TRIBUNAL DA RELAÇÃO DE COIMBRA | CÍVEL

Acórdão

Processo	Data do documento	Relator
8592/17.9T8CBR.C1	11 de fevereiro de 2020	Isaías Pádua

DESCRITORES

Contrato de conta bancária > Abertura de conta > Contrato de homebanking > Ataques > Hackers > Fraude eletrónica > Phishing > Pharming

---

SUMÁRIO

I- O contrato de conta bancária (correntemente também designado por contrato de abertura de conta) configura um acordo havido entre uma instituição bancária e um cliente através do qual se constitui, disciplina e baliza a respetiva relação jurídica bancária, e ao qual se encontra indissociavelmente ligado o depósito bancário.

II- Com esse contrato - sendo dominantemente qualificado como contrato de depósito irregular, e ao qual aplicam, na medida da sua compatibilidade, as regras do mútuo - inicia-se toda uma relação jurídica complexa entre banco e cliente, no qual assentam, a ele estando associados, os mais diferentes contratos posteriormente celebrados entre ambos, mas em relação ao qual, todavia, assumem ou podem assumir-se como autónomos.

III- Entre esses contratos que se encontram associados à abertura de conta encontra-se o designado contrato de homebanking, que normalmente se concretiza através da possibilidade conferida pela entidade bancária aos seus clientes, mediante a aceitação de determinados condicionalismos, de utilizar toda uma panóplia de operações bancárias, on line, relativamente às contas de que sejam titulares, os quais têm vindo a obter um forte incremento e adesão pelas inegáveis vantagens que propicia às partes, quer aos clientes, permitindo-lhes um acesso mais rápido, continuado (sem limitação de horários) e cómodo (sem deslocações aos balcões) às suas contas e, desse modo, a realização das mais variadas operações, quer aos bancos, permitindo agilizar serviços e otimizar a gestão dos seus recursos humanos, com a inerente diminuição de custos.

IV- Tratando-se de serviços prestados via internet, os mesmos são frequentemente alvo de ataques dos designados hackers, com objetivo de se apropriarem, de forma ilícita, dos fundos existentes nas contas bancárias.

V- De entre essas técnicas de fraude informática mais comuns, destacam-se o phishing que, grosso modo, consiste no envio “ao cliente” de mensagens de correio eletrónico, que provêm aparentemente do banco

prestador do serviço, visando obter dados confidenciais que permitam o acesso ao serviço de pagamento eletrónico, e o pharming, que se consubstancia numa técnica mais sofisticada através da qual é corrompido o próprio nome de domínio de uma instituição financeira, redirecionando o utilizador para um site falso – mas em tudo similar ao verdadeiro – sempre que este digita no teclado a morada correta do seu banco, ou seja, através dessa técnica suplanta-se o sistema de resolução dos nomes de domínio para conduzir o usuário a uma pagina Web falsa, clonada da página real, ou melhor ainda, essa técnica baseia-se em alterar o IP numérico de uma direção no próprio navegador, através de programas que captam os códigos de pulsação do teclado. o que pode ser feito através da difusão de vírus via spam, e que leva o usuário a pensar que está a aceder a um determinado site – por exemplo o do seu banco –, quando na realidade está a entrar no IP de uma página Web falsa.

VI- Os contratos de homebanking encontram a sua disciplina e enquadramento jurídico no Regime Jurídico dos Serviço de Pagamento e da Moeda Eletrónica (RJSPME), aprovado pelo DL nº. 317/2009, de 30/10, e do qual, e visando evitar que terceiros acedam fraudulentamente às contas bancárias, resultam, além do mais, um conjunto de deveres impostos tanto para o prestador dos serviços como para o seu utilizador, cuja violação é geradora de responsabilidade (vg. civil), sendo que no que concerne particularmente ao utilizador, e tendo daí resultado perdas/danos para si, a medida da sua reparação varia em função da sua atuação culposa.

VII- Negando o utilizador ter dado autorização para uma operação de pagamento que foi executado pela instituição bancária, é sobre esta que impende o ónus de prova de que a operação de pagamento não foi afetada por avaria técnica ou qualquer outra deficiência e/ou que esse pagamento só foi possível devido à atuação fraudulenta daquele ou ao incumprimento deliberado ou com negligência grave dos deveres/obrigações decorrentes do artº. 67º do RSPME.

TEXTO INTEGRAL

Acordam neste Tribunal da Relação de Coimbra

I- Relatório

1. No Tribunal Judicial da Comarca de Coimbra – Juízo Local Cível de Coimbra, os autores, **J...**, divorciado, e **R...**, divorciada, residentes na Rua ..., instauraram (em 16/11/2017) contra a ré, **C...**, com sede na Rua ...**,** a presente ação declarativa, sob a forma de processo comum, pedindo a condenação desta última a:

a) Restituir ao autor a quantia de €21.036,17;

b) Restituir à autora a quantia de €9.954,01;

c) Restituir as aludidas importâncias acrescidas de juros à taxa legal acrescidos de dez pontos percentuais

desde a data em que foram executadas as operações não autorizadas até integral pagamento e que, à data da propositura da ação, ascendem a €2.477,07 e € 1.172,12, respetivamente;

d) Pagar uma indemnização a cada um dos autores por danos não patrimoniais no valor de €2.500,00, acrescida de juros de mora, à taxa legal, desde a citação até integral pagamento.

Para tanto, e em síntese, alegaram:

Viverem em união de facto, em condições análogas às dos cônjuges, e enquanto clientes da ré eram então titulares de duas contas de depósitos à ordem e uma conta de depósitos a prazo (que melhor identificam), sedeadas no balcão do ..., em Coimbra.

No ano de 2016, e após ter sido convencido para tal pela sua gestora de conta (na base de uma relação de confiança que se estabelecera entre ambos) que lhe deu conta das vantagens daí resultantes, o autor aderiu ao serviço homebanking fornecido pela ré (conhecido por serviço Net 24), que lhe permitia realizar operações bancárias por via da internet.

Acontece que no dia 11/01/2017 o autor recebeu um telefonema da sua gestora de conta, dando-lhe conta da necessidade de comparecer imediatamente no aludido balcão da ré, alegando que haver uns problemas com as aludidas contas o que veio a fazer.

Aí foi informado pela sua gestora de conta e pelo gerente do balcão que as referidas contas tinham sido alvo de um "ataque informático", exibindo-lhe extratos das mesmas, tendo o autor então constatado uma série de operações de transferências e pagamentos que não foram por si ordenadas ou autorizadas e que ocorreram entre os dias 3 e 11 de janeiro de 2017, num total de €21.036,17.

Também a conta à ordem titulada pela autora fora alvo de operações de débito, não ordenadas nem autorizadas, entre os dias 3 e 5 de janeiro de 2017, num total de €9.954,01.

Numa das outras idas ao balcão da ré foi comunicada ao autor a receção de uns códigos e cartão do aludido serviço que lhe foram entregues, sem que então nenhuma informação lhe tenha sido comunicada/dada ao nível dos procedimentos a adotar e nomeadamente no que concerne àqueles referentes à segurança (apenas lhe tendo sido dito que teria que introduzir tais dados sempre que quisesse aceder ao site).

Que naquele citado dia dia 11 de janeiro, os identificados colaboradores da ré perguntaram ao autor se havia recebido algum email por parte do Banco, ao que o autor respondeu recordar-se de o ter recebido, tendo posteriormente reenviado o mesmo para aquela sua gestora de contra.

No dia 8 de novembro de 2016, pelas 13h34, o autor recebeu um email proveniente de "M...pt", pelo que, confiando tratar-se de um email fidedigno que lhe havia sido remetido pela ré, terá "clicado" sobre os dizeres "ACTIVAR CARTÃO MATRIZ", que o reencaminhou para a página/site da ré, tendo seguido as instruções que lhe foram dadas.

Autores que responsabilizam a ré por terem sido desfalcados daquelas importâncias, que se tem vindo a recusar a pagar-lhas/repô-las, e pelos danos não patrimoniais que sofreram em consequência dessa situação, e cuja indemnização igualmente reclamam nos termos acima peticionados.

2. Contestou a ré, defendendo-se por impugnação.

Na sua essência, e com relevância, negou qualquer responsabilidade pelo sucedido aos AA. – com as

operações de transferência e pagamentos indevidos de que foram alvo as suas contas, nos termos que se deixaram exarados -, alegando ter cumprido com todas as suas obrigações técnicas e legais a que estava vinculada, inexistindo da sua parte qualquer quebra de segurança na criação, gestão e execução de operações no seu sitio informático, tendo prestado todas as informações necessárias aos AA. para acederem de forma segura àquelas suas contas, através do serviço homebanking que lhes disponibilizou, pelo que tal situação se ficou exclusivamente a dever à utilização imprudente/negligente que o A. fez desse serviço ("Net 24") e do acesso ao mesmo, o que permitiu que terceiros, apropriando-se dos respetivos códigos, tivessem acesso às referidas contas e as movimentassem nos termos que que se deixaram referidos, sem a que a ré nada pudesse fazer para a tal obstar.

Terminou pedindo a improcedência da ação, com a sua absolvição do pedido.

3. Na audiência prévia foi proferido o despacho saneador, onde se afirmou a validade e a regularidade da instância, após que se fixou o objeto do litígio e se enunciaram os temas de prova, sem que tivesse sido alvo de qualquer reclamação.

4. Realizou-se a audiência de discussão e julgamento (com a gravação da mesma).

5. Seguiu-se a prolação da **sentença** que, no final, decidiu julgar a ação parcialmente procedente e, em consequência, condenar a ré a pagar:

« **1**. **Ao Autor:**

a) A quantia de €21.036,17 (vinte e um mil e trinta e seis euros e dezassete cêntimos), acrescida da quantia de €2.477,07 (dois mil quatrocentos e setenta e sete euros e sete cêntimos), bem como de juros de mora, à taxa legal sobre a quantia de € 21.036,17, acrescida de dez pontos percentuais, desde a citação até integral pagamento, a título de danos patrimoniais;

b) A quantia de €2.000,00 (dois mil euros), acrescida de juros de mora, à taxa legal, desde a presente decisão até integral pagamento, a título de danos não patrimoniais;

2. **À Autora**:

a) A quantia de €9.954,01 (nove mil novecentos e cinquenta e quatro euros e um cêntimo), acrescida de €1.172,12 (mil cento e setenta e dois euros e doze cêntimos), bem como de juros de mora, à taxa legal sobre a quantia de €9.954,01, acrescida de dez pontos percentuais, desde a citação até integral pagamento, a título de danos patrimoniais;

b) A quantia de €2.000,00 (dois mil euros), acrescida de juros de mora, à taxa legal, desde a presente decisão até integral pagamento, a título de danos não patrimoniais;

Absolvendo a ré do demais peticionado. **»**

6. Inconformada com tal sentença, **a ré dela apelou, tendo concluindo as suas alegações de recurso nos seguintes termos:**

...

7. Contra-alegaram os autores (fls. 143/153 do processo físico), pugnando pela improcedência total do recurso e pela manutenção do julgado.

8. Corridos os vistos legais, cumpre-nos, agora, apreciar e decidir.

II- Fundamentação

1. Do objeto do recurso

1. Como é sabido, e é pacífico, é pelas conclusões das alegações dos recorrentes que se fixa e delimita o objeto dos recursos, pelo que o tribunal de recurso não poderá conhecer de matérias ou questões nelas não incluídas, a não ser que sejam de conhecimento oficioso (cfr. artºs. 635º, nº. 4, e 639º, nº. 1, e 608º, nº. 2 – fine -, do CPC).

1.1 Ora, calcorreando as conclusões das alegações do recurso da R./apelante, verifica-se que as questões nelas colocadas e que cumpre aqui apreciar são as seguintes:

a) Da impugnação/alteração da decisão da matéria de facto;

b) Da responsabilidade da ré (pelos danos, e sua indemnização, que os autores alegam ter sofrido).

2. **Factos dados como provados pelo tribunal da 1ª. instância.**

...

3. Quanto à 1ª. questão.

3.1 Da impugnação/alteração da decisão da matéria de facto.

A ré impugna a decisão proferida sobre a matéria de facto, no que concerne aos pontos a seguir indicados, alegando, quanto a eles, ter o tribunal a quo procedido a uma incorreta apreciação da prova produzida (a qual indica para suportar essa mesma impugnação e o sentido da decisão que entende dever ser proferida sobre os mesmos).

A prova produzida nos autos é natureza documental e testemunhal, acrescida ainda da declarações de parte do A. marido.

Importa, desde já, referir que não estamos perante factos sujeitos a prova vinculada; pelo que estão sujeitos (no que concerne à prova produzida) à livre apreciação do tribunal.

Procedemos à audição integral do registo da prova produzida em audiência de julgamento (através do suporte áudio que nos foi remetido para o efeito).

E desse registo de gravação, verificamos que em audiência de julgamento foram ouvidos:

...

Devemos dizer que, ouvida tal gravação, a descrição feita na sentença sobre o teor das declarações do A. e depoimentos das referidas testemunhas corresponde, a nosso ver, à essência daquilo que mais de relevante disseram em audiência de julgamento.

3.2 Passemos, agora, à enunciação dos concretos pontos impugnados da decisão da matéria de facto e à sua apreciação.

...

Termos, pois, em que se decide julgar parcialmente procedente a impugnação deduzida à decisão da matéria de facto proferida pelo tribunal a quo, na exata medida em que atrás se deixou exarado.

Pelo que, de seguida, se passará a proceder, em conformidade, à descrição da matéria de facto dada (definitivamente) como assente/provada, e com a alteração da sua numeração, daí decorrente

4. Os Factos (definitivos) Provados

1. Os autores vivem em comunhão de mesa e habitação, em condições análogas às dos cônjuges, há mais de 20 anos;

2. A ré é uma instituição de crédito, da espécie caixa económica, que exerce profissionalmente actividade bancária;

3. Há data dos factos, a seguir descritos, os autores eram clientes da ré, sendo então titulares das seguintes contas (sedeadas no Balcão da mesma sito em ...):

a) De depósitos à ordem nº ..., titulada pelo autor, constando a autora como autorizada;

b) De depósitos à ordem nº ..., titulada pela autora, constando o autor como autorizado;

c) De depósito a prazo ..., titulada pelo autor.

4. No dia 1 de Janeiro de 2017, a conta nº ..., titulada pelo autor, apresentava um saldo credor de valor baixo uma vez que era uma conta muito pouco utilizada por este, quase que limitada ao depósito de valores correspondente às cotizações enquanto associado da instituição M...;

5. No dia 11 de Janeiro de 2017, na hora de almoço, o autor recebeu um telefonema da sua gestora de conta – Drª ... – do balcão do ... da ré – dando-lhe nota da necessidade de comparecer imediatamente nas aludidas instalações, alegando que havia "uns problemas" com as respectivas contas bem como com a conta da autora R...;

6. O autor deslocou-se de imediato ao referido balcão, tendo aí sido informado, quer pela Drª ..., quer pelo gerente do balcão – Dr. ... – que as contas tinham sido alvo de um "ataque informático";

7. E exibiram-lhe extractos das aludidas contas, tendo o autor se deparado com uma série de operações de transferências e pagamentos que não foram por si ordenadas nem autorizadas, e que ocorreram entre os dias 3 e 11 de Janeiro de 2017;

8. Nomeadamente através de transferências não ordenadas nem autorizadas pelos autores de montantes retirados da sua conta de depósitos a prazo nº ... e transferidos para a sua aludida conta à ordem nº ..., nas seguintes datas e valores:

- 05.01.2017 - €3.750,00;
- 06.01.2017 - €3.750,00;
- 08.01.2017 - €3.750,00;
- 08.01.2017 - €3.750,00;
- 09.01.2017 - €3.750,00;
- 10.01.2017 - €1.250,00;
- 11.01.2017 - €1.000,00;

9. Sendo que, após cada uma das aludidas transferências, nos mesmos dias, se seguiram movimentos a débito, com uma cadência praticamente regular de 7 movimentos após o crédito, todos eles não ordenados, nem autorizados pelos autores, sendo 33 dos 36 pagamentos de serviços efectuados para a entidade 11249 e os restantes 3 para a entidade 11854, entidades que os autores desconhecem;

10. Bem como uma transferência, não ordenada nem autorizada pelos autores, no valor de €1.992,00, ocorrida no dia 11 de Janeiro de 2017, com a indicação "TRF.J...";

11. Dos aludidos "PAG.SERV", 26 foram no valor de €483,80, 2 no valor de €482,78, 2 no valor de €997,00 e os restantes 6 de valor diferenciado de €481,75 (dia 06.01), €482,01, €484,23, €527,37 e €532,45 (todos no dia 10.01) e um de €998,00 (no dia 11);

12. A conta à ordem nº ... titulada pela autora R..., entre os dias 3 e 5 de Janeiro de 2017, foi alvo de operações de débito não ordenadas nem autorizadas pelos autores;

13. Com uma cadência praticamente regular de 7 movimentos/dia, num total de 20, todos eles com a

indicação PAG.SERV. para a entidade 11249;

14. Dos aludidos 20 "PAG.SERV", 8 foram no valor de €483,80, 6 no valor de €482,78, 4 no valor de €532,00 e os restantes de valor diferenciado de €530,99 e €527,94;

15. Nessa mesma data (11.01.2017), os aludidos gerente e gestora aconselharam o autor a apresentar, de imediato, queixa na Polícia Judiciária, bem como a subscrever uma declaração/autorização que ditaram ao autor e que este escreveu, assinou e lhes entregou;

16. O que fez, confiando nas aludidas pessoas que lhe referiram que tal seria o teor e o procedimento adequados à restituição pronta dos valores retirados das aludidas 3 contas;

17. O autor estava transtornado com o sucedido, limitando-se a agir de acordo com as instruções que lhe iam sendo referidas como acertadas pelos aludidos colaboradores da ré, pessoas em quem confiava;

18. O autor é depositante na instituição da ré há mais de 40 anos;

19. Em Setembro/Outubro de 2016, numa das muitas idas do autor à sucursal da ré, aquele foi abordado pela sua gestora de cliente – Drª ... – que lhe deu nota da eventual relevância de uma adesão ao sistema de homebanking que a ré oferecia aos seus clientes conhecida por Net24;

20. O autor por insistência sugestiva daquela sua gestora de conta acabou por aceitar aderir ao dito sistema.

21. No dia 11 de Janeiro de 2017, os referidos colaboradores da ré perguntaram ao autor se tinha recebido algum email por parte do Banco, ao que o autor respondeu recordar-se de o ter recebido, tendo ficado de confirmar tal recepção e reenviá-lo para a Drª ..., o que fez ainda no mesmo dia, cerca das 17h15;

22. No dia 8 de Novembro de 2016, pelas 13h34, o autor recebeu no seu email jose.sararomeicentro.com um email proveniente de "M...pt", com o assunto: "Estimado, seu acesso ao Net24 pode ser suspenso. Regularize seu Utilizador";

23. O autor, confiando tratar-se de um email fidedigno que lhe havia sido remetido pela ré, terá clicado sobre os dizeres "ACTIVAR CARTÃO MATRIZ", tendo seguido as instruções que lhe foram dadas;

24. O autor não sabe se o referido email é fidedigno ou não e se a página para a qual foi direccionado ao clicar nos aludidos dizeres é uma página do M... verdadeira ou falsa;

25. Em 16 de Fevereiro de 2017 a ré enviou aos autores as cartas com o teor dos documentos de fls. 16 e 17, informando que não iria restituir os montantes retirados das suas contas;

26. Nos dias 12 e 13 de Janeiro, os autores apresentaram no balcão da ré do ... as cartas com os teores dos documentos de fls. 18;

27. No dia 17 de Janeiro os autores remeteram ao Departamento de Qualidade da ré as cartas com os teores dos documentos de fls.19 e 20;

28. Em consequência dos factos narrados, os autores ficaram transtornados e incomodados, tendo perdido a paz e o sossego, sofrendo perturbação emocional e angústia, com prejuízo na sua saúde e produtividade;

29. A ré presta um serviço de homebanking, designado por "M24", nos termos do contrato celebrado entre as partes;

30. A sociedade P..., Ldª, aderiu ao serviço de homebanking, designado por "M24 Empresas", em 2009 e 2013;

31. Figurando o autor, em ambos os documentos de adesão, como 1º representante (sócio-gerente da

aludida sociedade);

32. O M24 é um serviço através do qual os clientes bancários têm a possibilidade de aceder a informações sobre produtos e serviços do M..., realizar operações sobre todas as contas que (co)titulam, realizar operações de compra e venda, subscrição ou resgate de produtos financeiros ou serviços disponibilizados pelo M... aos seus clientes;

33. Permite ao cliente realizar operações bancárias sem necessidade de se deslocar aos balcões do banco e sem estar sujeito ao horário de atendimento ao público, sendo que o cliente efectua operações bancárias sem intervenção do pessoal, com diminuição de custos de financiamento;

34. Foram atribuídos ao autor, pela ré, códigos de acesso/credenciais de utilização;

35. Tais códigos e credenciais permitem aceder a todas as contas tituladas por singulares em que seja titular ou autorizado;

36. A Conta de Depósitos à Ordem nº..., titulada pelo autor, foi por aquele aberta junto da ré em Dezembro de 2002, tendo na mesma sido inserida, em 2007, na qualidade de autorizada, a autora, tendo esta última sido removida dessa conta em 2017;

37. A Conta de Depósitos à Ordem nº ..., titulada pela autora, foi aberta em 1987 e encerrada em 06.06.2017, tendo o autor constado dessa conta, desde a abertura, na qualidade de autorizado;

38. A Conta de Depósitos a Prazo encontra-se encerrada desde 11.11.2017;

39. Um autorizado constitui, para todos os efeitos legais, um procurador, um representante do titular da conta, tendo plena autorização para movimentá-la em nome e representação do titular da conta bancária;

40. Valendo a acesso ao “homebanking” para todas as contas em que o seu utilizador conste como titular ou autorizado;

41. Os mencionados códigos de acesso/credenciais de utilização são pessoais e intransmissíveis e funcionam a três níveis de segurança:

- um número de identificação M..., atribuído e entregue ao cliente no momento da adesão;
- um código PIN multicanal, composto por seis dígitos, atribuído e entregue ao cliente no momento da adesão (permitindo estas duas credenciais a realização de operações e consultas que não comportem alterações de património);
- um cartão matriz que consiste num cartão de coordenadas com 72 posições, cada uma com 3 dígitos (216 dígitos no total) para validação de operações passíveis de alteração do património detido pelos autores junto da ré;

42. O cartão matriz é remetido via CTT para o endereço dos clientes em estado de pré-activo, apenas passível de ser activado pelos clientes mediante validação de códigos de acesso (através do número de cliente e do PIN do multicanal)

43. A partir do momento da adesão ao serviço de homebanking, os clientes autorizam o M... a realizar as operações ordenadas através daquele meio electrónico;

44. No dia 11 de janeiro de 2017 o autor foi contactado pelos serviços da ré, na sequência de um email enviado ao balcão da ré, sito no ..., pelo Departamento de Auditoria e Inspecção (DAI);

45. Os funcionários da ré aconselharam o cliente a intentar queixa-crime, tendo solicitado ao autor que prestasse um esclarecimento escrito, com verdade, sobre todos os acontecimentos de que se recordasse;

46. Foi interditado o acesso ao homebanking relativamente a todos os clientes intervenientes nas contas envolvidas;

47. A adesão do autor ao serviço M24 aconteceu em 22 de Dezembro de 2016, data em que o autor foi informado dos procedimentos de utilização e de segurança do serviço, tendo-lhe sido entregue toda a documentação necessária para a activação do serviço, que foi feito no balcão da ré, com o acompanhamento dos funcionários da ré, tendo-se, nesse acto, alterado o pin de acesso.

48. O autor foi recordado que o cartão matriz é sempre enviado para a morada do cliente, devendo ser por ele activado, o que veio a suceder no dia 3 de Janeiro de 2017;

49. No corpo do texto do email referido em 22. dos factos provados consta:

“:: Atenção Cliente M... – Seu acesso foi desactivado ::

Seu Cartão Matriz não está actualizado,

Por esta razão o teu Utilizador Net24 foi temporariamente desactivado.

Por gentileza, para continuar utilizando nosso serviço Net24, efectue agora mesmo o processo de actualização do seu cartão matriz agora mesmo. Caso contrário somente em seu balcão de origem”;

50. A ré veicula, nos acessos ao M24, alertas de segurança e recorda as boas práticas, os perigos e exemplos conhecidos de fraudes, designadamente através de um alerta que surge sempre, em todos os acessos ao M24, após introdução dos dígitos correspondentes ao código de identificação de utilizador M(...)24 e imediatamente antes da introdução de acesso personalizado, conforme consta do documento de fls. 52;

51. Em todos e cada um dos acessos ao M24 constam avisos de cuidados de segurança e boas práticas a ter pelos clientes;

52. Os acessos às operações em causa foram efectuadas através da Net24 (logon) com introdução de código de cliente e PIN (6 posições), e 128 posições do cartão matriz, todos correctos e à 1ª. tentativa.

53. Com excepção de uma situação ocorrida no dia 5 de Janeiro de 2017 (às 03:20:35h) em que a operação não foi autorizada por erro na introdução dos dígitos do cartão matriz, sendo que, passados 30 segundos, aproximadamente, foi efectuada nova tentativa, para a qual foram solicitadas as mesmas posições e na qual foram correctamente introduzidas as duas posições do cartão matriz;

54. As operações financeiras efectuadas nos dias 3 e 4 de janeiro de 2017, até às 02:55:29h de dia 4, foram feitas através da internet e NetMóvel;

55. No cartão matriz encontra-se impressa a seguinte indicação: “Atenção: nunca indique mais do que 2 dígitos deste Cartão Matriz”;

56. Sempre que se efectua um acesso ao sítio institucional da ré, na mesma página onde se insere o código PIN, encontram-se medidas de segurança/precauções que devem ser tomadas pelos utilizadores, designadamente:

- “O M... apenas lhe solicita a indicação de 2 posições do seu Cartão Matriz nas operações em que o seu património é alterado, por exemplo na realização de uma Transferência Interbancária ou Pagamento de Serviços, entre outros”;
- “Na activação do cartão Matriz não são solicitadas posições do mesmo”;
- “O M... nunca lhe solicitará a realização de qualquer actualização de segurança de códigos de

identificação via e-mails com links diretos para o site oficial";

57. E de exemplos de páginas fraudulentas e de email de Phishing, onde consta expressamente:

- "Suspeite de qualquer e-mail, chamada telefónica ou SMS, que peça uma "acção imediata" ou crie um sentido de urgência ou risco grave. Em caso de dúvida contacte o seu banco";

- "Suspeite de e-mails, supostamente do seu banco mas que inicia o seu texto com cumprimentos como "Querido Cliente" ou qualquer outra saudação diferente das que o seu banco habitualmente utiliza nas suas comunicações";

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

58. Esta página é regularmente actualizada pela ré;

59. Na referida página existe um "layer" de segurança, que surge no acesso ao M24 sempre que se efectua o acesso de um computador novo ou no mesmo computador, desde que os "cookies" tenham sido limpos, layer este que está on-line no sítio da ré desde Abril de 2009;

60. Os movimentos indicados pelos autores foram efectuados através do serviço homebanking M24;

61. À data em que foram detectados, os mesmos já estavam consumados;

62. Os pagamentos de compras e pagamentos de serviços são imediatos;

63. Os movimentos efectuados nas contas dos autores referenciados nos pontos 8. e seguintes apenas foram possíveis porque em cada um deles:

- Foi introduzido o número de identificação M...;

- Foi introduzido o número de código Pin M24;

- Foi validado o Pin, foram introduzidas duas coordenadas e posições do cartão matriz, que são sempre solicitadas de forma aleatória pelo sistema e nunca repetidas.

64. A ré utiliza no cartão matriz o sistema de "one time password", sistema de segurança acrescida, baseado na inutilização (irrepetibilidade) de cada dígito utilizado.

5. Quanto à 2ª. questão.

- Da responsabilidade da ré (pelos danos, e sua indemnização, que os autores alegam ter sofrido).

Essa questão tem a ver com o julgamento do mérito da causa.

Em síntese, refira-se que com a presente ação os AA. vieram responsabilizar a ré pelas quantias que foram retiradas das suas contas bancárias de que eram titulares num dos balcões dessa instituição bancária, de qual eram então clientes, na sequência de operações/movimentações bancárias (transferências e pagamentos) que não foram por si autorizadas, pedindo, em consequência, a condenação das última a restituir-lhes (já que a mesma se recusa a fazê-lo) essas importância se ainda a indemniza-los pelos danos não patrimoniais/morais que sofreram com tal situação, com o acréscimo de juros moratórios legais.

A ré declinou qualquer responsabilidade pelo sucedido, imputando essa responsabilidade ao A., devido ao facto de, em desrespeito de todas as instruções/recomendações que lhe foram transmitidas para o efeito, o mesmo ter feito uma utilização imprevidente/negligente do sistema que lhe permitia aceder ao serviço homebanking prestado pela ré aos seus clientes (denominado serviço Net 24 ou M24) e ao qual o autor tinha aderido, o que terá, com toda a probabilidade, motivado que o A. fosse vitima de burla/fraude informática, conhecida por phishing, e para a qual a ré em nada contribuiu e não pode na altura evitar.

Na sentença recorrida, embora tribunal a quo tenha admitido ter ocorrido uma movimentação fraudulenta das contas dos AA., concluiu, todavia, que, à luz dos factos apurados, a ré não logrou demonstrar, como lhe competia, qualquer culpa daqueles (e particularmente do A.) nessa movimentação de que foram alvo essas suas contas, e nessa medida, por força das obrigações que decorriam da relação contratual com eles estabelecida, condenou-a a reembolsar os AA. das quantias que ficarem desembolsados na sequência daquela movimentação das suas contas e ainda a indemniza-los pelos danos não patrimoniais/morais que sofreram em consequência dessa situação, a acrescerem os juros moratórios às taxa legais.

Neste seu recurso dessa sentença, e à luz dos factos apurados (cuja alteração, em relação a alguns daqueles ali fixados, requereu, como vimos) a ré - contra a posição defendida pelos AA. (nas suas contra-alegações) no sentido da manutenção daquela decisão - mantém a sua posição antes assumida, declinando qualquer responsabilidade pela aludida movimentação fraudulenta das contas dos do AA. (que apenas atribui ao comportamento negligente do autor ao permitir, devido à inobservância das instruções que lhe foram recomendadas para o efeito, que um terceiro se tenha apropriado das suas credenciais para a realização dessas aludidas operações, através do serviço homebanking, e desfalcado, assim, as contas bancárias), e nessa medida pugna pela sua revogação da sentença, com a improcedência da ação e a sua absolvição do pedido.

Apreciemos.

Perscrutando a materialidade factual apurada (cfr. ponto 3.) dela se extrai, desde logo, e como bem se acentuou na sentença recorrida, que entre os autores e a ré foi estabelecida uma relação contratual por via da abertura de, pelo menos, três contas bancárias, no âmbito da qual foi também celebrado um contrato de depósito bancário, e mais tarde (como iremos ver) um contrato de e-banking ou homebanking, denominado Serviço M24.

O contrato de conta bancária (correntemente também designado por contrato de abertura de conta) configura um acordo havido entre uma instituição bancária e um cliente através do qual se constitui, disciplina e baliza a respetiva relação jurídica bancária (cfr. **Engrácia Antunes,** in **“Direito dos Contratos Comerciais, Almedina, pág. 483”**).

Associado a essa abertura de conta, aparece o depósito bancário (regulado pelo DL nº. 430/91, de 02/11, com as alterações introduzidas pelo DL nº. 88/2008, de 29/05), 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.

A abertura de conta essa que, no fundo, configura um “contrato normativo, uma vez que regula toda uma actividade jurídica ulterior, ainda que facultativa" sendo que com ele se inicia toda uma relação jurídica complexa entre banco e cliente, em que assentam os diferentes contratos celebrados posteriormente entre eles, ou seja, esse contrato de abertura de conta constitui o ponto de partida para um vasto complexo negocial em que se decompõe a relação bancária (cfr. **Meneses Cordeiro,** in **“Manual de Direito Bancário, Almedina, 4ª. ed., pág.. 510**” e **Engrácia Antunes,** in **“Ob. cit., pág. 484”**).

Contratos esses, associados à conta, mas autónomos, com caráter necessário (por ex., a conta-corrente bancária), usual ou normal (por ex., o depósito) ou meramente eventual (por ex., convenção de cheque, cartão bancário, homebanking, etc.).

Como transparece do que atrás já deixámos referido, entre a ré (instituição bancária) e cada um dos AA. foi celebrado um contrato de depósito bancário (regulado pelo DL nº. 430/91, de 02/11, com as alterações introduzidas pelo DL nº. 88/2008, de 29/05).

Este contrato vem sendo dominantemente qualificado como contrato de depósito irregular, a que se aplicam, na medida do possível as regras do mútuo (artº. 12016º do CC), isto é, com as necessárias adaptações, ou seja, "na medida em que sejam compatíveis com a função específica do depósito, mais as normas do depósito que não colidam com o efeito real da transferência da propriedade do dinheiro depositado" (cfr., **Calvão da Silva,** in **"Direito Bancário, 2001, págs. 347/351; Meneses Cordeiro,** in "**Ob. cit., pág. 572,**" e **Acs. do STJ de 18/12/2013, proc. 6479/09.9TBBRG.G1.S1**, e **de 22/02/2011,** disponíveis in www.dgsi.pt.).

Assim, (e como se salienta no **Ac. do STJ de 14/12/2016, proc. 1063/12.1TVLSB.L1.S1,** disponível in www.dgsi.pt, cujo pensamento vimos seguindo de perto) efetuado o depósito, o depositário fica obrigado a outro tanto do mesmo género (artº. 1142º do CC); o dinheiro depositado torna-se propriedade do depositário pelo facto da entrega (artº. 1144º). Desse modo, "o depositante troca a propriedade da soma depositada por um direito de crédito à restituição de outro tanto, com a transferência do risco a acompanhar a transmissão da propriedade (res perit domino – art. 796º, nº. 1, do CC)" (cfr. **Calvão da Silva, "Ibidem**").

O que significa que as disponibilidades monetárias depositadas numa conta bancária passam para o domínio e propriedade do Banco – embora com a obrigação de restituir outro tanto logo que tal lhe seja solicitado pelos depositantes -, sendo que, nos termos do disposto no citado artigo 796º do Código Civil, "nos contratos que importem a transferência do domínio sobre certa coisa ou que constituam ou transfiram um direito real sobre ela, o perecimento ou deterioração da coisa por causa não imputável ao alienante corre por conta do adquirente."

Como decorre da material factual apurada (cfr. pontos 19, 20, 29, 32, 33, 34, 40, 43, 47), dentro daquele complexo negocial, entre a ré e o autor veio a ser celebrado um contrato que permitia a este aceder ao serviço de homebanking (designado por M24) prestado pela ré, através do qual do qual os seus clientes bancários têm a possibilidade de aceder (via internet) a informações sobre produtos e serviços do M..., realizar operações sobre todas as contas que (co)titulam, realizar operações de compra e venda, subscrição ou resgate de produtos financeiros ou serviços disponibilizados pelo M... aos seus clientes, permitindo, assim, a esses clientes realizar operações bancárias sem necessidade de se deslocar aos balcões do banco e sem estar sujeito ao horário de atendimento ao público, permitindo ainda ao seu utilizador o acesso, por essa via, a todas a contas de que seja titular ou esteja autorizado a movimentá-las.

É inolvidável, assim, que entre a ré e o autor foi celebrado contrato de homebanking, que a lei qualifica também como "contrato-quadro": "um contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento" – artº. 2º, al. m), do Regime Jurídico dos Serviço de Pagamento e da Moeda Eletrónica (doravante RJSPME), aprovado pelo DL nº. 317/2009, de 30/10 (que transpôs, para a nossa ordem jurídica o novo enquadramento comunitário em matéria de pagamentos, máxime a Diretiva 2007/64/CE, de 13/11).

Este contrato tem vindo a obter um forte incremento e adesão, pelas inegáveis vantagens que propicia às partes; quer para o cliente, permitindo-lhe um acesso mais rápido, continuado (sem limitação de horários) e cómodo (sem deslocações aos balcões) às suas contas e, desse modo, a realização das mais variadas operações; quer para o banco, permitindo agilizar serviços e optimizar a gestão dos seus recursos humanos, com a inerente diminuição de custos.

Na verdade, (e como se dá nota citado **Ac. do STJ de 18/12/2013**) através do referido contrato - também designado home banking (Banco internético, do inglês Internet banking), e-banking, banco online, online banking e às vezes também banco virtual ou banco eletrónico -, concretiza-se a possibilidade conferida pela entidade bancária aos seus clientes, mediante a aceitação de determinados condicionalismos, a utilizar toda uma panóplia de operações bancárias, on line, 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 que se 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 desse serviço que os bancos põem à disposição dos seus clientes, estes podem efetuar, 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.

Dispõe o artigo 73º Regime Geral Das Instituições De Crédito e Sociedades Financeiras (DL nº 298/92, de 31/12) que “as instituições de crédito devem assegurar, em todas as atividades que exerçam, elevados níveis de competência técnica, garantindo que a sua organização empresarial funcione com os meios humanos e materiais adequados a assegurar condições apropriadas de qualidade e eficiência”.

Numa concretização desse dever geral, e visando o eficaz e seguro funcionamento daquele tipo de serviços foram plasmados no referido RJSPME um conjunto de obrigações impostas ao prestador dos mesmos e aos seus utilizadores.

Assim, naquilo que aqui mais releva, decorre do referido regime (RJSPME) que o prestador dos serviços de pagamento tem a obrigação de “assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento (…)” (artº. 68º, nº. 1 al. a),).

Por sua vez, nos termos do seu artº. 67º, nº. 1, o utilizador de serviços de pagamento com direito a utilizar um instrumento de pagamento tem a obrigação de utilizar esse instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização” (al a)) e “de comunicar, sem atrasos injustificados, ao prestador de serviços de pagamento, logo que deles tenha conhecimento, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento” (al. b)), sendo certo que“para efeitos da alínea a), o utilizador de serviços de pagamento deve tomar todas as medidas razoáveis, em especial ao receber um instrumento de pagamento, para preservar a eficácia dos seus dispositivos de segurança personalizados.” (nº. 2).

Dispõe ainda o artº. 70º desse RJSPME que:

“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 par**a **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" (sublinhado e negrito nossos)

Compreende-se este regime: por um lado, só o prestador do serviço de pagamentos, também fornecedor deste serviço, pode assegurar a operacionalidade do complexo sistema informático utilizado e a regularidade do seu funcionamento, garantindo também a confidencialidade dos dispositivos de segurança que permitem aceder ao instrumento de pagamento.

Daí que (como se salienta no **Ac. do STJ de 14/12/2016,** acima citado, cujo pensamento vimos seguindo de perto) recaia sobre o banco prestador do serviço o risco das falhas e do deficiente funcionamento do sistema (como decorreria também do disposto no arº. 796º do CC, como já supra deixámos referenciado), impendendo ainda sobre este o ónus da prova de que a operação de pagamento não foi afetada por avaria técnica ou qualquer outra deficiência.

Como refere **Calvão da Silva** (**Ibidem**), e supra também já deixámos assinalado, resulta das boas regras de conduta impostas por lei aos bancos (arts. 73º a 75º do RGICSF) que "o serviço de homebanking, como outros serviços de pagamento presenciais ou electrónicos prestados aos seus clientes, deve ser, não só de qualidade e eficiente, mas também serviço seguro (…)."

"Ao prestador dos serviços bancários cabe, pois, por lei assegurar a qualidade e segurança do sistema que permita movimentar a conta apenas a quem tem legitimidade, depositando, levantando ou transferindo fundos. O risco de funcionamento deficiente ou inseguro do sistema de prestação de serviços de pagamento ou transferência localiza-se, portanto, na esfera do seu prestador, a quem incumbe a responsabilidade por operações não autorizadas pelo cliente nem devidas a causa imputável ao cliente."

Por outro lado, o utilizador do serviço de pagamento tem de dispor de um conjunto de dispositivos de segurança (código de acesso, cartão matriz, etc.) que lhe vão permitir aceder a esse serviço.

Esses dispositivos de segurança personalizados têm uma função de autenticação (artº. 2º, al. t) do RJSPME) permitindo identificar o utilizador e verificar se este é efetivamente o cliente que contratou o serviço de homebanking (cfr. **Maria Raquel Guimarães,** i n **"A repartição dos prejuízos decorrentes de operações fraudulentas de banca electrónica, CDP 41-6**1").

E daí que se exija ao utilizador dos serviços que tome todas as medidas razoáveis em ordem a preservar a eficácia desses dispositivos de segurança personalizados.

Dispositivos de segurança personalizados esses que visam, assim, fundamentalmente evitar que terceiros consigam aceder, fraudulentamente, através do sistema, à conta do cliente utilizador do serviço de homebanking, logrando apropriar-se de fundos aí existentes.

É que (como se refere no citado **Ac. do STJ de 18/12/2013**) sendo a criptografia, apanágio do sistema,

porém, por si só, não elimina a possibilidade de ataques informáticos por hackers e a interceção 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 atuações 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.

E entre as técnicas de fraude informática mais comuns, visam essencialmente as instituições de crédito, encontra-se o **phishing** (do inglês fishing: pesca) que, grosso modo, consiste no envio de mensagens de correio eletrónico, que provêm aparentemente do banco prestador do serviço, tentando obter dados confidenciais que permitam o acesso ao serviço de pagamento eletrónico, e o **pharming,** que se consubstancia numa técnica mais sofisticada através da qual é corrompido o próprio nome de domínio de uma instituição financeira, redirecionando o utilizador para um site falso – em tudo similar ao verdadeiro – sempre que este digita no teclado a morada correta do seu banco, ou seja, através dessa técnica suplanta-se o sistema de resolução dos nomes de domínio para conduzir o usuário a uma pagina Web falsa, clonada da página real, ou melhor ainda, essa técnica baseia-se em alterar o IP numérico de uma direção 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., entre outros, **Pedro Verdelho**, in "**Phishing** e **outras formas de defraudação nas redes de comunicação, in Direito da Sociedade De Informação, Volume VIII, págs. 407/419"** e **Maria Raquel Guimarães,** in **"Ibidem"**)

Em tais situações de fraude informática - através das quais se realizam de operações de pagamento não autorizadas, resultantes da apropriação abusiva de instrumento de pagamento, com quebra da confidencialidade dos dispositivos de segurança personalizados - coloca-se a questão de saber quem deve ser responsabilizado pelas perdas daí resultantes?

A este respeito, decorre do disposto no artº .72º do RJSPME:

- se a situação (quebra da confidencialidade daqueles dispositivos de segurança) é imputável ao utilizador, ordenante, este suporta as perdas relativas a essas operações de pagamento dentro do limite do saldo disponível até ao máximo de €150 (nº. 1);

- se as perdas forem devidas a atuação fraudulenta ou ao incumprimento deliberado de obrigações previstas no artº. 67º, não é considerado o referido limite máximo, suportando o ordenante todas as perdas resultantes dessas operações (nº. 2);

- havendo negligência grave do ordenante, este suporta as perdas resultantes das referidas operações até ao limite do saldo disponível da conta, ainda que superiores a € 150 (nº. 3).

Porém, se tiver procedido à notificação a que alude o artº. 67º, nº 1 al. b), (comunicação ao banco da apropriação abusiva do instrumento de pagamento) o ordenante não suporta quaisquer perdas, salvo em

caso de atuação fraudulenta (nº. 4).

Aqui chegados, e tendo presentes todas as considerações de cariz teórico-técnico que se deixaram expendidas, é altura de avançarmos, de forma mais incisiva, para a resolução do caso em apreço, dando resposta à questão acima colocada.

Perscrutando a matéria factual apurada dela resulta que entre os dias 3 e 11 de janeiro de 2017 foram efetuados movimentos a débito nas contas bancárias tituladas pelos autores, através de transferências e pagamentos que não foram por eles ordenadas nem autorizadas, num total de €21.036,17 (relativamente às contas tituladas pelo autor) e num total de €9.954,01 (relativamente à conta titulada pela autora). (pontos 7 a 14).

Movimentos esses que foram efetuados através da utilização do serviço homebanking (M24) prestado pela ré e a que o autor tinha contratualmente aderido - no dia 22//12/2016 -, que lhe permitia o acesso online (via net) àquelas contas e movimentá-las e realizar diversas operações bancárias, tais como efetuar pagamentos e transferências, e que autorizava a ré a realizar essas operações através desse meio electrónico, tendo para o efeito esta entregue àquele todos os códigos e credenciais necessários para esse efeito, vindo este a ativar o cartão matriz em 03/01/2017 (cfr. pontos 60, 52, 54, 19, 20, 29, 32, 33, 34, 35, 40, 42, 43, 47 e 48).

Os acessos a tais operações em causa foram efetuadas através da Net24 (logon) com introdução de código de cliente e PIN (6 posições), e 128 posições do cartão matriz, todos correctos e à 1ª. tentativa, com exceção de uma situação ocorrida no dia 5 de janeiro de 2017 (às 03:20:35h), sendo que, passados 30 segundos, aproximadamente, foi efetuada nova tentativa, para a qual foram solicitadas as mesmas posições e na qual foram corretamente introduzidas as duas posições do cartão matriz, (cfr. pontos 52 e 53), sendo que tais movimentos apenas foram possíveis porque em cada um deles foi introduzido o número de identificação M...; o número de código Pin M24 e validado o Pin, tendo ainda sido introduzidas duas coordenadas e posições do cartão matriz, que são sempre solicitadas de forma aleatória pelo sistema e nunca repetidas. (cfr. ponto 63).

Perante tal factualidade afigura-se-nos ser patente que houve uma fraudulenta intromissão de terceiros nas contas dos AA., - através do sistema de serviços homebanking (M24) prestado pelo a ré e a que o A. havia aderido -, donde foram desviadas as importâncias acima referidas, tudo apontando que para o efeito foi utilizada a técnica informática (fraudulenta) designada por **phishing,** tendo sido utilizados os códigos e as credenciais que permitiam o acesso do A. esse serviço.

Sendo esses códigos/credenciais pessoais e intransmissíveis, foi, todavia, expressamente dado como não provado (cfr. ponto nº. 3 dos factos dados como não provados pelo tribunal a quo, e que não foi sequer objeto de impugnação) não só que fosse o A. que tivesse efetuado os aludidos movimentos (que sempre negou) como também que tivesse sido ele que forneceu a terceiros aqueles dados para o acesso ao serviço.

Como ressalta do plasmado nom citado artº. 70º, nº. 2, do RJSPME, nessas circunstâncias a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, por si só, não é necessariamente suficiente para provar não só que a operação de pagamento foi autorizada pelo ordenante, como também que este último agiu de forma fraudulenta ou sequer que não cumpriu,

deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do acima citado artigo 67º do mesmo diploma a que estava obrigado.

A única circunstância factual indiciadora que pode ter potenciado ou permitido o apoderamento por tais terceiros dos referidos códigos ou credenciais de acesso ao referido serviço por parte dos mesmos tem a ver com aqueles factos descritos nos pontos 23/24 e 49 dos factos e dos quais resulta que no dia 8 de Novembro de 2016, pelas 13h34, o autor recebeu no seu email j....com um email proveniente de "M... – pt", com o assunto: "Estimado, seu acesso ao Net24 pode ser suspenso. Regularize seu Utilizador" e que o autor, confiando tratar-se de um email fidedigno que lhe havia sido remetido pela ré, terá clicado sobre os dizeres "ACTIVAR CARTÃO MATRIZ", tendo seguido as instruções que lhe foram dadas.

Porém, esse facto, por si só isolado, não permite extrair conclusões seguras se foi esse facto que levou ao apossamento por terceiros dos referidos códigos/credenciais de acesso ao dito serviço que permitiu a movimentação de tais contas, e tanto mais que, e como se salienta na sentença recorrida, não podemos deixar de considerar a distância cronológica temporal decorrida entre esse procedimento (receção do email em 08/11/2016 – desconhecendo a data em que o A. fez nele clique, se foi nessa mesma data ou em outra qualquer posterior) e as datas posteriormente ocorridas de 22/12/2016, em que o autor veio só aí aderir ao referido sistema, e de 03/01/2017, em que só pelo 1ª. vez ativou o cartão matriz, ou seja, e por outras palavras, não ficou demonstrado o nexo de causalidade (adequado) entre tais procedimentos ou condutas que conduziram ao referido resultado.

Porém, mesmo que fosse esse o facto motivador do apossamento por estranhos dos referidos códigos/credenciais de aceso ao dito serviço que permitiu a movimentação de tais contas (o que, como vimos, não se mostra provado), tem-se vindo a entender que, pela própria natureza das coisas, não se pode qualificar a conduta de quem fornece credenciais de segurança sujeita a uma prática fraudulenta (vg. **"phishing"** ou **"pharming"**) como gravemente negligente. É que essas práticas fraudulentas são levadas a cabo porque um grande número de pessoas é ludibriado através delas e não apenas as extremamente descuidadas ou incautas; e para uma conduta poder ser qualificada como grosseiramente negligente ela não pode ser suscetível de ser levada a cabo por um número significativo dos homens médios, sendo certo que a negligência grave ou grosseira corresponde à falta grave e indesculpável, consistente na omissão de deveres a que sem está adstrito e que só uma pessoa especialmente desleixada, descuidada e incauta deixaria de observar. (cfr. **Ac. do STJ de 14/12/2016,** acima citado, **e Ac. da RC de 15/01/2019, proc. 5600/11.0TBLRA.C1,** disponível, tal como aquele, em dgsi.pt).

Desse modo, perante a matéria factual apurada, não é, a nosso ver, possível, concluir, sem hesitações, que no caso dos autos o acesso às contas dos AA., através do serviço homebanking prestado pela ré, e as movimentações nelas efetuadas com a retirada das importâncias acima aludidas, contra a sua vontade, se ficou a dever ao comportamento daqueles, e particularmente do autor, e nomeadamente que tal se tenha a ficado a dever a qualquer quebra por parte deste último da confidencialidade dos dispositivos de segurança que permitiam o acesso e a utilização desse serviço, ou a qualquer atuação fraudulenta do mesmo ou incumprimento deliberado das obrigações a que legal ou contratualmente estava obrigado, ou mesmo sequer a qualquer seu comportamento negligente, que tenha posto em causa a segurança do sistema.

Note-se ainda que só decorrido s cerca de 8 dias, sobre o início das mesmas, é que tais operações ilícitas

vieram a ser detetadas pelo banco.

E sendo assim, e dado que, como vimos (numa decorrência, quer dos conjugados artºs. 795º, nº. 1, do CC e 70º do RJSPME, quer mesmo da presunção de culpa consagrada no artº. 799º, nº. 1, do CPC), era sobre a ré que impendia o ónus dessa prova (vg. da culpa do A. pelo sucedido) - apontado nesse sentido vide os Acs. do STJ e da RC acima citados -, que não logrou fazer, pelo que deve a mesma assumir o risco e a responsabilidade decorrente desse serviço que contratualmente presta, e daí dever ser responsabilizada pela obrigação de reembolso aos AA./depositantes das sobreditas quantias que ilicitamente foram retiradas das suas contas e bem assim pelos demais danos (nestes caso não patrimoniais/morais) que sofreram com tal situação, acrescida do pagamento dos respetivos juros moratórios legais que foram peticionados e atribuídos na sentença recorrida.

Termos, pois, em que se decide negar provimento ao recurso e confirmar a sentença da 1ª. instância.

III- Decisão

Assim, em face do exposto, acorda-se em negar provimento ao recurso e confirmar a sentença da 1ª. instância.

Custas pela R./apelante (artº. 527º, nºs. 1 e 2, do CPC).

Sumário:

I- O contrato de conta bancária (correntemente também designado por contrato de abertura de conta) configura um acordo havido entre uma instituição bancária e um cliente através do qual se constitui, disciplina e baliza a respetiva relação jurídica bancária e ao qual se encontra indissociavelmente ligado o depósito bancário.

II- Com esse contrato - sendo dominantemente qualificado como contrato de depósito irregular, e ao qual aplicam, na medida da sua compatibilidade, as regras do mútuo- inicia-se toda uma relação jurídica complexa entre banco e cliente, no qual assentam, a ele estando associados, os mais diferentes contratos posteriormente celebrados entre ambos, mas em relação ao qual, todavia, assumem ou podem assumir-se como autónomos.

III- Entre esses contratos que se encontram associados à abertura de conta encontra-se o designado contrato de homebanking, que normalmente se concretiza através da possibilidade conferida pela entidade bancária aos seus clientes, mediante a aceitação de determinados condicionalismos, de utilizar toda uma panóplia de operações bancárias, on line, relativamente às contas de que sejam titulares, os quais têm vindo a obter um forte incremento e adesão pelas inegáveis vantagens que propicia às partes, quer aos clientes, permitindo-lhes um acesso mais rápido, continuado (sem limitação de horários) e cómodo (sem deslocações aos balcões) às suas contas e, desse modo, a realização das mais variadas operações; quer aos bancos, permitindo agilizar serviços e otimizar a gestão dos seus recursos humanos, com a inerente diminuição de custos.

IV- Tratando-se de serviços prestados via internet, os mesmos são frequentemente alvo de ataques dos designados hackers com objetivo de se apropriarem, de forma ilícita, dos fundos existentes nas contas bancárias.

V. De entre essas técnicas de fraude informática mais comuns, destacam-se o **phishing** que, grosso modo,

consiste no envio “ao cliente” de mensagens de correio eletrónico, que provêm aparentemente do banco prestador do serviço, visando obter dados confidenciais que permitam o acesso ao serviço de pagamento eletrónico, e o **pharming,** que se consubstancia numa técnica mais sofisticada através da qual é corrompido o próprio nome de domínio de uma instituição financeira, redirecionando o utilizador para um site falso – mas em tudo similar ao verdadeiro – sempre que este digita no teclado a morada correta do seu banco, ou seja, através dessa técnica suplanta-se o sistema de resolução dos nomes de domínio para conduzir o usuário a uma pagina Web falsa, clonada da página real, ou melhor ainda, essa técnica baseia-se em alterar o IP numérico de uma direção no próprio navegador, através de programas que captam os códigos de pulsação do teclado. o que pode ser feito através da difusão de vírus via spam, e que leva o usuário a pensar que está a aceder a um determinado site – por exemplo o do seu banco –, quando na realidade está a entrar no IP de uma página Web falsa.

VI- Os contratos de homebanking encontram a sua disciplina e enquadramento jurídico no Regime Jurídico dos Serviço de Pagamento e da Moeda Eletrónica (RJSPME), aprovado pelo DL nº. 317/2009, de 30/10, e do qual, e visando evitar que terceiros acedam fraudulentamente às contas bancárias, resultam, além do mais, um conjunto de deveres impostos tanto para o prestador dos serviços como para o seu utilizador, cuja violação é geradora de responsabilidade (vg. civil), sendo que no que concerne particularmente ao utilizador, e tendo daí resultado perdas/danos para si, a medida da sua reparação varia em função da sua atuação culposa.

VII- Negando o utilizador ter dado autorização para uma operação de pagamento que foi executado pela instituição bancária, é sobre esta que impende o ónus de prova de que a operação de pagamento não foi afetada por avaria técnica ou qualquer outra deficiência e/ou que esse pagamento só foi possível devido à atuação fraudulenta daquele ou ao incumprimento deliberado ou com negligência grave dos deveres/obrigações decorrentes do artº. 67º do RJSPME.

Coimbra, 2020/02/11

Fonte: http://www.dgsi.pt