”) à pergunta se ‘o Banco não sabe qual é que é este o código? O Banco apenas consegue verificar se o código inserido é correto, ou não?’

Os autores respondem que a testemunha S não carregou qualquer facto com relevo para o caso dos autos, pois que é senso comum que o Banco não deve ser conhecedor dos dados de cartão matriz dos seus clientes, ainda que seja a sua entidade emitente; e é um mínimo de segurança que palavra passe, credenciais e códigos de acesso não sejam divulgados ou levados ao conhecimento de mais ninguém que o seu destinatário e utilizador final e que tal validação seja feita pelo *software* informático, sem intervenção de pessoas. Assim, o depoimento não trouxe qualquer dado relevante, limitando-se a declarar o procedimento de contratação bancária; tal procedimento, não só é de senso comum, a qualquer pessoa que haja celebrado contrato bancário, como já havia, aquando do início do julgamento, sido explicitado, com detalhe, nas declarações de parte da autora que se mostrou conhecedora e cumpridora de todos os procedimentos. Mais à frente, no entanto, os autores dizem: não se alcança como pode o Banco declarar que “o sistema apenas consegue verificar se as coordenadas inseridas se encontram correctamente inseridas ou não” pois que, em momento algum conseguiu produzir qualquer prova

neste sentido. A testemunha que alegadamente fez tal prova, não foi assim, a testemunha S [minuto 00:03:19] que é bancária em F e celebrou o contrato bancário com a autora.

Apreciação:

Continua-se perante simples pressupostos lógicos que o Banco tenta estabelecer para, a nível de facto, tentar concluir pela culpa da sua cliente apesar de não ter prova de factos positivos dessa culpa.

Volta-se ao que há pouco se afirmou: como não se sabe como é que o terceiro se apoderou das credenciais da autora (n.º do contrato, *password* e cartão matriz) não se pode dizer desde quando é que a autora deixou de ser a única conhecedora delas o que, como é lógico, teve que acontecer a dada altura.

Dito de outro modo: como não se sabe quando é que a pessoa que fez os movimentos bancários em causa nos autos ficou na posse das credenciais da autora e a afirmação que o Banco quer que se dê como provada não está localizada no tempo, não se pode dizer que “a autora era a única conhecedora das credenciais de acesso ao *homebanking*.” De resto, é uma evidência que quando foram feitos os movimentos, a autora não era a única conhecedora.

Quanto à afirmação de que “o sistema do Banco apenas é capaz de verificar se as coordenadas inseridas estão, ou não, correctas” faltava ao Banco esclarecer se se está a referir ao momento em que o sistema informático do Banco está a lidar com as movimentações bancárias em causa nos autos. Mas, mesmo assim estaria errado, pois que o sistema informático é capaz de verificar muitas outras coisas, como se vê na folha dos *logs*, doc.5, junto com a contestação. Assim, o máximo que se poderia dizer é que, no momento das movimentações bancárias em causa e quanto às credenciais que são utilizadas, o sistema informático do Banco limita-se a verificar se as credenciais utilizadas coincidem com aquelas que devem ser utilizadas. Mas isto não tem nenhum interesse para a questão dos autos, já resulta da lógica dos factos provados (19, 39 a 47 e 51) e não é a afirmação que o Banco quis que fosse aditada.

*

V. A autora tinha uma fotografia do cartão matriz guardada no seu telemóvel, incumprindo com as regras de segurança estabelecidas pelo Banco.

O Banco fundamenta isto com o depoimento da testemunha I de que a autora lhe tinha dito – enquanto estava a contar que tinha sido vítima de uma burla através de uma segunda via do cartão de telemóvel - que tinha uma fotografia do cartão-matriz no telemóvel.

Os autores respondem que: Não corresponde à verdade a alegação da existência de fotografias com o cartão matriz, pois que desde o primeiro momento do julgamento, nas declarações de parte da autora, esta foi clara e firme quanto ao total conhecimento dos procedimentos de segurança e não ter

qualquer fotografia da chave ou palavra passe no telemóvel, nem em qualquer dispositivo.

Apreciação:

Nas declarações de parte, a autora fala sobre a questão desde o minuto 17:58 ao minuto 19:08, dizendo que nunca tirou fotografias do cartão matriz, nem o digitalizou ou fotocopiou. A testemunha invocada pelo Banco foi ouvida depois da autora, o essencial do seu curto depoimento, de cerca de 8,30 minutos, versa sobre esta questão, de um modo que sugere que foi só isso que a testemunha veio dizer ao tribunal, e o mandatário do Banco não lhe pergunta nada sobre a evidente discrepância entre o seu depoimento e as declarações da autora. Acrescente-se que o depoimento da testemunha não está corroborado por qualquer elemento objectivo, como, por exemplo, uma nota tomada na hora e rubricada pela autora a confirmar que tinha dito isso, nem é invocado na contestação do Banco. Ou seja, temos um depoimento de uma testemunha trabalhadora do Banco a dizer uma coisa que cabia a este provar, depoimento sem qualquer suporte objectivo, o que o torna pouco credível, contraditado pelas declarações da autora que reforçam a dúvida que já dele resultava, pelo que a questão tem de ser decidida contra o Banco (art. 346 do CC).

*

VI. Após a autora tomar conhecimento da existência de movimentos não autorizados, cerca das 08:26 de dia 26/10/2018, na sua conta e até avisar o Banco do sucedido foram processados 4 movimentos não autorizados que totalizaram 4.949€.

A pretensão do Banco tem o seu fundamento na impugnação do facto 11, mais abaixo.

A resposta dos autores encontra-se no que dizem a propósito da impugnação dos factos 12, 13 e 11.

Apreciação:

Descontando as conclusões que o Banco quer retirar dos factos, ver-se-á na discussão que se fará mais à frente – principalmente através das declarações de parte da autora que o Banco transcreve, sem contradizer, para as aproveitar e que não há nenhuma razão para pôr em causa - que se pode realmente acrescentar/esclarecer/precisar, no facto 11, que a autora teve conhecimento de movimentos não autorizados por si pouco depois das 08:26, hora a que ela fez uma operação, e que depois disso foram feitos ainda vários movimentos constantes do facto 11-A. Esta discussão permite ainda perceber que nos factos provados há uma falha (não detectada pelo Banco): o Banco, no art. 79 da contestação, tinha feito uma enumeração e datação dos movimentos descritos no facto 11, que constam dos factos provados de 54 a 62, mas a

sentença esqueceu-se de dar a hora dos dois últimos movimentos que estavam no começo da página seguinte da contestação. De modo a suprir essa falta, esclarece-se a hora a que ocorreram esses dois movimentos (utilizando a mesma prova documental utilizada pela sentença para dar como provados os factos 54 a 62) mas, de modo a evitar a repetição de factos, aproveita-se o facto 11 para fazer constar dele a hora de cada movimento (subdividindo-o para melhor descrição dos factos) e eliminam-se os factos 54 a 62.

*

VII. A autora contactou o Banco às 09:24 horas de dia 26/10/2018 para dar ciência que tinha evidenciado movimentos na sua conta que não haviam sido feitos ou autorizados por si.

Também aqui esta pretensão do Banco tem a sua fundamentação na discussão dos factos 12, 13 e 11.

Os autores respondem, para além do que dizem a propósito de 12, 13 e 11, que:

Após detectar os movimentos, a autora, aflita, encerrou as plataformas que estava a usar, *homebanking* e redacção de sumários escolares, correu e pediu ajuda às testemunhas que encontrou, nomeadamente, testemunha A que inclusivamente procurou perceber o que se passaria com o telemóvel e procurou colocá-lo a funcionar até ter percebido que algo de errado acontecia e posteriormente, foi ao PBX falar com o Banco onde obteve o inócuo apoio declarado pela testemunha L. A verdade é que ainda com toda a comoção e estado de pânico e desespero em que se encontrava, a autora pediu socorro aos colegas com os quais se cruzou na escola e, ainda neste local, pediu de imediato apoio do Banco.

Apreciação:

O Banco refere-se ao contacto já constante do facto 12 que, se se esclarecer que é o mesmo que está em causa nos factos 52 e 63, já se sabe ter sido realizado às 09:24. Como de outro modo não se sabe isso e como foi isso que aconteceu, é importante esse aditamento no facto 12.

Mas, como decorre da discussão abaixo (facto 11), das declarações de parte não decorre só isso; a autora diz – nas transcrições ali feitas pelo próprio Banco que as invoca e não contradiz – ter feito várias tentativas para o efeito e que só à terceira é que foi atendida e lhe foi dado um número para ligar para Lisboa, com o qual acabou por fazer a chamada registada e referida nos factos 52 e 63, cuja anotação só terminou às 09:41 (sendo de notar que os movimentos que estão registadas como desconhecidos pelo cliente vão até ao de 1.950€ feito às 08:38, o que aponta para que a autora tenha estado *online* até essa hora – tudo conforme documento 18 junto com a contestação do Banco). Pelo que tudo isto também tem de ser acrescentado nos factos

provados.

*

O Banco entende que não deviam ter sido dados como provados os factos 12 e 13 [na parte que importa, do facto 12 consta que a autora contactou imediatamente o Banco (depois de ter detectados os movimentos em causa e que foi aconselhada a ir à PSP apresentar queixa-crime), sendo que no facto 13 consta que assim fez - doc. 8 que é a participação à PSP]]

A pretensão do Banco fundamenta-se, segundo ele, na prova já transcrita, quer testemunhal quer documental, dela retirando que a autora não contactou imediatamente o Banco, mas sim apenas uma hora depois de ter conhecimento dos movimentos e que tal importa[ria] para uma rápida actuação do Banco para impedir que mais movimentos ocorr[esse]m, conforme teria sido esclarecido pelo depoimento da testemunha L falando sobre o documento 18 (referido no facto 63).

Os autores respondem que:

A testemunha C referiu (em passagens do depoimento que transcrevem) não ter certeza da hora, que a autora estava de saída e que já havia pedido ajuda a outros transeuntes na escola, nomeadamente, à testemunha A que trabalha com informática na escola e que havia tentado perceber e reiniciar o telemóvel para tentar recuperar a cobertura de rede, só após alguns testes, esta testemunha que, reitere-se, trabalha na sala de informática da escola, constatou que o que se passava com o telemóvel da autora não era normal, pois ela havia ido a locais onde habitualmente há cobertura de rede e não se justificava que o telemóvel não funcionasse. E depois fazem várias considerações sobre a forma como a autora gastou o seu tempo, com base nos factos que já estão provados, e criticam o Banco por aventar que a autora demorou a agir, sendo que, numa situação destas não faz sequer o menor sentido que um singelo contacto não tenha resolvido de imediato a situação e congelado a conta a fim de que nenhum montante fosse retirado e que se tentasse e pudesse reverter as operações eventualmente ordenadas e não concretizadas.

Apreciação:

Apesar da insistência do Banco em considerar não provados os factos 12 e 13, a argumentação dele apenas aponta no sentido de a comunicação dos factos não ter sido imediata. Ou seja, apenas a palavra imediata é que teria de ser retirada do facto 12, sendo despropositada a pretensão do Banco em eliminar totalmente os factos 12 e 13, referindo-se ao facto 13 como se ele dissesse o mesmo que o facto 12, o que não tem qualquer razão de ser. Para além disso, o Banco faz considerações de Direito com base neste facto, considerações de Direito que não têm qualquer interesse para esta questão de facto.

Limitada assim a pretensão do Banco, ela deve ser julgada procedente: sabendo-se apenas que a autora fez um movimento às 08:26, que teve conhecimento dos movimentos não autorizados pouco depois e acabou por conseguir fazer a participação às 09:24, não se pode utilizar a expressão imediatamente. Isto sem prejuízo daquilo que já foi acrescentado por outras razões.

*

O Banco entende que não devia ter sido dado com provado o facto 29 [que consta, lembre-se, do seguinte: “Esses terceiros conseguiram ainda aceder aos dados pessoais e bancários dos autores, através da sua página “*homebanking*” acima referida, disponibilizada aos autores pelo Banco.”]

Isto com base nos depoimentos transcritos já transcritos das testemunhas P e S: o sistema do banco não foi alvo de qualquer ataque informático e o sistema apenas consegue verificar se as coordenadas inseridas se encontram correctamente inseridas ou não.

Os autores respondem que não entendem como é que o facto 29 se pode considerar não provado se, em face dos factos verificados e comprovados, quer por documento, quer por testemunhas, é evidente que terceiros tiveram acesso aos dados; aliás, estes terceiros tiveram acesso a ponto de inclusivamente terem logrado obter o n.º de telemóvel associado à conta, do qual pediram, a segunda via cartão.

Apreciação:

A pretensão do Banco tem evidente razão de ser, mas não com base nas suas alegações, sendo evidente, por outro lado, que os autores não têm razão nas contra-alegações, não havendo qualquer prova de que o número de telemóvel tenha sido obtido através dos dados associados à conta (nem há prova do contrário). O que se passa é que é, realmente, evidente, por uma questão de simples lógica, que o acesso ao *homebanking* da autora não permitia aceder aos dados da autora que tiveram que ser introduzidos para aceder ao *homebanking* (o n.º do contrato e o *password*) e fazer depois operações nele: as coordenadas no cartão matriz e o código fornecido pelo SMS.

O facto 29 tem, por isso, de ser eliminado.

*

O Banco entende que se impõe uma correcção ao facto provado sob 11 [neste facto, lembre-se, diz-se, agora em síntese, que no dia 26 a autora acedeu à sua conta e foi surpreendida com todos os movimentos em causa nos autos]:

Diz que devia ter sido dado como provado que no dia 26/10/2018, cerca das 08:26 da manhã, a autora acedeu à sua conta bancária através da *internet* e do portal N24, para fazer um pagamento e constatou que haviam sido feitos entre o dia 25 e o dia 26/10 três movimentos (pagamentos de serviços) com

saída de património detido pelos autores no Banco (de 1.969,50€ + 1.969,50€ + de 1.010€ [o Banco volta a incorrer no lapso de escrever 1.810 quando o valor certo é o referido]).

Isto é, o facto 11 devia incluir a hora que a autora teve conhecimento da ocorrência de movimentos na sua conta e a que horas deu conhecimento ao seu banco [...], sendo que tal resultaria das declarações de parte da autora. O Banco transcreve a seguir uma extensa série de passagens das declarações de parte da autora, sendo que aquelas que têm relevância para o que já se disse acima são as seguintes:

Autora: [00:09:11] [...] tentei ligar imediatamente para o número do Banco que eu tinha. Acontece que o meu telefone estava sem... pronto, eu não conseguia fazer... não conseguia fazer chamadas. Â... vim para o P.B.X. da escola, que foi através do P.B.X. da escola que eu contactei â... â... as agências do Banco, penso que foi à terceira tentativa que eu consegui que alguém me atendesse, expliquei a situação, disse o que é que estava a acontecer, foi-me dado um número para eu ligar para Lisboa, foi o que eu fiz, liguei esse número, fui extremamente bem atendida â... â... em Lisboa, disseram-me tudo aquilo que eu tinha que fazer, e o que eu tinha que fazer é ir imediatamente à polícia.

[...]

Autora: [00:12:20] eu penso que devo ter ligado [o computador – parenteses deste TRL] por volta das 08:20, por aí, talvez.

Juíza: E fez primeiro a transferência, e depois é que foi ver os movimentos para trás, foi isso?

Autora: [00:12:28]. Exactamente, sim. Primeiro fiz os meus sumários, e depois é que abri o site do Banco para fazer a transferência, sim.

[...]

Mandatário do Banco: Muito bem. Depois fez então o movimento dos 12€...

Autora: [00:19:45] Sim.

[...]

Mandatário do Banco: E só depois é que reparou que existiam transferências.

Autora: [00:19:52] reparei porque voltei atrás, e entrei na minha conta à ordem para ver. Porque eu faço sempre esse procedimento. Sempre. Sempre. Sempre.

Mandatário do Banco: E isto por volta das 08:20, 08:25, correto?

Autora: [00:20:03] [ininteligível] Sim. Por aí. Sim. Já não sei precisar. Mais minuto, menos minuto, não é? Já não sei.

A seguir o Banco diz que conjugando as declarações de parte da autora com o extracto de conta [doc.3 junto com a contestação do Banco] e os detalhes de cada movimento em causa [docs.7 a 17 juntos com a contestação do Banco]

verifica-se aquilo que o Banco quer provar nesta pretensão, que é aquilo que já foi determinado acima ser aditado, precisando o que consta dos factos 11 e 11-A.

Depois passa a invocar passagens do depoimento da testemunha C do qual resultaria que o contacto com o Banco só teria ocorrido às 09:34 [é erro do Banco, que quer escrever 09:24] e mais outras passagens do depoimento da sua testemunha L que esclareceu o teor do doc.18 junto com a contestação do Banco e do qual resultaria o mesmo, ou seja, chamada, a dar conta dos movimentos não autorizados / pedido de cancelamento, só às 09:24.

Os autores respondem, para além do que já tinham dito a outros propósitos, designadamente sobre o depoimento da testemunha C, que:

A testemunha L, mais uma testemunha do banco, não soube acrescentar nada em concreto sobre os factos, apenas se cinge a indicar procedimentos em abstracto, tendo declarado que *[os autores transcrevem a seguir passagens que já tinham sido transcritas pelo Banco e depois fazem comentários sobre elas que não têm relevo para a discussão de facto]*.

Apreciação:

A autora acedeu ao *homebanking* por volta das 08:26. Mas isso não quer dizer que tenha ido logo ver os movimentos feitos. Pelo que o que se pode dar como provado são apenas os movimentos que foram feitos até essa hora e os que foram feitos depois dessa hora. Mas esta separação já foi feita acima, com um resultado mais perfeito do que o pretendido pelo Banco, pois que não interessam apenas os movimentos de saída, mas os outros movimentos referidos no facto 11 que foram feitos para permitir esses movimentos de saída.

Esta impugnação do Banco também tinha a ver com as horas a que a autora fez a chamada a denunciar os movimentos e a fazer o pedido de cancelamento, isto é com outras pretensões de aditamento de factos e já foi tomada em consideração para o efeito, como decorre do que antecede.

*

O Banco entende que se impõe uma correcção aos factos provados sob 30 e 71 [nestes dois factos, na parte que importa, diz-se que no dia 23/08/2019 foi creditado na conta dos autores o valor de 1.950€, a título de reembolso efectuado pelo Banco de um dos referidos pagamentos]:

A fundamentação para isto é a seguinte: Efectivamente, corresponde à verdade que o Banco no dia 23/08/2019 creditou na conta da autora a quantia de 1.950€ [cf. doc.10 junto com a PI], o que fez no âmbito das diligências que levou a cabo após a comunicação pela autora que não tinha autorizado os movimentos. Mas tal não corresponde a um reembolso, mas ao resultado das diligências de reocupação de verbas levadas a cabo pelo Banco. Invoca o

depoimento da testemunha S para falar sobre essas diligências do Banco e para concluir – o que já resulta da condenação da sentença - que após as diligências do Banco o montante dos movimentos não autorizados se fixava nos 7.949€ e não no valor peticionado pelos autores.

Os autores não respondem nada quanto a isto.

Apreciação:

Os pormenores não interessam e o doc.10, dado objectivo que tem relevo, não diz o que o Banco pretende, mas também não diz precisamente o que consta dos factos provados sob 30 e 71. O que é possível e relevante dizer, sobre o assunto, em substituição de 30 e 71 é que:

30 e 71. Em 23/08/2019 foram, em virtude da actuação do Banco, creditados na conta dos autores 1.950€ relativamente a um dos movimentos denunciados.

*

O Banco, no corpo das alegações, defende ainda não ter sido produzida qualquer prova que sustente os factos provados sob 32 e 33.

Os factos 32 e 33 não constam como impugnados nas conclusões do recurso, pelo que não há que ter em conta esta impugnação (art. 639/1 do CPC).

Não interessa, por isso, a resposta que os autores deram a isto nas contra-alegações. Para além disso, os autores não impugnaram a absolvição do Banco do pedido de indemnização por danos morais, pelo que, também por aqui, não interessa a apreciação dos factos provados 32 e 33.

*

Nas conclusões L a FF do seu recurso, o Banco, para além de repetir considerações quanto à actuação da autora, já apreciadas, diz que:

Para que os movimentos em causa se verificassem foi necessária e indispensável a actuação da V, Na medida em que para validar as operações em causa, conforme facto 47, terceiros, de identidade desconhecida, obtiveram dos serviços da V uma 2.ª via do cartão SIM da autora.

A V não dispõe de procedimentos adequados a prevenir este *modus operandi* de apropriação ilegítima de quantias na medida em que, por telefone, através da sua linha de apoio ao cliente, e mediante a confirmação de 2 dados tão simples como nome e morada de facturação qualquer pessoa consegue obter uma 2.ª via do cartão SIM de outra.

A testemunha J, técnico da área de fraude, demonstrou que a V é conhecedora dos SMS que contêm *tokens* bancários e que este tipo de situações [substituições de cartão SIM estão associados a esquemas de *phishing*] levou à instituição de um procedimento para prevenção de tais ocorrências, mas claramente insuficientes, na medida em que, sem atestar a identidade da pessoa, à semelhança do que esclareceu ser feito em loja, emitiu uma 2.ª via do cartão SIM que viabilizou os movimentos em causa.

Contudo, resulta do doc.3 junto com a contestação da V, o Banco remeteu para o número de telemóvel da autora os *tokens* bancários associados a cada movimento, que apenas não chegaram à sua posse, não por facto imputável ao Banco, mas à V que permitiu que terceiros obtivessem uma segunda via do cartão SIM.

Pelo que a V foi parte imprescindível na concretização deste esquema de engenharia social.

Apreciação:

Daqui não decorre a invocação, pelo Banco, de qualquer ponto da matéria de facto que estivesse mal decidido. Ou melhor, não decorre a impugnação de qualquer decisão da matéria de facto. Pelo que, a este nível, nada há a decidir.

Quanto à parte de Direito, desta matéria não decorre qualquer colaboração da autora com a actuação da V, pelo que é irrelevante no sentido de provar que a autora actuou fraudulentamente, ou que incumpriu, deliberadamente ou com negligência grave, obrigações de cuidado, pelo que é irrelevante no sentido de evitar a condenação do Banco. E, não tendo nada a ver com a actuação da autora, é irrelevante se a actuação da V contribuiu para os factos em causa nos autos, já que o Banco não se pode eximir da sua responsabilidade para com a autora pelo facto de terceiro/V, sem nada a ver com a autora, ter contribuído para os movimentos bancários ilícitos.

Pelo que, toda a discussão relativa a esta parte do recurso é irrelevante.

Dito de outro modo, este acórdão não vai discutir a responsabilidade da V pois que é evidente que não se prova qualquer facto que permita a conclusão da colaboração da V com a/os autora/es e a eventual responsabilidade da V não afastaria a responsabilidade do Banco perante os autores. O Banco pode querer e pode ter razões para responsabilizar a V, mas não o pretendeu fazer nesta acção, nem neste recurso, designadamente não recorreu quanto à absolvição da V do pedido, nem defendeu a condenação isolada da V a favor dos autores, ou que a V fosse condenada solidariamente consigo a pagar a indemnização aos autores.

*

Do recurso sobre matéria de Direito

No caso dos autos e na parte que ainda importa está só em causa a alegada responsabilidade do Banco – prestador de um serviço de pagamento – por operações de pagamento não autorizadas pelo aparente ordenante/utilizador/cliente do serviço de pagamento, no âmbito de um contrato de prestação de serviços de banca ao domicílio (*homebanking*).

Não interessa, por isso, o regime do art. 796 do CC, que regula a “questão jurídico-real” da distribuição do risco do perecimento ou deterioração da coisa

por causa não imputável ao alienante nos contratos que importem a transferência do domínio sobre certa coisa ou que constituam ou transfiram um direito real sobre ela (neste sentido, Raquel Guimarães, obra citada, páginas 28-29, a autora da expressão entre aspas, e Francisco Mendes Correia, obra citada, pág. 724, nota 34, que lembra que o artigo 796 se refere ao risco de perecimento de coisas determinadas o que não é o caso de fundos bancários), possa embora o resultado alcançado ser o mesmo. Interessam ao caso, sim, os artigos 70 a 72 do anexo I ao DL 317/2009, de 30/10, alterado pelo DL 242/2012, que era o regime em vigor à data dos factos e por isso o aplicável.

Esses artigos têm o seguinte teor:

Artigo 70.º - Prova de autenticação e execução das operações de pagamento

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

2 - Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, por si só, não é necessariamente suficiente para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 67.º

Artigo 71.º - Responsabilidade do prestador do serviço de pagamento por operações de pagamento não autorizadas

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

2 - Sempre que o ordenante não seja imediatamente reembolsado pelo respectivo prestador de serviços de pagamento nos termos do número anterior, são devidos juros moratórios, contados dia a dia desde a data em que o utilizador de serviços de pagamento haja negado ter autorizado a operação de pagamento executada, até à data do reembolso efectivo, calculados à taxa legal, fixada nos termos do Código Civil, acrescida de 10 pontos percentuais, sem prejuízo do direito à indemnização suplementar a que haja lugar.

Artigo 72.º Responsabilidade do ordenante por operações de pagamento não autorizadas

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

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

3 - Havendo negligência grave do ordenante, este suporta as perdas resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, ainda que superiores a (euro) 150, dependendo da natureza dos dispositivos de segurança personalizados do instrumento de pagamento e das circunstâncias da sua perda, roubo ou apropriação abusiva.

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

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

Portanto, se um utilizador de serviços de pagamento (o cliente) – sendo o serviço em causa, no caso, o *homebanking* – nega ter autorizado uma operação de pagamento executada pelo prestador de serviço (o Banco), é o Banco que tem de fornecer prova de que a operação de pagamento foi autorizada pelo utilizador ou que este agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações associadas a esse instrumento de pagamento. E para o efeito não basta, em princípio, ao prestador provar a utilização do instrumento de pagamento pelo cliente – nem, por maioria de razão, que foram utilizados os dados do cliente. Se não conseguir fornecer aquela prova, o prestador deve reembolsar imediatamente o utilizador do montante dessa operação de pagamento e repor a conta de pagamento debitada na situação em que estaria

se a operação de pagamento não autorizada não tivesse sido executada, com juros moratórios, contados dia a dia desde a data em que o utilizador de serviços de pagamento haja negado ter autorizado a operação de pagamento executada, até à data do reembolso efectivo (à taxa legal acrescida de 10 pontos percentuais, sem prejuízo do direito à indemnização suplementar a que haja lugar).

Perante este regime, Bruno Silva Palhão conclui: “O ónus da prova é, portanto, do PSP [prestador do serviço de pagamento], que não o pode atenuar. Trata-se de um desvio ao regime geral e, apresenta-se como mais favorável ao utilizador. Acresce ainda que o registo da utilização do *homebanking*, ou dos códigos de acesso, não é necessariamente suficiente para provar a autorização, a existência de fraude ou a inobservância de obrigações por parte do utilizador. Em suma, e como regra geral, caberá ao PSP provar o grau de culpa do utilizador, titular do instrumento de pagamento, e a sua contribuição para os prejuízos ocorridos.” (Os serviços de pagamento e as operações não autorizadas – Cadernos de Direito Privado, n.º 65, Jan/Mar 2019, Cejur, pág.11.

Em nota (78) na mesma página acrescenta: “[...] Salvo melhor opinião, deve entender-se que uma operação ser ordenada com recurso aos códigos pessoais e intransmissíveis do utilizador não é suficiente para operação qualquer presunção, já que a fraude informática tem como efeito prático a obtenção dos ditos códigos e o operar de tal presunção obrigaria o utilizador a fazer prova de factos relacionados com sistemas informáticos que não domina.”

Miguel Pestana de Vasconcelos, por sua vez, diz, embora escrevendo sobre o novo RSP (o de 2018, que, nos pontos agora em causa não é diferente): “[...] Para afastar a sua responsabilidade, o prestador de serviços terá de apresentar elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento [...]. A imposição ao prestador de serviços de apresentar provas da alegada negligência resulta do facto de, como se refere na DSP 2 [Directiva de Serviços de Pagamento] (considerando 72), o ordenante apenas dispor de meios muito limitados para o efeito.

Trata-se de uma carga probatória muito pesada. Ou o prestador de serviços consegue demonstrar a existência de uma fraude, recorrendo aos meios técnicos à sua disposição para o efeito, onde se incluem evidentemente aqueles destinados a esse fim, ou então terá de demonstrar o dolo ou negligência grosseira. Note-se, conforme já se sublinhou, que não basta negligência simples (ou culpa leve), é preciso negligência grosseira, o que significa uma falta de cuidado extremamente grave, que só uma pessoa muito pouco cuidadosa teria. Mas não será fácil ao prestador fazer a prova.” [A

responsabilidade do banco por operações de pagamento não autorizadas no *online banking*, decorrente do novo serviços de pagamento (RSP II), Julgar, 42, Set/Dez 2020, Almedina, páginas 204-205].

Francisco Mendes Correia, numa análise mais demorada do regime das operações não autorizadas e que aqui se vai referir numa síntese curta, esclarece que o art. 70/1 do RSP é “[...] uma regra de ónus da prova objectivo, visando permitir uma decisão nos casos de operações não autorizadas”.

Estabelece “uma presunção de ilicitude a favor do utilizador”, identificando “os factos que devem ser provados pelo prestador para a afastar: a correcta autenticação, registo e contabilização da ordem, bem como a inexistência de avaria técnica ou qualquer deficiência.” O Banco tem pois de demonstrar “que a ordem de pagamento foi recebida após uma autenticação regular, que a operação foi devidamente registada e contabilizada e que os sistemas técnicos não foram, naquela ocasião, afectados por uma avaria técnica ou por outra deficiência de outra natureza.” Depois, “como norma suplementar deste regime especial”, existe “o art. 70/2 do” RSP: “ainda que o prestador de serviços consiga demonstrar” tudo aquilo, “e, além disso, prove que foi utilizado o sistema de pagamento registado pelo utilizador, essa demonstração não é suficiente para dissipar a situação de incerteza quanto à factualidade subjacente à operação não autorizada. Nestes casos, a demonstração da utilização do instrumento de pagamento – e, com esta referência tem-se obviamente por incluídos todos os protocolos e dados de autenticação -, não é suficiente para ‘provar que a operação foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações.’ E conclui: “A norma em apreço não permite que a situação de incerteza se resolva com uma sobrevalorização do facto de a operação ter sido iniciada na sequência da utilização dos dispositivos e procedimentos de segurança e autenticação contratados com o cliente, permitindo então que subsista a incerteza quanto à eventual intervenção de terceiro.” (Operações não autorizadas e o regime jurídico dos serviços de pagamento e da moeda electrónica, RDC, 2017, 3, Almedina, páginas 721-724).

Este autor, a propósito do que antecede, lembra que, num sentido equiparável, o acórdão do TRL de 24/05/2012, proc. [192119/11.8YIPRT.L1-2](#), declarou a nulidade de uma cláusula das condições gerais utilizadas por um banco, nos termos da qual se presumia “que as operações realizadas com a inserção dos elementos de segurança pessoais e intransmissíveis do subscritor do serviço são da autoria do subscritor do serviço” e que havia consentimento ou disponibilização culposa a terceiro, quando se demonstrasse “que as operações (transferências) realizadas foram efectuadas por terceiros.”

Este pesado regime probatório - “a responsabilidade do banco é [...] excepcionalmente intensa” - não é fruto de um acaso, mas é intencional pois, como refere Pestana de Vasconcelos (obra citada, pág. 209, que é o autor da frase entre aspas), “o objectivo é claro: dado o relevo central dos sistemas de pagamentos na vida moderna e fonte crescente de rendimentos que os prestadores de serviços deles retiram, visa-se estabelecer uma protecção máxima dos titulares das contas.” O autor está-se a referir especificamente ao DSP 2, mas este, nas normas citadas, não difere, no essencial, do anterior.

*

Posto isto,

No caso dos autos, o que se apurou, em síntese, foi apenas o seguinte: alguém que não a cliente do Banco utilizou as credenciais da autora (cliente), tendo-as obtido não se sabe como (excepto um dos dados, o SMS bancário com o código - este sabe-se como é que foi obtido), para, através do *homebanking*, aceder à conta desta no Banco e com ela fazer operações de pagamento de bens que ele, terceiro, estava a comprar. Isto corresponde a dizer, noutra perspectiva, que o Banco não conseguiu provar que essas operações de pagamento foram autorizadas pelo utilizador/cliente. Assim sendo, o Banco só poderia afastar a sua responsabilidade por esta sua conduta presumidamente ilícita - já que debitou a conta da autora por ordens de quem não tinha legitimidade para o fazer - perante a cliente, se conseguisse provar que a utilização das credenciais por terceiro se deveu ou tornou possível graças a um comportamento deliberado ou gravemente negligente da autora. O que, perante a síntese do que se passou, feita acima, se tem de concluir que não conseguiu fazer.

Logo, o Banco devia ter reembolsado a autora do montante das operações de pagamento não autorizadas, imediatamente depois de esta lhe ter dado conhecimento que negava ter dado a autorização daquelas operações e, não o tendo feito, o Banco devia ter sido condenado a fazê-lo, e ainda devia ter sido condenado a repor a conta da autora na situação em que estaria se essas operações de pagamento não tivessem sido executadas, com juros moratórios contados dia a dia desde então e até efectivo reembolso, calculados à taxa legal civil acrescida de 10 pontos percentuais, para além de outra indemnização suplementar a que houvesse lugar, sem qualquer “franquia” por nem a negligência leve da autora o Banco ter provado.

Todas estas condenações estava sujeitas a terem sido pedidas (art. 609/1 do CPC) ou de ter havido recurso quanto ao facto de não terem sido concedidas (art. 635/5 do CPC), e daí que se compreenda o alcance limitado da sentença (por exemplo, quanto aos juros) e a sua confirmação por este acórdão.

Como foi isto que a sentença recorrida decidiu, no essencial com a mesma

fundamentação, conclui-se que em princípio a sentença deve ser confirmada. No entanto, o Banco quer a sua revogação, com base no seguinte, a que se responde a seguir a cada um dos argumentos constantes das conclusões assinaladas:

- Nas conclusões GG a I, diz que o momento da recepção de uma ordem de pagamento deve coincidir com o momento da sua execução, não podendo o prestador de serviços de pagamento recusar-se a executar as ordens correctamente inseridas, sem causa justificativa; não se evidenciando qualquer indício de fraude nos movimentos em causa nos autos, o Banco estava obrigado a concretizá-los.

Isto só seria assim se o Banco tivesse feito prova da autenticidade das ordens de transferência e de pagamento em causa.

- Nas conclusões JJ e RR, diz, por duas vezes, que a autora incumpriu com as normas de segurança ao dispor de uma fotografia do cartão matriz guardada no seu telemóvel, e na conclusão MM diz que a autora transmitiu as suas credenciais a terceiros.

Como se viu, não está minimamente provada nenhuma destas afirmações.

- Nas conclusões KK a OO, o Banco diz que encaminhou correctamente as mensagens com os *tokens* bancários para o telemóvel da autora; foi a V que não as entregou à autora mas a terceiro a quem permitiu a obtenção de uma via do cartão Sim da autora; pelo que há um incumprimento contratual por parte da V, responsável pelos danos causados aos autores.

Já se viu que a eventual responsabilidade da V – sem prova de que os autores lhe tivessem dado qualquer colaboração - não afastaria a responsabilidade do Banco para com os autores e é só isto que se discute neste recurso.

Nas conclusões PP e OO, o Banco diz que não concorda com o Tribunal *a quo* quanto [ao que ele disse relativamente] ao ónus da prova, pois provado que está o correto funcionamento do sistema, os mecanismos necessários para autenticar uma operação, o exclusivo conhecimento de tais credenciais pela autora, a inexistência de ataques informáticos no seu sistema e o cabal cumprimento dos seus deveres de informação pré-contratual e contratual [, não se pode] entender que [o Banco] não logrou em ilidir a presunção de culpa.”

Já se viu que o Banco não ilidiu a presunção de ilicitude da sua conduta, nem o poderia fazer apenas do modo como o tentou fazer neste recurso, com base em supostas presunções baseadas em regras da lógica ou da experiência comum das coisas.

- Por fim, na conclusão SS, o Banco diz que o disposto nos artigos 67/1-b e 72/4 do [RSP anexo ao] DL 317/2009 (*a contrario sensu*) determina a responsabilidade da autora pelos movimentos ocorridos após ter tomado

conhecimento da existência de movimentos não autorizados na sua conta e o momento em que informa o seu banco.

O Banco está a utilizar o art. 72/4 do RSP sem razão: o que a norma diz é que, nas hipóteses em que o cliente deve responder, em medida sucessivamente menos grave, pelas operações não autorizadas, por ter actuado (4) fraudulentamente, ou com incumprimento (3) deliberado ou (2) gravemente negligente, ou mesmo com (1) negligência leve, deixaria de ter de responder a partir da notificação ali prevista. Ora, como não se provaram quaisquer factos que permitam a imputação à autora ou aos autores de qualquer responsabilidade, a questão da aplicação do art. 72/4 do RSP não se coloca. De qualquer modo, diga-se que, tendo-se apenas apurado que a autora deu conta de movimentos não autorizados cerca das 08:26, não se sabe precisamente quando (mas provavelmente só às 08:38), e que, antes das 09:24, tentou contactar, por três vezes, com o Banco até ser atendida à terceira vez, para ser então remetida para o número onde conseguiu, finalmente, fazer a notificação às 09:24, o que quer dizer que a tentou começar a fazer bem antes, embora não se saiba quando, não é possível dizer, com o mínimo de precisão, qual o período de tempo que mediou entre esses momentos, mas apenas que, no máximo terá sido de uma hora, mas que poderá ter sido de apenas 15 ou 30 minutos, e, por isso não é possível censurar a autora por essa dilação, para mais sabendo-se que os movimentos não autorizados foram feitos de um modo que levou a que a autora tivesse deixado de ter acesso a chamadas pelo seu telemóvel sem que a autora se tivesse percebido de imediato que tal situação derivava disso. Mais ainda: visto que o Banco, só para receber/anotar a notificação levou 17 minutos sem demonstrar ter feito alguma coisa nesse período para impedir novos movimentos, não se vê que possa censurar a autora por ter demorado a reagir por um período de tempo que pode ser igual àquele que ele levou a anotar a notificação feita pela autora. Mas tudo isto, já se viu, nem sequer tem interesse no caso dos autos porque, como se disse, no caso, perante os factos provados, nem sequer é de aplicar a norma do art. 72/4 do RSP.

Em suma, improcedem todos os argumentos do Banco contra a sentença recorrida que, por isso, e sem mais, deve ser confirmada.

Note-se que é também isto que tem acontecido em quase todos os casos analisados em acórdãos publicados (sendo inúmeros aqueles que estão referidos nos quatro estudos acima citados, que os analisam e por isso não se vão repetir aqui as referências aos mesmos), sendo que os poucos casos em que tal não aconteceu correspondem a situações que nada têm a ver com o caso dos autos. Daí que o Banco não tenha invocado um único acórdão ou estudo doutrinário que sustente a construção feito por ele nas alegações de

recurso.

*

Pelo exposto, julga-se o recurso improcedente.

Custas, na vertente de custas de parte, pelo Banco (por ter perdido o recurso).

Lisboa, 15/12/2022

Pedro Martins

Inês Moura

Laurinda Gemas