TRIBUNAL DA RELAÇÃO DE LISBOA | CÍVEL

Acórdão

Processo	Data do documento	Relator
19530/17.9T8LSB.L-8	1 de outubro de 2020	Maria Amélia Ameixoeira

DESCRITORES

Contrato de conta bancária > Homebanking > Phishing > Negligência da vítima > Responsabilidade bancária

---

SUMÁRIO

I) Tendo-se apurado que as transferências “sub judice” foram efectuadas fraudulentamente por terceiros, com recurso à técnica conhecida por phishing, logo se conclui que as mesmas não ocorreram por uma qualquer avaria ou deficiência do sistema informático da Ré/BANCO , como defende a Autora . E,

II) Resultando provado que a utilização do serviço homebanking por banda da autora, se produziu com total desrespeito pela mesma das condições acordadas, maxime no que concerne às que se reportam à segurança , designadamente em sede de transmissão da totalidade dos dados do seu cartão matriz a terceiros, temos assim que ,

III) Acaba em última análise a Ré/BANCO por provar a culpa da Autora e o seu incumprimento do contrato de homebanking - por violação das mais elementares regras de segurança impostas pelo mesmo - , logrando ilidir a presunção de culpa prevista no art. 799º nº 1 do Código Civil, que sobre si impendia, pelo que não é responsável pela movimentação das contas bancárias de forma fraudulenta.

TEXTO INTEGRAL

Acordam os Juízes da 8ª Secção do Tribunal da Relação de Lisboa

RELATÓRIO:

A [ERCÍLIA ....] , casada no regime de separação de bens com B [Manuel ....] , residente na Rua ....., Zambujal, 2970-128 em Sesimbra, NIF 124 743 293, veio instaurar

AÇÃO DECLARATIVA COMUM, contra:

C [CAIXA .....] , com os sinais nos autos.

Pedindo a condenação da Ré Caixa a pagar-lhe a quantia de 26.630,24 Euros (vinte e seis mil seiscentos e

trinta euros e nove cêntimos) acrescida de juros moratórios vincendos até integral pagamento.

Alegando para o efeito, que, no âmbito do contrato de depósito bancário, previamente existente, a A. aderiu ao serviço "NET 24" da R. e que, em 04 de Janeiro de 2017, ao dirigir-se à agência do Banco Réu no Cartaxo, foi informada da existência de elevadas movimentações nas suas contas, através do NET BANCO, designadamente ocorridas entre 28 de Dezembro de 2016 a 4 de Janeiro de 2017, não autorizadas, no valor de 26.630,24 Euros, sendo vítima de Burla Informática, sabendo que tais movimentos não haviam sido por si efectuadas, de imediato a A. comunicou com os serviços da R.

Citada, contestou a Ré Caixa, alegando, por um lado, a ilegitimidade da Autora e, por outro, em síntese, que ocorreu por mera negligência, por terem sido fornecidas todas as credenciais de acesso ao serviço a terceiro que levou à concretização da operação.

*

Procedeu-se à discussão da causa.

Foi proferida sentença, com o teor seguinte que julgou a acção procedente, por provada, e, em consequência, condenou a Ré Caixa a pagar à Autora a quantia de 26.630,24 Euros (vinte e seis mil seiscentos e trinta euros e nove cêntimos) acrescida de juros moratórios vincendos até integral pagamento.

*

Inconformada com o teor da sentença, veio a Ré Caixa Económica Montepio Geral interpor recurso, concluindo da forma seguinte:

II.I) DA NULIDADE DA SENTENÇA RECORRIDA

1. A conta depósitos à ordem n.º 168.10.005058 - 7 e conta depósitos a prazo associada, n.º 168.15.011897 – 9. são co tituladas pela A., mãe e irmã, conforme documento n.º 1 junto com a contestação.

2. A A. porém apresentou a presente ação, desacompanhado das restantes cotitulares das contas.

3. Nos termos do art 516.º do CC e 28.º e 28.º-A n.º 1 do CPC a presente ação teria de ser proposta por todos os titulares da conta, ou por um, com consentimento dos outros (em sua representação), na medida em que estamos perante uma situação de litisconsórcio necessário ativo, o que a ora recorrente alegou em sede de contestação,

4. Invocando que a falta de intervenção necessária dos cotitulares das contas em questão era motivo de ilegitimidade, o que constitui uma exceção dilatória e como tal, uma deficiência do processo que obsta a que o tribunal conheça do mérito da causa.

5. Em face do exposto a A. requereu a intervenção principal das demais cotitulares da conta.

6. Cuja citação foi ordenada e concretizada nos autos.

7. Porem, no capítulo V da sentença, reservado à Decisão, o Tribunal recorrido julgou a ação procedente condenando a Ré C a pagar exclusivamente à A., a quantia de €26.630,24, a importância que se encontrava depositada em conta co titulada, não só pela A., mas também pelas intervenientes mãe e irmã.

8. Conta afeta ao regime de movimentação solidária, presumindo-se que os seus titulares

participam nos valores depositados em montantes iguais.

9. Não tendo a A., sequer alegado, que as respetivas partes são diferentes, ou que só um dos titulares deve

beneficiar de todo o crédito, ilidindo tal presunção.

10. Pelo que, para alem de todas as razões que a seguir se enunciarão, nunca poderia a R. ser condenada a pagar um valor à A. que pertence não só a esta, como às demais cotitulares da conta.

11. Sob pena de vir, mais tarde, a ser acionado em sede de responsabilidade civil, para devolução dos valores em causa – porque como anuncia o velho jargão "quem paga mal, paga duas vezes".

12. Termos em que, padece a sentença recorrida de nulidade, nos termos dos arts. 577, e), 608.º n.º 2, 615.º, n.º 1 d) e 617.º, n.º 1 do CPC, nulidade que desde já se invoca e se requer seja declarada nos presentes autos.

*

II.II) RECURSO QUANTO À MATÉRIA DE FACTO

II.II.I) DOS FACTOS PROVADOS - INSUFICIÊNCIA/INCONGRUÊNCIA, DA MATÉRIA DE FACTO DADA COMO PROVADA, FACE AO ACERVO PROBATÓRIO RECOLHIDO NOS AUTOS

13. Nenhum documento junto pela R., com a contestação, foi impugnado pela A.

14. Em face do acervo probatório recolhido nos autos, e salvo devido respeito, entende a Recorrente que o douto despacho recorrido fez uma incorreta apreciação dos factos e dos meios de prova apresentados pelas partes,

15. Sempre se impondo o aditamento à matéria de facto provada, dos seguintes factos:

a. Depois do facto 2 deverão ser aditados os seguintes factos:

i. Em 07/07/2015, a pedido da A., a R. celebrou com aquela um contrato de adesão ao serviço de "homebanking", designado por "Montepio24 - Particulares" – Doc 2 junto com a contestação

ii. Na mesma data e mediante a assinatura da proposta de adesão ao serviço Montepio 24 a A. declarou ter tomado conhecimento e aceitar as clausulas gerais do Serviço Montepio 24 e as clausulas Particulares de Utilização do Serviço Montepio 24,

iii. Em 07/07/2015 a A. recebeu a comunicação da R. junta com a pi. sob o n.º 2,

b. Após o facto 4 deverão ser aditados os seguintes factos:

i. Do cartão matriz Montepio 24 consta o alerta: "Atenção: Nunca indique mais do que 2 dígitos deste Cartão Matriz"

ii. Na página do Serviço Montepio 24 constava as informações de segurança que resultam de Doc 5 junto com a contestação.

iii. Imediatamente após introdução do código de identificação de utilizador do Montepio24 e imediatamente antes deste introduzir o seu código de acesso personalizado o sistema dispara um alerta com o aviso de alerta constante de Doc. 6 junto com a contestação, sendo necessário – conforme imagem do aviso - que confirmem que leram e tomaram conhecimento do aviso de segurança para que possam prosseguir com qualquer operação.

c. Após o facto 6 deverão ser aditados os seguintes factos:

i. Em 28 de dezembro de 2016, às 11.41h, o marido da A. B, recebeu no endereço de correio eletrónico manuel…@gmail.com a comunicação junta com a p.i., sob Doc. 8.

ii. O marido da A., na sequência desse contacto eletrónico, facultou as credenciais de acesso da conta co titulada pela A., mãe e irmã – Doc 3 junto com a contestação, Doc 7 junto com a p.i., conjugado com arts

26.º e 27.º da pi.

Destarte,

16. Foi celebrado, entre A e R, um contrato de adesão ao serviço de "homebanking", designado por "Montepio24 - Particulares" (DOC. 2 junto com a contestação – não impugnado). Serviço que permitia à autora:

a. aceder a informações sobre produtos e serviços do Montepio,

b. realizar operações sobre as contas que titula,

c. realizar operações de compra e venda, subscrição ou resgate de produtos financeiros ou serviços disponibilizados pelo Montepio aos seus clientes - como decorre da cláusula 2.2. do contrato junto aos autos.

17. Em resultado da referida adesão, cujas condições gerais e particulares a A. declarou ter tomado conhecimento, foram atribuídos pela R, à A os códigos de acesso/credenciais de utilização – como decorre do Doc 2 junto pela própria A. com a pi.

18. Como a A. bem sabia – Vd Docs. 2, 4, 5 e 6 juntos com a contestação da R, não impugnados pela A. e depoimento Daniel .... – as credenciais de acesso são secretas, pessoais e intransmissíveis e funcionam a três níveis de segurança, designadamente:

a. Um número de identificação Montepio, atribuído e entregue no momento da adesão –

cfr. Doc 2 junto com a PI;

b. Um código PIN multicanal, composto por seis dígitos, atribuído e entregue ao cliente

no momento da adesão - permitindo estas duas credenciais apenas a realização de operações e consultas que não comportem alterações de património;

c. Um Cartão Matriz - cartão de coordenadas com 72 posições, cada uma com 3 dígitos,

que nunca se repetem, para validação de operações passíveis de alteração do património, detido pela Autora, na Ré. O cartão matriz é remetido via CTT, para o endereço dos clientes, em estado de pré-ativo, só podendo ser ativado pelos clientes, através da validação dos códigos de acesso (através do número de cliente e do PIN multicanal) e contem a menção "Atenção: nunca indique mais do que 2 dígitos deste cartão matriz".

19. A partir do momento da adesão ao serviço de homebanking, a A passou a autorizar o Montepio a realizar as operações ordenadas, através daquele meio eletrónico, desde que introduzidas as necessárias credenciais de utilização.

20. Pelo que todas as ordens transmitidas ao Montepio, através do serviço Montepio24, gozam de plenos efeitos jurídicos, como consta da cláusula 2.3. do referido contrato de adesão

Acresce que,

21. Conforme decorre de gravação de chamada, autorizada pela A. e marido, datada de

04/01/2017, o marido da A. depois de receber um email a solicitar a ativação do cartão matriz forneceu/introduziu todas as credenciais de acesso da conta da A., mãe e irmã.

22. A ocorrida e reconhecida divulgação e introdução de todas das credencias de acesso, contraria: a. todas as informações de segurança veiculadas à A. aquando da celebração do contrato de adesão ao serviço - que a mesma declarou ter tomado conhecimento, b. avisos de segurança disponíveis no seu

cartão matriz – documento não impugnado,

c. avisos de segurança disparados em sistema, Montepio 24, quando cliente vai efetuar uma transação – documento não impugnado d. avisos de segurança constantes do sítio de internet da R – documento não impugnado,

23. Representando, tal atuação, uma ostensiva quebra das regras de segurança instituídas e uma violação das normas de acesso ao serviço de homebanking fornecido pela ré,

a. Facultando ao marido (que não era, nem é, titular da conta em questão), as suas credenciais de acesso que, bem sabia, pessoais e intransmissíveis.

b. Permitindo que o marido os tenha divulgado, na sua integralidade, a terceiros, ao arrepio de todos os avisos de segurança emitidos pelo banco - não tendo este estranhado tal solicitação, apesar de se encontrar inscrito no cartão matriz, que utilizou para inserir todas as coordenadas (processo bastante demorado, diga-se) o seguinte aviso: "Atenção: Nunca indique mais do que dois dígitos deste cartão matriz"

24. Ignorando, assim, de forma voluntária e grosseira, os diversos e inequívocos alertas veiculados pela R, no sentido de nunca facultar mais de duas coordenadas do cartão matriz:

a. quer no próprio cartão matriz (DOC. 4 junto com a contestação),

b. quer no seu sítio de acesso ao homebanking (DOC. 5 junto com a contestação)

c. alertas esses que, no sitio de homebanking, surgem também, através de janela "pop up" - imediatamente após introdução do código de identificação de utilizador do Montepio24 e imediatamente antes da introdução do código de acesso personalizado, sendo necessário que o cliente confirme que leu e tomou conhecimento deste aviso de segurança para que possa prosseguir com qualquer operação (DOC. 6 junto com a contestação);

25. Sendo notório que sempre que se efetua um acesso ao sítio da ré, na mesma página onde insere o código PIN, encontra-se em formato de fácil leitura e apreensão, informação diversa e bastante explícita sobre medidas de segurança por aquela adotadas, medidas de segurança/precauções que deverão ser tomadas pelos utilizadores. Bem como exemplos de páginas fraudulentas e de e-mail de Phishing, por forma a alertar os utilizadores para eventuais fraudes, (cfr. DOC. 5 junto com a contestação), que se junta e para cujo teor se remete, designadamente para onde consta:

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

b. Ter sempre presente que os bancos nunca solicitam informações pessoais e/ou confidenciais através de mensagens de correio eletrónico ou SMS, pelo que perante qualquer solicitação neste âmbito, contacte os nossos serviços

c. Suspeite dos erros gramaticais ou de escrita nas mensagens que recebe através de qualquer canal habitual de comunicação

d. Os códigos de acesso/passwords são pessoais e intransmissíveis, pelo que nunca deverão ser fornecidos/disponibilizados a terceiros, nem mesmo a outro(s) titular(es) da(s) conta(s)

26. E no caso concreto, chama inclusivamente a atenção, para alem de tudo o mais, o português do brasil e a deficiente construção frásica, com que o e-mail está redigido, sinal mais do que suficiente para colocar de

sobreaviso o utilizador mais descuidado: “Caso não efectue o processo de activação teu cartão matriz será cancelado permanentemente, será possível apenas em seu balcão de origem”

27. Foi, por isso, apenas e só, a conduta negligente da A. (em contravenção com os procedimentos estatuídos no contrato de adesão ao homebanking e sucessivos alertas emitidos pelo banco) que permitiu que terceiros se tenham apropriado das suas credenciais de acesso e efetuado as operações de transferência descritas nos autos,

28. Factos a que a R foi alheia,

29. Só à A podendo ser imputadas responsabilidades pelos aludidos movimentos.

30. Porquanto é à A. a quem cabe assegurar a integridade dos códigos de acesso/credenciais de utilização, pessoais e intransmissíveis e a sua não divulgação a terceiros.

31. Uma vez que, como decorre do contrato de adesão (cl. 5.1 e 5.3) e até das regras da experiência comum, o cliente de qualquer banco tem a obrigação de acautelar a vigilância dos códigos/credenciais pessoais, evitando desde logo, que eles possam ser objeto de furto, extravio ou apropriação ilegítima, por parte de terceiros.

*

II.II.

III) RECURSO DA MATÉRIA DE DIREITO:

AUSÊNCIA DE PRESSUPOSTOS DE DIREITO QUE JUSTIFIQUEM A CONDENAÇÃO DA RÉ

32. Assistimos, à exploração e implementação de novas ferramentas bancárias, nomeadamente on line, que visam satisfazer os, cada vez mais apurados níveis de exigência do cliente bancário, contribuindo para um vértice de aperfeiçoamento da capacidade de resposta bancária, em benefício da sua clientela e onde forçosamente se inclui o alegado serviço Montepio NET24, como manifestação típica do chamado homebanking, que permite a utilização de canais telemáticos, no interesse e para comodidade dos seus utilizadores.

33. Realidade distinta do depósito, o homebanking constitui uma faculdade de utilização pelo cliente, mediante a adesão a um contrato, do qual constam condições de utilização (com particular enfase para as que respeitam à segurança), que o cliente aceita e sem as quais não pode beneficiar da ferramenta informática.

34. Na execução deste específico contrato, o cliente obriga-se a garantir a segurança dos elementos de identificação que aí lhe são exigidos, bem como a sua utilização estritamente pessoal, nomeadamente:

a. não permitindo a sua utilização por terceiro, ainda que seu procurador ou mandatário;

b. não os revelando nem por qualquer forma os tornando acessíveis ao conhecimento de terceiro e

c. memorizando-os e abstendo-se de os registar, quer diretamente, quer por qualquer forma ou meio que se mostre inteligível por terceiros.

35. In casu, a R logrou provar que a falta de cumprimento não procedeu de culpa sua, mas antes de culpa do seu cliente, ora recorrida.

36. Como se extrai do acervo probatório recolhido nos autos e contrariando o que deva ser tido por elementares regras de procedimento de segurança, no acesso ao homebanking, em particular ao Montepio 24, a A forneceu a terceiros todas as credenciais de acesso à sua conta bancária, permitindo viabilizar a

realização de operações de pagamento não autorizadas por terceiros.

37. Sendo abundante a jurisprudência que neste caso acolhe o entendimento de que esta conduta não pode deixar de ser configurada como negligência grave, preenchendo assim o estatuída no art. 72.º, nº 3,

38. Ou seja, a resposta liminar de que deve ser o banco quem suporta o risco de uma utilização abusiva do serviço de homebanking não é correta do ponto de vista estritamente jurídico, pois muitas vezes os clientes, pelo seu comportamento, dão azo a acessos indevidos às suas contas.

39. Os clientes que aderem ao contrato de homebanking não podem deixar de ter consciência dos perigos que isso importa, mas que seguindo à risca as instruções do banco, não resultará qualquer perigo.

40. Este dever de informação tem integral cabimento dentro do aludido dever de segurança que impende sobre o Banco Réu pois que, com a correta utilização dos dados fornecidos, sem que sejam transmitidos a terceiros, o sistema é seguro.

Em suma,

41. Tendo-se apurado nestes autos que as transferências "sub judice" foram efetuadas fraudulentamente por terceiros, com recurso à técnica conhecida por phishing, logo se conclui que as mesmas não ocorreram por uma qualquer avaria ou deficiência do sistema informático da Ré.

42. Já no que tange à questão da utilização do serviço homebanking por banda da autora, resulta óbvio, que se produziu em total desrespeito das condições acordadas, maxime no que concerne às que se reportam à segurança.

43. Pelo que, a decisão proferida, viola os artigos 570º e 799º ambos do Código Civil e ainda os art 67º e 72º do DL 317/2009.

44. Termos em que deverá ser revogada a douta sentença recorrida absolvendo-se a apelante da condenação proferida.

TERMOS EM QUE, DECLARANDO A NULIDADE DA SENTENÇA PROFERIDA EM PRIMEIRA INSTÂNCIA, OU CONCEDENDO PROVIMENTO AO RECURSO INTERPOSTO E REVOGANDO A SENTENÇA RECORRIDA, ABSOLVENDO A APELANTE DA CONDENAÇÃO PROFERIDA

*

A AUTORA A e outras, apresentaram contra-alegações, concluindo da forma seguinte:

1.ª Tendo em vista o exposto na 1.ª questão, o erro ou lapso material não contempla a nulidade que o banco recorrente aponta à R. decisão proferida;

2.ª Tratando-se, no caso de mero lapso de escrita, deverá ser retificado sendo a condenação do banco réu a pagar a quantia em causa à A. e intervenientes;

3.ª Tal como se demonstrou na 2.ª questão, foram selecionados os factos importantes e relevantes para a decisão de mérito.

4.ª Dos factos dados como provados, e, tal como considerado na R. decisão, a culpa do

banco réu no caso em concreto, é grosseira na falha dos sistemas de segurança e controlo, pelo que perante tal factualidade, a R. decisão recorrida não merece censura ou reparo, e em consequência, deverá rejeitar-se o recurso, com a manutenção integral da decisão recorrida.

*

Colhidos os vistos legais, cumpre decidir:

*

QUESTÕES A DECIDIR:

-DA NULIDADE DA SENTENÇA.

-DA IMPUGNAÇÃO DA DECISÃO DE FACTO.

-SABER SE HOUVE VIOLAÇÃO DO CONTRATO DE HOMEBANKING

-DA RESPONSABILIDADE EM CASO DE PISHING

-DA OBSERVÂNCIA POR PARTE DO RÉU DOS DEVERES DE INFORMAÇÃO.

-SABER SE A AUTORA AGIU COM NEGLIGÊNCIA GROSSEIRA, EXCLUINDO A OBRIGAÇÃO DE O APELANTE PAGAR O VALOR PETICIONADO.

*

FUNDAMENTAÇÃO:

II –Fundamentação de Facto

A) Dos Factos.

1.º A autora é juntamente com a sua Mãe Palmira ..... e sua irmã Maria ..... , Cotitulares de uma conta solidária com os números:

i) 168.10005058-7;

ii) 168.15011897-9, conforme se verifica dos documentos juntos com o número 1 a 3.

2.º Tratando-se de uma conta do tipo solidário, as Cotitulares acordaram que tais contas seriam movimentadas pela assinatura de qualquer uma delas, conforme consta da ficha de assinaturas.

3º Em data que a autora não consegue precisar, mas que a autora situa ter sido em Julho de 2015, o banco Réu passou a disponibilizar-lhe das contas bancárias acima referidas, a sua movimentação através do sistema “NET24”.

4º Fornecendo para o efeito, os respetivos códigos de segurança na movimentação da conta, designadamente da conta à ordem e da conta a prazo;

5º A movimentação de tais contas através do sistema homebanking do banco réu, designado NET24, era usado muito “esporadicamente” para pagamentos pontuais:

(a) No mês de Janeiro de 2016, tal sistema foi usado por uma vez;

(b) Em Abril de 2016, por uma vez;

(c) Em Maio de 2016 por três vezes;

(d) Em Junho de 2016, por duas vezes;

(e) Em Agosto de 2016, por duas vezes;

(f) Em Setembro de 2016, por duas vezes;

(g) Em Outubro de 2016, por uma vez;

(h) Em Novembro de 2016, por uma vez;

(i) Em 21/12/2016, a autora fez uma transferência de 141,28€ para o Banco de Portugal como habitualmente fazia conforme consta do extrato que se junto com tais movimentos.

6º Conforme consta do acima exposto, verifica-se que a autora fazia uma movimentação reduzida quer de valores (1) quer de operações bancárias em média de uma/duas por mês.

7º No dia 4 de janeiro de 2017, a 1.ª titular da conta e Mãe da Autora, dirigiu-se à agência do Banco Réu

para levantar a importância de 100,00€ e ali foi informada pelo empregado do banco que a atendeu, da existência de elevadas movimentações nas contas a prazo e à ordem, através do "Netbanco".

8º Designadamente ocorridas entre 28/12/2016 e 4 de Janeiro de 2017.

9º As cotitulares, logo que tiveram notícia de tal facto, ficaram alarmadas.

10º Constataram então do extrato bancário, naquele período de 28/12/2016 a 4/1/2017, em menos de uma semana, as seguintes movimentações:

(a) Da conta 168.15011897-9 para a conta à ordem com o n.º 168.10.005058-7, sete operações no valor global de 29.000,00€ (vinte e nove mil euros);

(b) Da conta à ordem 168.10.0050-7 para supostamente "PAG.SER" 54 (cinquenta e quatro) operações, no valor global de 26.630,24€ (vinte e seis mil e seiscentos e trinta euros e vinte e quatro cêntimos), conforme consta dos extratos que ora se juntam.

(1) Com exceção das transferências em Maio de 5.000,00€ cada que constam do extrato.

11º Na mesma data de 4.1.2017, logo que tiveram conhecimento de tal facto, a Autora procedeu ao cancelamento da movimentação bancária por tal via.

12º Em consequência, logo que apuraram os factos, a Autora através de carta datada de 24.1.2017, notificou o banco Réu, nos termos que constam do documento 4, ali salientando a sua surpresa e indignação pelo facto do Banco Réu ter permitido tal utilização abusiva, anormal e absolutamente imprudente e irresponsável do banco, ao permitir tal movimentação naquelas contas, de forma repetida em tão curto espaço temporal quando o cliente em causa não tinha tradição naquele tipo de movimentação.

13º Tanto mais grave quando tudo isto acontece num curto espaço temporal entre o dia 28/12/2016 e 4.1.2107 num total de operações superior a 60 quando o cliente habitualmente fazia UMA e NUNCA "PAG. SERV", como repetidamente consta de tais operações fraudulentas.

14º Na carta em que notificou o banco Réu bem como na Reclamação apresentada no respetivo livro, a Autora reclamou do banco, a reposição dos valores ilicitamente retirados da conta, sem qualquer autorização ou consentimento dos seus titulares.

15º Com data de 6 de Fevereiro, o Banco Reu, respondeu à Autora através da carta junta como doc. 5, e, em resumo, refere:

- Que o sistema de segurança do Montepio é revestido dos mais rigorosos sistemas de segurança!
- Sugerindo a utilização de antivírus e que o utilizador não forneça a terceiros os seus códigos;
- Que, terceiros apoderaram-se de coordenadas do cartão matriz e que ao que tudo indica, terá ocorrido um crime de burla informática, alheio ao C;

16º Consequentemente declinou o banco Réu, qualquer responsabilidade na restituição das quantias ilicitamente retiradas da conta da Autora.

17º Conforme consta do documento 6 enviado pela Autora ao Banco Réu em 4/1/2017, ali refere o seguinte:

"Exmos Senhores

Venho por este meio manifestar os meus maiores protestos pelo vosso sistema de segurança da NET24, que permite que alguém possa através dela fazer qualquer tipo de movimentos, sem qualquer outra

validação.

Como é admissível que desta forma se movimentem, sem qualquer outro controlo tanto contas a prazo como contas à ordem, valores elevados e tão concentrado no tempo.

No caso em concreto trata.se de contas praticamente baixo movimento (funcionam, praticamente, como contas poupança) que, de um momento para o outro (em 8 dias), uma regista uma altíssima atividade: 61 movimentos, 7 da conta a prazo (168.15.011897-9) para a conta à ordem (168.10.005058-7) e desta para "PAG. SERV": 54 de PAG. SERV. 11249 … (45 movimentos, no valor de 22.482,74€) e PAG. SERV. 11854… 8 movimentos, no valor de 4.147,50€.

Tudo isto sem qualquer das titulares terem sido contactadas por qualquer meio, possibilidade que é admitida na cláusula 3.4 das "Clausulas Gerais de Utilização".

Admito que o aceso às contas tenha sido originado num mail que o meu marido recebeu do endereço net24@montepio.pt a informar que "o seu Utilizador foi desativado temporariamente porque o Cartão Matriz ainda não foi ativado" e dando orientações para o fazer.

O meu marido costuma ser muito cauteloso com estas contas, mas a experiencia com o NET24 não é grande: aderi ao serviço em 07.JUL.2015; uns tempos depois, quando pretendo fazer um pagamento (penso que Julho de 2016), fui informada que o Cartão Matriz tinha caducado por não ter sido validado no prazo estabelecido. Pedi novo Cartão, o que fiz.

Entretanto chega o referido mail…

PS – Informo que hoje suspendi o serviço NET24 e, depois de pedir extrato das contas na vossa Agencia de Sesimbra, apresentei queixa contra terceiros na GNR de Sesimbra."

*

DE DIREITO:

-DA INVOCADA NULIDADE

O banco Réu faz decorrer a nulidade da sentença do facto de a condenação apenas da Autora violar o regime da solidariedade, já que,

1.º A autora é juntamente com a sua Mãe Palmira ….. e sua irmã Maria …., Cotitulares de uma conta solidária com os números i) 168.10005058-7;

ii) 168.15011897-9, conforme se verifica dos documentos juntos com o número 1 a 3.

2.º Tratando-se de uma conta do tipo solidário, as Cotitulares acordaram que tais contas seriam movimentadas pela assinatura de qualquer uma delas, conforme consta da ficha de assinaturas, conforme provado.

Tem razão o Réu quando diz que, sendo a conta afeta ao regime de movimentação solidária, onde como se referiu e nos termos da lei, se presume que os titulares de depósitos solidários participam nos valores depositados em montantes iguais. Não tendo a A. sequer alegado, que as respetivas partes são diferentes, ou que só um dos titulares deve beneficiar de todo o crédito ilidindo tal presunção.

É o que decorre do art. 516.º do CC que faz presumir que os titulares de depósitos solidários participam nos valores depositados em montantes iguais, sem prejuízo de tal presunção ser ilidível, mediante prova de que as respetivas partes são diferentes, ou que só um dos titulares deve beneficiar de todo o crédito

Pelo que não pode a R. ser condenada a pagar um valor à A. que pertence não só a esta, como às demais

cotitulares da conta, sob pena de vir a ser mais tarde acionado em sede de responsabilidade civil, para devolução dos valores em causa.

Dai que, a sentença dos autos, ao condenar a Ré C a pagar apenas à A. a quantia de €26.630,24, omitindo a condenação solidária às três titulares da conta, incorreu em omissão de pronúncia, geradora de nulidade, nos termos da al.d) do nº1, do art.615º do CPC.

Deveria o Tribunal a Quo ter condenado a Ré a pagar a quantia de €26.630,24, solidariamente, à Autora, à sua Mãe Palmira .... e sua irmã Maria ....., co-titulares das contas indicadas em 1).

Tal nulidade é passível de ser conhecida neste momento, não obstando ao conhecimento do objecto da apelação, nos termos do art.665º, nº1, do CPC, dispensando-se a audição das partes nos termos do nº3 do mesmo normativo legal, por já se terem pronunciado nas respectivas alegações e contra-alegações sobre a matéria em causa.

Sanado este vicio da sentença, passemos ao conhecimento do objecto da Apelação.

*

-DA IMPUGNAÇÃO DA DECISÃO DE FACTO

A Ré veio alegar que estão provados por documento, juntos com a contestação e não impugnados pela Autora, uma série de factos que reputa de relevantes para a aferição do seu grau de observância do dever de informação e da negligência grave por parte da Autora.

Consideramos que os factos em causa estão provados por documento e são relevantes para a apreciação da matéria alegada no recurso, razão porque, ao abrigo do disposto no art. 662º, nº1, do CPC, se aditam aos factos provados os seguintes:

18- Em 07/07/2015, a pedido da A., a R. celebrou com aquela um contrato de adesão ao serviço de "homebanking", designado por "Montepio24 - Particulares" – Doc 2 junto com a contestação

19-Na mesma data e mediante a assinatura da proposta de adesão ao serviço Montepio 24 a A. declarou ter tomado conhecimento e aceitar as clausulas gerais do Serviço Montepio 24 e as clausulas Particulares de Utilização do Serviço Montepio 24,

20-Em 07/07/2015 a A. recebeu a comunicação da R. junta com a pi. sob o n.º 2, a saber,

cópia do verso do cartão matriz recebido pela A. e a comunicação da CEMG, datada de 07/07/2015, endereçada à A., na sequência da sua adesão ao Serviço Montepio 24, onde:

-se indicava o n.º de cliente para identificação no serviço Montepio 24;

-se informava a A. que o referido n.º de cliente, só em conjunto com o código PIN e os códigos do cartão matriz (que lhe chegariam, como chegara - ver doc - por correio), possibilitariam o acesso a todos os canais do serviço, designadamente alertando que para operações de saída de fundos do seu património financeiro seriam solicitados 2 dígitos aleatórios das coordenadas do cartão matriz.

-Informando que com a adesão ao serviço Montepio subscrevia também o extrato digital para a conta principal de acesso ao serviço, pelo que passaria a receber o extrato de conta através do Serviço Net 24.

21- i. Do cartão matriz Montepio 24 consta o alerta: "Atenção: Nunca indique mais do que 2 dígitos deste Cartão Matriz"

ii. Na página do Serviço Montepio 24 constavam as informações de segurança que resultam de Doc 5 junto com a contestação, entre elas:

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

-Ter sempre presente que os bancos nunca solicitam informações pessoais e/ou confidenciais através de mensagens de correio eletrónico ou SMS, pelo que perante qualquer solicitação neste âmbito, contacte os nossos serviços.

-Suspeite dos erros gramaticais ou de escrita nas mensagens que recebe através de qualquer canal habitual de comunicação

-Os códigos de acesso/passwords são pessoais e intransmissíveis, pelo que nunca deverão ser fornecidos/disponibilizados a terceiros, nem mesmo a outro(s) titular(es) da(s) conta(s).

iii. Imediatamente após introdução do código de identificação de utilizador do Montepio24 e imediatamente antes deste introduzir o seu código de acesso personalizado o sistema dispara um alerta com o aviso de alerta constante de Doc. 6 junto com a contestação, sendo necessário – conforme imagem do aviso - que confirmem que leram e tomaram conhecimento do aviso de segurança para que possam prosseguir com qualquer operação.

22- i. Em 28 de dezembro de 2016, às 11.41h, o marido da A. B, recebeu no endereço de correio eletrónico Manuel…@gmail.com a comunicação junta com a p.i., sob Doc. 8, onde se pode ler:

- MENSAGEM IMPORTANTE – Cliente Montepio Net24 seu Utilizador foi desactivado temporariamente porque seu Cartão Matriz ainda não foi activado.

Para continuar utilizando os serviços Net24 Particulares Empresas, por favor efectue sua activação agora

Aceda em seu utilizador normalmente em “Activar Cartão Matriz”

O cartão Matriz deve ser activado completamente, para que também seja activado seu utilizador Net24.

Caso não efectue o processo de activação teu cartão matriz será cancelado permanentemente, será possível apenas em seu balcão de origem.

ii. O marido da A., na sequência desse contacto eletrónico, facultou as credenciais de acesso da conta co titulada pela A., mãe e irmã – Doc 3 junto com a contestação, Doc 7 junto com a p.i., conjugado com arts 26.º e 27.º da pi.

Procede nesta parte a Apelação, com a consequente alteração da matéria de facto provada.

*

-ENQUADRAMENTO JURIDICO:

A questão a resolver no âmbito do presente recurso consiste em saber se sobre o Réu/Recorrente impende a responsabilidade pela transferência fraudulenta dos fundos da conta da Autora.

Designa-se por contrato de conta bancária (ou abertura de conta) o acordo havido entre uma instituição bancária e um cliente «através do qual se constitui, disciplina e baliza a respectiva relação jurídica bancária», cfr Engrácia Antunes, Direito dos Contratos Comerciais, 483.

Associado a essa abertura de conta, aparece-nos o depósito bancário (regulado pelo DL 430/91, de 2 de Novembro com as alterações introduzidas pelo DL 88/2008, de 29 de Maio), operação essa que se encontra indissociavelmente ligada à abertura de conta e que constitui um pressuposto sine qua non desta, já que nenhuma conta poderá ser aberta sem quaisquer fundos.

De qualquer modo, aquela abertura de conta constitui o ponto de partida para o vasto complexo negocial

que constitui a relação bancária, cr Engrácia Antunes, ibidem, 484; Menezes Cordeiro, Manual de Direito bancário, 6ª edição, 325/417.

Esta complexa figura contratual, tem sido subsumida a nível jurisprudencial e pela maior parte da doutrina na espécie negocial de depósito, tal como a mesma nos é definida pelos artigos 1185º e 1187º do CCivil, através do qual a Autora colocou à disposição do Réu o seu dinheiro e para que este o guardasse e o restituísse quando fosse exigido, constituindo esta figura um depósito irregular ao qual se aplicam as regras do mútuo, com as necessárias adaptações, cf Calvão da Silva, Direito Bancário, 2001, 347/351; Ac STJ de 22 de Fevereiro de 2011 (Relator Sebastião Póvoas) e de 24 de Outubro de 2013 (Relator Granja da Fonseca), in www.dgsi.pt.

Sem prejuízo do exposto, a Autora, sua mãe e irmã, outorgaram com o Réu um contrato denominado um contrato de adesão ao serviço de "homebanking", designado por "Montepio24 - Particulares" Serviço.

Não obstante se encontrar provada a outorga de «outros contratos» com o Réu, não estamos perante uma multiplicidade de relações contratuais autónomas e estanques entre si, mas antes perante um complexo negocial interligado, configurando uma união de contratos, o qual tem por base aquele convénio principal e que vai ter a sua existência e razão de ser no mesmo, continuando o banco a ter a obrigação de guardar o dinheiro depositado, restituindo-o quando e se lhe for solicitado; sobre os depositantes, poderão acrescer outros deveres, consoante as obrigações que forem assumindo com o depositário por via de outras vias negociais encetadas e às quais podem ter acesso por serem titulares daquele contrato de conta bancária, maxime, através da submissão a cláusulas contratuais gerais, cfr Engrácia Antunes, ibidem, 483/488; Pedro Pais de Vasconcelos, Direito Comercial, Volume I, 221/222; Quirino Soares, Contratos Bancários, in Scientia Iuridica, separata, Janeiro-Abril, 2003. Tomo LII-nº295.

Resulta da factualidade provada, que foi celebrado entre o Banco Réu e a Autora, entre A e R, um contrato de adesão ao serviço de "homebanking", designado por "Montepio24 - Particulares" Serviço que que permitia à autora:

- aceder a informações sobre produtos e serviços do Montepio,
- realizar operações sobre as contas que titula,
- realizar operações de compra e venda, subscrição ou resgate de produtos financeiros ou serviços disponibilizados pelo Montepio aos seus clientes - como decorre da cláusula 2.2. do contrato junto aos autos.

Em resultado da referida adesão, cujas condições gerais e particulares a A. declarou ter tomado conhecimento, foram atribuídos pela R, à A os códigos de acesso/credenciais de utilização, como decorre do Doc 2 junto pela própria A. com a pi.

Como a A. bem sabia –cfm resulta dos Docs. 2, 4, 5 e 6 juntos com a contestação da R, não impugnados pela A. – as credenciais de acesso são secretas, pessoais e intransmissíveis e funcionam a três níveis de segurança, designadamente:

 Um número de identificação Montepio, atribuído e entregue no momento da adesão – cfr. Doc 2 junto com a PI;

 Um código PIN multicanal, composto por seis dígitos, atribuído e entregue ao cliente no momento da adesão - permitindo estas duas credenciais apenas a realização de operações e consultas que não

comportem alterações de património;

 Um Cartão Matriz - cartão de coordenadas com 72 posições, cada uma com 3 dígitos, que nunca se repetem, para validação de operações passíveis de alteração do património, detido pela Autora, na Ré.

O cartão matriz é remetido via CTT, para o endereço dos clientes, em estado de pré-ativo, só podendo ser ativado pelos clientes, através da validação dos códigos de acesso (através do número de cliente e do PIN multicanal) e contem a menção "Atenção: nunca indique mais do que 2 dígitos deste cartão matriz".

A partir do momento da adesão ao serviço de homebanking, a A passou a autorizar o Montepio a realizar as operações ordenadas, através daquele meio eletrónico, desde que introduzidas as necessárias credenciais de utilização.

Pelo que todas as ordens transmitidas ao Montepio, através do serviço Montepio24, gozam de plenos efeitos jurídicos, como consta da cláusula 2.3. do referido contrato de adesão.

Entramos aqui no chamado «home banking», Banco internético (do inglês Internet banking), e-banking, banco online, online banking, às vezes também banco virtual, banco electrónico), concretizado pela possibilidade conferida pela entidade bancária aos seus clientes, mediante a aceitação de determinados condicionalismos, a utilizar toda uma panóplia de operações bancárias, online, relativamente às contas de que sejam titulares, utilizando para o efeito canais telemáticos que conjugam os meios informáticos com os meios de comunicação à distância (canais de telecomunicação), por meio de uma página segura do banco, o reveste de grande utilidade, especialmente para utilizar os serviços do banco fora do horário de atendimento ou de qualquer lugar onde haja acesso à Internet.

Através deste serviço que os bancos põem à disposição dos seus clientes, estes podem efectuar, além do mais, consultas de saldos, pagamentos de serviços/compras, carregamentos de telemóveis, transferências de valores depositados para contas próprias ou de terceiros, para a mesma ou para diversa instituição de crédito.

Da aceitação pela Autora desta disciplina negocial, no âmbito do serviço ajustado com o Réu, em sede de home banking, podemos extrair dois corolários: o banco obrigou-se a manter sob sob rigorosa confidencialidade as Chaves de Acesso e a informação constante do Cartão de Coordenadas; por seu turno o cliente obrigou-se a guardar sob segredo, e a assegurar que os Utilizadores guardam sob segredo, as Chaves de Acesso e o Cartão de Coordenadas e, bem assim, a assegurar que a sua utilização é feita exclusivamente pelos Utilizadores e a prevenir o seu uso abusivo por parte de terceiros.

As relações contratuais assim estabelecidas entre a Autora e o Réu, correram dentro da normalidade desde a data da formalização do acesso a este serviço on line em Julho de 2015, até 4/1/2017. Na verdade, nesta data tomou a Autora conhecimento de que ocorreram movimentos anómalos na sua conta entre as datas de 28/12/2016 e 4/1/2017, com utilização do serviço Netbanco e levantamentos no total de 26.630,24, não autorizado por qualquer das titulares da conta, que também não tiveram conhecimento desses levantamentos.

Afigura-se que no caso, as transferências ocorridas da conta da Autora foram devidas a uma fraude informática, fraude essa caracterizada de phishing.

Na verdade, sendo o homebanking plena de benefícios, surgem situações patológicas em que o cliente vê o dinheiro sair da sua conta.

E essas situações são essencialmente caracterizadas em duas modalidades que passamos a enunciar, na senda do exposto no Ac. do STJ de 18-12-2013, relatado pela Senhora Juíza Conselheira Ana Paula Boularot, no Proc. nº 6479/09.8TBBRG.G1.S1, 6ª SECÇÃO, nos termos seguintes:

"O progresso tecnológico dos últimos anos, veio revolucionar todo o comércio jurídico, nomeadamente a nível das relações bancárias, pois começamos com a emissão de cartões, de crédito e de débito, sendo que com estes se podem realizar uma infinidade de operações utilizando-se para o efeito os terminais de caixa automática, vulgo ATM e podemos agora, através dos sistemas de homebanking, aceder a uma variedade de operações bancárias, on line, utilizando para o efeito um computador pessoal.

Para o efeito os bancos fornecem aos seus clientes senhas de acesso pessoais, bem como cartões matriz constituídos por uma infinidade de composições numéricas, que normalmente são solicitadas no final de cada operação efectuada por meios telemáticos e por forma a autentica-la, já que esse cartão matriz deverá apenas ser do conhecimento do cliente, único a poder utiliza-lo, não lhe sendo permitido fornecer nenhum dos dados nele insertos a terceiros, uma vez que, quer o protocolo da página bancária, quer o tráfego de toda a informação nela processada, o que inclui as sobreditas senhas de acesso, são encriptadas, tornando quase impossível um terceiro obter ou alterar a informação depois de enviada.

Todavia a criptografia, apanágio deste sistema, por si só, não elimina a possibilidade de ataques informáticos por hackers e a intercepção das senhas enquanto estão a ser digitadas, vulgo keylogging.

Embora os sites bancários sejam de uma maneira geral fiáveis, não nos podemos esquecer que a internet constitui uma fonte inesgotável de conhecimento e informação o que gera, concomitantemente e necessariamente uma apetência por banda dos aficionados na busca de quebras dos sistemas, sendo que estas actuações maliciosas são facilitadas pela circunstância de tudo na rede é tendencialmente anónimo, podendo-se tomar como certas determinadas actuações que na vida real nunca seriam admissíveis.

Os ataques cibernautas tornaram-se comuns, tendo surgido novas modalidades de actuações ilícitas como o phishing e o pharming, que visam essencialmente as instituições de crédito.

O phishing (do inglês fishing «pesca») pressupõe uma fraude electrónica caracterizada por tentativas de adquirir dados pessoais, através do envio de e-mails com uma pretensa proveniência da entidade bancária do receptor, por exemplo, a pedir determinados elementos confidenciais (número de conta, número de contrato, número de cartão de contribuinte ou qualquer outra informação pessoal), por forma a que este ao abri-los e ao fornecer as informações solicitadas e/ou ao clicar em links para outras páginas ou imagens, ou ao descarregar eventuais arquivos ali contidos, poderá estar a proporcionar o furto de informações bancárias e a sua utilização subsequente, cfr Pedro Verdelho, in Phishing e outras formas de defraudação nas redes de comunicação, in Direito da Sociedade De Informação, Volume VIII, 407/419: Maria Raquel Guimarães, in Cadernos de Direito Privado, nº41, Janeiro/Março de 2013; Mark A Fox, Phishing, Pharming and Identity Theft in The Banking Industry, in Journal of international banking law and regulation, editado por Sweet and Maxwel (2006), Issue 9, 548/552; Roberto Flor, Phishing, Identity Theft e Identity Abuse. Le Prospecttive Applicative Del Diritto Penale Vigente, in Revista Italiana di Diritto e Procedura Penale, Fasc 2/3-Aprile-Settembre 2007, 899/9446.

A outra modalidade de fraude on line é o pharming a qual consiste em suplantar o sistema de resolução dos nomes de domínio para conduzir o usuário a uma pagina Web falsa, clonada da página real, cfr ibidem.

O processo baseia-se, sumariamente, em alterar o IP numérico de uma direcção no próprio navegador, através de programas que captam os códigos de pulsação do teclado (os ditos keyloggers), o que pode ser feito através da difusão de vírus via spam, o que leva o usuário a pensar que está a aceder a um determinado site – por exemplo o do seu banco – e está a entrar no IP de uma página Web falsa, sendo que ao indicar as suas chaves de acesso, estas serão depois utilizadas pelos crackers, para acederem à verdadeira página da instituição bancária e aí poderem efectuar as operações que entenderem, cfr ibidem.

Qualquer uma destas técnicas visam a obtenção fraudulenta de fundos, obrigando os usuários a ter de usar das maiores precauções no uso destes meios informáticos, sendo usual os conselhos no sentido de verificar sempre os remetentes de e-mails e nunca abrir nenhum e-mail cujo remetente seja desconhecido; não abrir nem executar ficheiros que não tenham sido solicitados; ter sempre um antivírus actualizado no computador; ter sempre o Windows actualizado; e possuir um firewall habilitado.

Estas são as actuações pertinentes com vista a evitar qualquer ataque fraudulento ao sistema, sem embargo de, apesar de tais indicações serem seguidas à risca, o sistema não ser infalível, podendo mesmo com a observância de todos os cuidados adequados, ser alvo de brechas.

(Sobre esta distinção, cfr ainda Ac. da RP de 13-10-2016, Proc. nº 2513/14.8TBVFR.PI).

A situação caracterizada nos autos integra, sem qualquer sombra de dúvida, a figura do phishing, na medida em que o marido da Autora, ao receber no seu e-mail, o e-mail com o conteúdo provado nos autos nos pontos 17 e 22, facultou as credenciais de acesso da conta co titulada pela A., mãe e irmã, permitindo que terceiros acedessem à conta e furtassem o dinheiro.

*

Responsabilidade da Ré:

Refere a sentença recorrida que " resulta da factualidade provada, que a A Autora a A. aderiu ao serviço "NET BANCO" da R. e que, ao analisar os movimentos efectuados na sua conta bancária, verificou haverem sido realizadas movimentações elevadas, não autorizadas, de verbas desde as suas contas para terceiras contas, tendo, assim, sido vítima de PHISHING.

A jurisprudência tem vindo a entender, nesta matéria, que os riscos da falha do sistema informático utilizado, bem como dos ataques cibernautas ao mesmo, correm por conta do banco, por a tal conduzir o disposto no artigo 796º, n.º 1, do Código Civil desde que não se prove a culpa do utilizador – a título de exemplo, o Acórdão do Supremo Tribunal de Justiça, supra citado, ou, ainda, o instituto da responsabilidade civil contratual, fazendo recair a presunção de culpa, prevista no artigo 799º do Código Civil, sobre o banco por causa das deficiências de segurança no serviço home – baking.

Ao mesmo caminho, leva a consideração do Regime das Cláusulas contratuais legais que regula o acesso à actividade das instituições de pagamento e a prestação de serviços de pagamento e resultou da transposição para a ordem jurídica interna, da Directiva n.º 2007/64CE, do Parlamento Europeu de 13 de Novembro, relativa aos serviços de pagamento no mercado interno, que entrou em vigor em 1 de Novembro de 2009 – Cf. Acórdão da Relação de lisboa de 15.03.2016, in www.dgsi.pt."

Salvo o devido respeito, discordamos de tal entendimento.

Na situação dos autos, deparamo-nos com uma realidade distinta do depósito, tratando-se de homebanking que constitui uma faculdade de utilização pelo cliente, mediante a adesão a um contrato, do qual constam

condições de utilização (com particular enfase para as que respeitam à segurança), que o cliente aceita e sem as quais não pode beneficiar da ferramenta informática.

Na execução deste específico contrato, o cliente obriga-se a garantir a segurança dos elementos de identificação que aí lhe são exigidos, bem como a sua utilização estritamente pessoal, nomeadamente:

1. não permitindo a sua utilização por terceiro, ainda que seu procurador ou mandatário; 2. não os revelando nem por qualquer forma os tornando acessíveis ao conhecimento de terceiro, e

3. memorizando-os e abstendo-se de os registar, quer directamente, quer por qualquer forma ou meio que se mostre inteligível por terceiros.

Ora, no caso em apreço no presente recurso, a R logrou provar que a falta de cumprimento não procedeu de culpa sua, mas antes de culpa do seu cliente, ora recorrida.

A factualidade provada, com os aditamentos constantes do presente Acórdão, levam a concluir que a Apelada, contrariando o que deva ser tido por elementares regras de procedimento de segurança, no acesso ao homebanking, e em particular ao Montepio 24, forneceu a terceiros todas as suas credenciais de acesso à sua conta bancária, permitindo viabilizar a realização de operações de levantamentos não autorizadas por terceiros.

Saliente-se desde logo, que houve violação contratual por parte da Autora, ao ceder os dados do cartão matriz ao marido, em cujo e-mail surgiu o tal e-mail enganador ou fraudulento solicitando a activação do cartão. A Autora facultou o marido as credenciais de acesso da conta co titulada pela A., mãe e irmã. Lendo com atenção o e-mail solicitando a activação do cartão, fácil seria concluir que não poderia ter a sua proveniência no Banco Réu, atenta a sua linguagem abrasileirada e com um português incorrecto.

As regras contratuais e de segurança a que a Autora estava contratualmente sujeita nunca lhe permitiriam ceder os dados do cartão ao marido, gerando a conduta deste uma situação de negligência grosseira, que se reflecte na esfera jurídica daquela, por lhe ter facultado os dados do cartão.

Esta conduta deve ser configurada como negligência grave, preenchendo assim o estatuído no art. 72º, nº 3, do DL 317/2009, de 30/10.

Tendo-se apurado nestes autos que as transferências “sub judice” foram efetuadas fraudulentamente por terceiros, com recurso à técnica conhecida por phishing, logo se conclui que as mesmas não ocorreram por uma qualquer avaria ou deficiência do sistema informático da Ré, como defende a Autora.

Antes resulta que a utilização do serviço homebanking por banda da autora, se produziu em total desrespeito das condições acordadas, maxime no que concerne às que se reportam à segurança.

A Ré ao provar a culpa da Autora na transmissão da totalidade dos dados do seu cartão matriz a terceiros e, consequentemente, o seu incumprimento do contrato de homebanking por violação das mais elementares regras de segurança impostas pelo mesmo, ilidiu a presunção de culpa prevista no art. 799º nº 1 do Código Civil, que sobre si impendia, pelo que não é responsável pela movimentação das contas bancárias de forma fraudulenta.

Neste caso, é o cliente quem suporta as perdas resultantes de operações de pagamento efectuadas em execução de ordens dadas através do sistema de homebanking por terceiros, a quem, por actuação gravemente negligente, facultou os códigos e chaves necessários a que tais ordens fossem identificadas como tendo sido dadas por si.”

Estando ilidida a presunção de culpa por parte da Ré, deverá ser absolvida do pedido que contra si foi formulado.

Em sentido idêntico, na jurisprudência, pode ver-se:

-Ac. do Tribunal da Relação de Évora de 12/04/2018, disponível em www.dgsi.pt.

I- A responsabilidade por operações de pagamento não autorizadas, realizadas com recurso ao serviço de homebanking, incumbe, em princípio, ao prestador de serviço de homebanking, conforme estatuído no art. 71º do RSP, cabendo ao utilizador nas situações previstas nos nºs 1 a 3 do artigo 72º daquele regime, designadamente em caso de negligencia grave do ordenante;

II- A apreciação da culpabilidade do ordenante impõe a análise da respectiva conduta, com vista a verificar se omitiu o comportamento devido e, em caso afirmativo, se o fez voluntariamente;

III- Na graduação da culpabilidade do ordenante, há que ter em conta, entre outros factores que se mostrem relevantes, os valores ou interesses que se pretendem acautelar com o comportamento devido, bem como a intervenção da vontade na omissão de tal comportamento;

IV- O comportamento do autor que tendo acedido a uma página eletrónica ilícita convencido de que se tratava da página da entidade bancária, forneceu, a solicitação do sistema, além do número de identificação e do código PIN, a totalidade das coordenadas do cartão matriz, mostra-se adequando a viabilizar a e realização por terceiros de operações de pagamento não autorizadas;

V- A advertência que fora transmitida ao Autor e que constava do cartão matriz, de que a solicitação de mais do que duas posições desse cartão indica a presença de página fraudulenta, impunha cautela ao autor, permitindo-lhe prever a possibilidade de não se encontrar no sítio eletrónico correto e de estar a facultar os seus dados a terceiros.;

VI- A atuação do autor, ao inserir a totalidade das coordenadas inscritas no cartão matriz em páginas semelhante à do serviço de homebanking da Ré, configura negligencia grave, preenchendo a previsão do art. 72, nº 3 ... “ .

Ac. do Tribunal da Relação de Guimarães, em 25/11/2013, disponível em www.dgsi.pt

1. No contrato coligado de depósito bancário e de serviços de acesso via internet à sua movimentação e a outros serviços disponibilizados pela ré, entidade bancária esta tem o dever de protecção e informação, na sua execução continuada

2. O aderente tem de cumprir um conjunto de deveres conexos com a segurança do seu sistema informático e uso da chave de acesso concedida pela ré, não a fornecendo a terceiros.

3. A entidade bancária cumpre o seu dever de protecção e informação colocando no seu site toda a informação disponível sobre segurança, que os utentes têm o dever de consultar, para se prevenirem de fraudes.

4. Age com culpa o utente que fornece todo o seu conteúdo do cartão matriz perante uma solicitação numa página idêntica à do banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador.

Ac. do Tribunal da Relação de Évora de 12/12/2013 disponível em www.dgsi.pt

(...) 3.Provando a Ré que a Autora fez uma utilização imprudente, negligente e descuidada desse serviço, revelando a terceiros, na internet, os seus códigos pessoais de acesso ao serviço, bem como dos elementos

necessários para a confirmação/validação da operação bancária, não lhe é exigível o pagamento das quantias por eles indevidamente movimentadas.

Ac. do Tribunal da Relação de Évora de 25/06/2015 disponível em www.dgsi.pt

(…) V) Age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizados (…)

(…) (VIII) A Ré ao provar a culpa da Autora na transmissão da totalidade dos dados do seu cartão matriz a terceiros e, consequentemente, o seu incumprimento do contrato de homebanking por violação das mais elementares regras de segurança impostas pelo mesmo, ilidiu a presunção de culpa prevista no art. 799º nº 1 do Código Civil, que sobre si impendia, pelo que não é responsável pela movimentação das contas bancárias de forma fraudulenta."

Tendo presente o que acima ficou exposto, impõe-se julgar procedente o recurso, com a consequente revogação da sentença e consequente absolvição do Réu do pedido.

*

DECISÃO:

Nos termos vistos, Acordam os Juízes da 8ª Secção em julgar a Apelação procedente e em consequência, alterando a decisão da matéria de facto, nos termos que acima ficaram expostos, revoga-se a sentença objecto de recurso, absolvendo o Apelante do pedido.

Custas a cargo das Apeladas.

(Esta decisão foi elaborada pela Relatora e por ela integralmente revista)

Lisboa, 1/10/2020

Maria Amélia Ameixoeira

Rui Moura

Eleonora Viegas

Fonte: http://www.dgsi.pt