jurisprudência.pt

Tribunal da Relação de Évora
Processo nº 3052/11.4TBSTR.E1

Relator: CRISTINA CERDEIRA
Sessão: 25 Junho 2015
Votação: UNANIMIDADE
Meio Processual: APELAÇÃO
Decisão: IMPROCEDENTE

OPERAÇÃO BANCÁRIA **HOMEBANKING**

FACTOS INSTRUMENTAIS **PRESUNÇÃO DE CULPA**

Sumário

I) - O serviço de home banking prestado por uma instituição bancária aos seus clientes envolve obrigações recíprocas: por um lado, o Banco tem o dever de garantir a segurança na implementação do sistema informático e de informar os clientes das regras de segurança a seguir na utilização do serviço e, por outro, o cliente utilizador obriga-se a cumprir determinadas condições de segurança na utilização daquele serviço, designadamente a manter a confidencialidade do número do contrato, do código e do cartão matriz.
II) - Considerando a complexidade dos sistemas bancários de home banking, concebidos e controlados pelos Bancos, assim como a grande exigência dos mecanismos relacionados com a segurança das operações bancárias através deles realizadas, a par da propriedade do Banco sobre os valores depositados pelos seus clientes, em ambiente contratual, deverá funcionar, neste caso, a regra da presunção de culpa estabelecida no artº. 799º, nº. 1 do Código Civil, nos termos da qual recai sobre o Banco depositário o ónus da prova de que a falta de cumprimento ou o cumprimento defeituoso da obrigação (correspondente a avarias técnicas ou outras deficiências que levaram à utilização fraudulenta daqueles meios) não procede de culpa sua.
III) - Em todo o caso, avultando neste tipo de contratos de home banking a obrigação de utilização correcta do serviço por parte do utente, o qual assenta em boa parte na não divulgação dos seus elementos de segurança e códigos de acesso, o Banco pode elidir aquela presunção, afastando a sua culpa ou demonstrando mesmo a culpa do cliente pela deficiente utilização daqueles

meios expeditos, designadamente, alegando e provando que o cliente beneficiário violou o contrato, divulgando na internet dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de hackers.
IV) - Os riscos da falha do sistema informático utilizado, bem como dos ataques cibernautas ao mesmo, têm de correr por conta do Banco, por a tal conduzir o disposto no artº. 796º, nº. 1 do Código Civil, desde que não tenha resultado provado que houve culpa por parte do cliente utilizador.
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 utilizador.
VI) - Por força da subscrição do serviço "Caixadirecta Online", o cliente do Banco obriga-se a manter a confidencialidade do número do contrato, do código de acesso (vulgo, password) e ainda do seu cartão matriz, respeitando, assim, regras básicas de segurança que se encontram disponíveis aos utilizadores quer através do guia de utilizador, quer das Condições Gerais do serviço, quer dos alertas e Recomendações de Segurança disponibilizadas logo aquando do acesso ao serviço onde são anunciadas/publicitadas tais regras de segurança.
VII) - Ao divulgar na internet a totalidade dos dados do seu cartão matriz – apesar dos vários alertas de segurança no site da Ré na internet, advertindo os utilizadores para não reproduzirem os elementos do cartão matriz, e de ter tomado conhecimento das Recomendações de Segurança constantes do "guia de utilizador" que lhe foi entregue e que também se encontram acessíveis no mencionado site - a Autora actuou ao arrepio do contrato de home banking a que aderiu e em violação de regras básicas de segurança nele previstas para a utilização do serviço "Caixadirecta Online", o que permitiu que terceiros se apoderassem dos seus elementos de segurança e assim lograssem aceder às contas bancárias tituladas pelas Autoras e efectuar operações fraudulentas.
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 home banking por violação das mais elementares regras de segurança impostas pelo mesmo, ilidiu a presunção de culpa prevista no artº. 799º, nº. 1 do Código Civil que sobre si impendia, pelo que não é responsável pela movimentação das contas bancárias de forma fraudulenta.
(Sumário elaborado pela Relatora)

Texto Integral

Acordam na Secção Cível do Tribunal da Relação de Évora

I. RELATÓRIO

BB e **CC** intentaram a presente acção declarativa, sob a forma de processo sumário, contra **Caixa Geral de Depósitos, S.A.** pedindo a condenação da Ré a pagar à A. BB a quantia de € 6 600,00 e à A. CC a quantia de € 6 780,00, acrescidas de juros de mora vencidos e vincendos até integral pagamento.

Para tanto, alegam, em síntese, que a A. BB é filha da A. CC e ambas são titulares de duas contas abertas na agência da Ré em Santarém, sendo a 1ª A. titular de uma conta à ordem e a 2ª A. titular de uma conta poupança à qual a A. BB tem acesso como se fosse sua titular.

As AA. aderiram ainda ao serviço denominado "Caixadirecta Online", celebrando um contrato de *"home banking"*, qualificado como contrato de adesão e, por isso, sujeito às cláusulas contratuais gerais e de defesa do consumidor.

A Ré atribuiu às AA. um cartão matriz de coordenadas com um elemento de identificação e um código secretos, que as AA. utilizavam para realizar as suas operações em *home banking*.

Em 22/08/2008, através do serviço "Caixadirecta Online", a conta à ordem titulada pela A. BB foi movimentada a débito na quantia de € 5 000,00 e em 23/08/2008, através do mesmo serviço, foi movimentada a conta poupança titulada pela A. CC na quantia de € 4 900,00, movimentos estes traduzidos em transferências bancárias que foram realizados com o desconhecimento e contra a vontade das AA., nunca por elas tendo sido autorizados, ordenados, ratificados ou consentidos.

Ao aperceber-se das transferências, a A. BB de imediato alertou a Ré para a existência das movimentações ilícitas ocorridas nas suas contas.

Referem, ainda, que foi devido a uma falha do sistema de segurança criado, implementado e mantido pela Ré que as AA. se viram desapossadas das quantias supra mencionadas, pelo que está aquela obrigada a indemnizá-las das quantias subtraídas acrescidas dos respectivos juros de mora.

Mais alegam que estes factos causaram nas AA. profunda mágoa, angústia e insegurança, danos cujo ressarcimento é ora peticionado e cujo quantitativo deverá ser fixado em € 1 000,00 para a A. BB e em € 1 300,00 para A. CC.

A Ré contestou, invocando a excepção da incompetência territorial do Tribunal e impugnando os factos alegados pelas AA., designadamente que as duas AA. tenham aderido ao serviço “Caixadirecta Online”, pois só a A. BB subscreveu este serviço.

Impugna, ainda, o facto de que as transferências possam ser imputadas a falhas do sistema da Caixa Geral de Depósitos, alegando que as referidas transferências só ocorreram porque foram introduzidos no sistema todos os elementos de segurança respeitantes à utilização do serviço (número do contrato, password e uma combinação aleatória de 3 números do cartão matriz) e que apenas devem ser do conhecimento do cliente subscritor deste serviço e de rigorosamente mais ninguém. Uma vez introduzidos correctamente esses elementos de segurança, a operação foi tida como legítima não levantando quaisquer suspeitas para a Ré.

Mais alega que a A. BB não cumpriu com as regras de segurança inerentes à utilização do serviço “Caixadirecta Online”, porquanto a mesma revelou na internet a totalidade das combinações de três algarismos que compõem o seu cartão matriz e demais elementos de segurança (número do contrato e código de acesso), como ela própria confessou na carta de 26/08/2008 endereçada à Ré.

A A. BB não respeitou as recomendações e alertas de segurança divulgados pela Ré no seu site e que estão disponíveis aos utilizadores do serviço imediatamente antes do acesso ao serviço e sempre em cada utilização deste, e que eram do seu conhecimento tanto mais que, aquando da subscrição do serviço “Caixadirecta Online” foi fornecido à A. um número de contrato, um código de acesso e um cartão matriz com um conjunto único de 64 combinações de números de 3 algarismos cada uma, que funciona como um elemento de segurança adicional para as operações realizadas no serviço online, elementos estes que são absolutamente pessoais, secretos e intransmissíveis, conforme consta das Condições Gerais do serviço que a A. assinou e que recebeu naquela altura.

As operações cujo ressarcimento é ora peticionado só foram possíveis porque a A. BB revelou o número do contrato, o código de acesso e a totalidade das 64 combinações de 3 algarismos cada um que compõem o cartão matriz, elementos estes confidenciais e que o utilizador sabe que não pode revelar.

A Ré deduziu, ainda, o incidente de intervenção provocada de **DD**, nos termos do artº. 325º, nº. 1 do anterior CPC, por ser o beneficiário das quantias

transferidas das contas bancárias das AA. para a conta de que o mesmo é titular na Caixa Geral de Depósitos, e sobre o qual a Ré terá direito de regresso caso se venha a demonstrar que as transferências se processaram de forma ilícita e que a Ré é responsável pelas mesmas.

O chamado não apresentou qualquer contestação.

Foi realizada audiência prévia e proferido despacho saneador, no qual foi julgada improcedente a excepção dilatória de incompetência do tribunal, se definiu o objecto do litígio e se enunciaram os temas de prova assentes e controvertidos, que não sofreram reclamações.

Procedeu-se à realização da audiência de discussão e julgamento, com observância do legal formalismo.

Após, foi proferida sentença que julgou a presente acção improcedente e, em consequência, absolveu a Ré do pedido.

Inconformadas com tal decisão, as AA. dela interpuseram recurso, extraindo-se das respectivas alegações as seguintes conclusões [transcrição]:

«a) As autoras CC e BB, ora recorrentes, intentaram a presente acção com processo sumário contra a ora recorrida C.G.D., pedindo que esta fosse condenada a pagar-lhes a quantia global de 13.380/00 €, acrescida de juros, na qual se compreende os danos patrimoniais e não patrimoniais, e juros.

b) A recorrida contestou alegando, em súmula, que o ilícito só ocorreu por negligência e falta de cuidado da recorrente BB.

c) Em face dos factos provados entendeu o douto tribunal a quo absolver a recorrida porque, em síntese, considerou ter-se verificado "*... o incumprimento por parte da Autora encontra-se ilidido a presunção de culpa prevista no art.º 799.°, n.º 1 do Código Civil, que corria contra a Ré.*".

d) O douto tribunal *a quo*, a 6. Dos Factos Provados, julgou como provado que, no que respeita à recorrente BB: "tendo-lhe sido entregue o "guia do utilizador", pré elaborado e não susceptível de negociação prévia, junto a fls. 15 e segs., e que se dá aqui por integralmente reproduzido."

e) Deu ainda como provado o douto tribunal *a quo* (7. Dos Factos Provados) que: "Do guia consta a seguinte recomendação de segurança "*Nunca forneça mais de 3 dígitos do cartão matriz, e apenas para validar operações por si solicitadas dentro dos serviços mobile ou internet Banking da Caixa.*"

f) Para adiante (37. e 38. dos mesmos Factos Provados) dar como assente que "À Ré (trata-se certamente de mero lapso material pois o douto tribunal *a quo* quereria dizer "Às Autoras) foram ainda entregues as condições gerais de fls. 70 e segs." e que "A Ré (repete-se aqui a observação anterior) tinha conhecimento das condições gerais que lhe foram entregues aquando da adesão ao serviço de *homebanking*, idênticas aquelas juntas a fls. 70 e segs.".

g) Para fundamentar a sua convicção o douto tribunal *a quo* remete para o depoimento da testemunha EE, funcionário da recorrida.

h) Tal depoimento ficou registado digitalmente no programa H@bilus Média Studio, no período compreendido entre as 12 horas e 30 minutos e 51 segundos e as 12 horas e 41 minutos e 26 segundos, com a refª 20131219123049-158401-65106.

i) Tal testemunha, contrariamente ao considerado pelo douto tribunal *a quo*, tem um depoimento marcado pela incerteza e insegurança, sendo certo que, inquirido aos factos refere expressamente que não se recorda se entregou, ou não, à recorrente BB as condições gerais do contrato de *homebanking*.

j) O depoimento desta testemunha pauta-se pelo mero relato dos procedimentos habituais com todos os clientes não recordando nada em concreto no que respeita à aludida recorrente.

k) Todo o depoimento desta testemunha, que fundamentou, em exclusivo, a convicção do douto tribunal *a quo*, é determinado pelo relato dos procedimentos normais e habituais de todos os clientes, sem nunca concretizar o que se teria passado com a recorrente.

l) Questionado pelo mandatário das recorrentes, ao minuto 8:44, se se recordava se as condições gerais haviam sido entregues à recorrente BB, respondeu:
08:46 - "*As condições gerais são entregues a todos os clientes*"
08:49 - Advogado das recorrentes: "*Isso é o procedimento normal*"
Testemunha: "*É o procedimento normal*"
Advogado: "*O que eu lhe pergunto é relativamente à Dra. BB*"
08:54 - Testemunha: "*Foi certamente entregue à Dra. BB*".
Advogado: "*Mas recorda-se ?*"
09:04 - Testemunha: "*Quer dizer ... isto foi em 2005 não tenho um conhecimento preciso mas foi seguramente porque eu não faço o contrato sem entregar as condições gerais.*"

m) Questionado pelo mandatário das recorrentes quanto ao local aonde havia sido celebrado o contrato, referiu a testemunha, após várias hesitações e após localizar temporalmente o seu local de trabalho (com isso evidenciando não se recordar do caso concreto), referiu ao minuto 09:25: "*Deve ter sido aqui na Caixa Geral de Depósitos, na agência em Santarém, não foi no BNU foi na agência da Caixa Geral de Depósitos.*"

n) Novamente questionado se se recordava da ocasião, confirmou, ao minuto 10:00, não se recordar.

o) Ora, tal depoimento, eivado pela vacuidade, incerteza e pouca clareza, não permitiria ao douto tribunal *a quo* dar por assente a matéria dos pontos 7. (ficando, em consequência, prejudicado o ponto 8.) 37. e 38. dos factos provados.

p) Em reforço de tal convicção - da insuficiência de prova para o efeito - cumpre ainda destacar que a recorrida foi incapaz de apresentar nos autos as cláusulas contratuais gerais devidamente assinadas pela recorrente BB.

q) Razão pela qual não pode o teor das mesmas ser oponível à recorrente já que, tratando-se de mero contrato de adesão, ou cláusulas contratuais gerais, em fase da insusceptibilidade de negociação prévia e da sua pré elaboração, deverá tal contrato ser apreciado à luz da lei das cláusulas contratuais gerais que exclui as cláusulas não comunicadas (artºs 8.º e 5.º Dec. Lei nº 446/85 de 25/10), impondo, neste caso, à recorrida o ónus da prova da comunicabilidade das cláusulas em crise.

r) Não tendo a recorrida logrado, efectivamente, produzir prova cabal e adequada de que comunicou à recorrente BB o clausulado contratual, não lhe é este oponível.

s) De entre toda a jurisprudência, que tende para a unanimidade, produzida a este respeito, cumpre destacar o Ac. STJ de 24.03.2011, in www.dgsi.pt.

t) Na sua p.i. alegaram as recorrentes que: "*As transferências em causa, pelos elevados e invulgares, naquelas contas, montantes movimentados e pela proximidade de datas, deveriam ter suscitado na ré fundadas suspeitas que, consequentemente, deveriam ter levado a mesma a recusar a realização de tais movimentos.*"

u) Constam dos autos os Docs. 4 e 5 juntos com a p.i. que consistem em extractos das aludidas contas.

v) O extracto referente à conta nº 2...930 **(Doc. 4)** reproduz os movimentos no período compreendido entre os dias 1 e 31 de Agosto de 2008 e o extracto referente à conta nº 0...365 **(Doc. 5)** reproduz os movimentos ocorridos entre 16 de Março de 2006 e 23 de Agosto de 2008.

w) A conta nº 2...930 **(Doc. 4)** apresenta os movimentos típicos de uma gestão familiar e doméstica, com saídas de reduzido valor destinadas ao pagamento das despesas domésticas comuns de qualquer família típica;

W.1) A conta nº 0...365 **(Doc. 5)** apresenta os movimentos típicos de uma conta exclusiva destinada ao aforro, ou seja, todos os movimentos nela registados ao longo dos anos de 2006/ 2007 e 2008 retratam depósitos sem que verifique um só levantamento, com excepção da transferência que configurou o acto ilícito.

x) Em qualquer das contas jamais se registou qualquer movimento a débito - levantamento, transferência ou pagamento de cheque - cujo valor fosse sequer aproximado dos valores das transferências que deram azo à presente acção.

y) Os movimentos em causa – transferências - configuraram operações verdadeiramente anómalas e, portanto, merecedoras de controlo adequado por parte da recorrida, tanto mais se atendermos à publicitação que esta última fazia dos seus serviços caracterizando os mesmos como "*... sistemas de verificação e prevenção de fraudes ...*" que permitem "*... identificar actividades online suspeitas, ajudando-nos a proteger online as contas dos clientes ...*" (15. Dos Factos Provados).

z) Acresce ainda o depoimento da testemunha FF, registado, cfr. acta, no programa H@bilus Média Studio, no período compreendido entre as 10:32:56h e as 10:43;30h, com a refª: 20131219103254-158401-65106, que ao minuto 6 e 52 segundos a instância do mandatário das AA. se "*As contas donde foram retiradas estas verbas eram contas que habitualmente faziam movimentos deste montante ou eram contas que faziam movimentos pequenos?*", respondeu:
- 06:58 - "*A conta ... era a conta onde caiam os vencimentos que nós temos da administração pública e que sistematicamente caiam lá, 22, 23, 24, à volta disso e era uma conta usada para a gestão ...*"
- 07:23 - Mandatário das AA. - "*22, 23, 24 está a falar do dia do mês?*";
- 07:25 - Testemunha - "*Do dia do mês ...*" "*E que caíam aí os dois vencimentos, o meu e o da minha esposa, e que servia para a gestão corrente da casa, ainda hoje serve para a gestão corrente da casa*".

Acrescentando ao 07:40 minuto - "*Portanto são levantamentos, dois depósitos maiores e os levantamentos são os 100, os 150, os 20, os 30, as compras nos supermercados, etc., etc. ... É uma conta que claramente tem uma gestão corrente da nossa vida mensal. Não há levantamento significativos aí. Nunca.*" Aos 08:02, refere ainda acerca da conta nº 0...365 **(Doc. 5)** "*Da conta poupança, aí é uma conta que a minha sogra tem e pontualmente, de vez em quando, com as suas poupanças, porque ela vive connosco, com as suas pequenas poupanças ia aumentando a conta, la aumentando lentamente a sua conta. Não tem movimentos.*"

aa) Os movimentos ilícitos efectuados nas contas das recorrentes assumem contornos de evidente anormalidade e que, em consequência, deveriam ter suscitado na recorrida profundas e fundadas dúvidas e suspeitas.

bb) Caso o sistema de segurança "implementado e anunciado" pela recorrida e que pugnava pela "*... utilização destes sistemas de verificação e prevenção de fraudes ...*" que "*... permite identificar actividades online suspeitas, ajudando-nos a proteger online as contas dos clientes*" correspondesse à verdade necessariamente que os actos ilícitos praticados nas contas das recorrentes haveriam de ter sido detectados, porque movimentos verdadeiramente anómalos para as contas em questão, e evitados.

cc) Tanto mais se atendermos ao facto dos ataques terem ocorrido às 22 horas e 18 minutos do dia 22.08.2008 e as 01 horas e 10 minutos do dia 23.08.2008 (40. Factos Provados).

dd) No curto espaço temporal de 3 horas as contas das recorrentes, que somente registavam pequenos movimentos, uma delas, e movimentos a crédito, na outra, viram-se desapossadas de perto de 10.000,00 €.

ee) Não obstante a evidente anormalidade da situação, o sistema de "*verificação e prevenção de fraudes*" utilizado pela recorrida que, segundo ela, "*permite identificar actividades online suspeitas*" e a ajuda "*a proteger online as contas dos clientes*", nada detectou como suspeito ou anómalo.

ff) Verificou-se, por isso, uma grave e evidente falha do publicitado sistema de segurança da recorrida.

gg) Sendo factos manifestamente relevantes para apreciação da culpa da recorrida C.G.D. deveria o douto tribunal *a quo* considerado tal factualidade como imputável à C.G.D.

hh) Tal não sucedeu.

ii) Ao desconsiderar essa factualidade essencial o douto tribunal a quo violou o disposto no art.º 608.º nº 2 do C.P.C. por omissão de pronúncia.

jj) Omissão essa que, a jusante, veio a repercutir-se negativamente na douta sentença ora sindicada.

kk) O douto tribunal *a quo* desconsiderou factos instrumentais, apurados no decurso da audiência de julgamento, que deveria ter considerado em face da sua importância para a descoberta da verdade e boa decisão da causa.

ll) Em face da presunção de culpa estabelecida no art.º 799.º n.º 1 do Código Civil, haveria a C.G.D. de ter provado, de forma cabal, que as "investidas" ilícitas às contas das recorrentes não se deviam a fragilidades ou falhas do sistema de segurança por esta implementado e que a robustez deste último era total e adequada à protecção das contas susceptíveis de utilização *online*.

mm) Para o efeito o tribunal haveria de ter atendido, não só aos factos essenciais alegados pelas pastas, mas também aos factos instrumentais emergidos da produção da prova em julgamento.

nn) Os poderes do tribunal de averiguação e de consideração de factos instrumentais ou complementares apurados, com respeito pelo contraditório, durante a instrução ou julgamento são hoje de vasta amplitude, atento, inclusivamente, o reforço do princípio do inquisitório e inserem-se no elenco de poderes/deveres do julgador estabelecidos, entre outros, nos artºs 5.º nº 2; 6.º e 602.º nº 1 do C.P.C.

oo) Tendo, como corálio final a produção de sentença que vise a verdade material e, com base nela, a boa decisão da causa, o julgador tem ainda o dever de, na fundamentação da sentença, indicar "... as ilações tiradas dos factos instrumentais e especificando os demais fundamentos que foram decisivos para a sua convicção; ... , compatibilizando toda a matéria de facto adquirida e extraindo dos factos apurados as presunções impostas pela lei ou por regras de experiência" (sublinhado nosso), art.º 607.º nº 4 do C.P.C.

pp) Nesse sentido, Ac. RP de 15.12.2010, Proc. 114/09.1TTGDM.P1, in http://biblioteca.mj.pt; Ac. STJ de 23.9.2003, Proc.03B1987, in www.dgsi.pt e Ac. RC de 12.3.2013, Proc. nº 2611/12.2T2AVR.C1, in www.dgsi.pt.

qq) No caso em apreço e com relevância para o apuramento da robustez ou eficácia do sistema de segurança implementado e gerido pela C.G.D. resultou ainda provado que, a partir de Novembro de 2009/ esta introduziu regras de

segurança que indiciam sobre as transferências e que impõem que estes movimentos com valor superior a 500,00 € sejam validados pelo titular da conta através de sms via telemóvel.

rr) A prova de tais factos foi clara e cabalmente produzida através dos depoimentos das testemunhas da própria C.G.D., nomeadamente:

rr.1) Do depoimento da testemunha GG registado no programa H@bilus Média Studio, no período das 11:03:34 horas e as 11:41:50 horas, refª: 20131219110332-158401-65106, que ao minuto 36 e 31 segundos, inquirido acerca da data da entrada em vigor deste novo processo e segurança, respondeu: "*Foi seguramente depois desta altura*", referindo-se às datas dos "ataque" às contas das recorrentes;

Do depoimento da testemunha HH registado no programa H@bilus Média Studio, no período das 11:48:19 e as 12:07:42 que, com a refª: 20131219114816-158401-65106, inquirida acerca dos montantes susceptíveis de serem actualmente transferidos somente com o cartão matriz e confirmando a redução do valor, respondeu, ao minuto 17 e 40 segundos, "com a matriz agora são 500,00 €". Inquirida pelo Sr. Juíz ao minuto 18:48 segundos: "Este sistema de funcionamento de sms já existia em 2008?", respondeu: "Não", e insistindo o Sr. Juiz: "Não existia de todo ou existia para um montante mais elevado?", respondeu: "Não existia de todo", Sr. Juiz: "Quando é que foi instituído?", testemunha: "Novembro de 2009".

Do depoimento de JJ, registado no programa H@bilus Média Studio, entre as 12:08:42 e as 12:29:56, com a refª: 2013121912084-158401-65106, com o seguinte teor:
14:50 - Advogado das AA - "Em 2008 isto (transferência ou operação fora do normal, atendendo aos movimentos da conta) fazia despertar um alarme?"
Respondeu testemunha - "Não".
Para acrescentar, ao minuto 15:20: "Foi a partir de Outubro de 2008 que implementamos este sistema de gestão de fraude à leí."
Ao minuto 16:28, afirmou esta testemunha: "No sistema que nós temos, nos temos pessoas permanentemente a monitorizar esse sistema e nós damos ordens para bloquear ou para cancelar um determinado contrato, mas nessa altura não." (sublinhado nosso).
A instâncias do Sr. Juiz ao minuto 16:50: "Hoje em dia para além do cartão matriz há ainda a inserção do sms. Esse sistema foi instituído em 2011".
Testemunha: "Creio que em Outubro de 2009".

ss) Em face da prova produzida parece indubitável que a recorrida CG.D., à data dos factos em apreço, não possuía ainda os procedimentos de segurança, que veio a implementar em 2009, e que lhe permitiria, caso os utilizasse, impedir as transferências ilícitas, não só porque o valor em si a isso obstava mas também porque, para os valores em questão, ficariam dependentes de validação por sms o que, obviamente, despertaria suspeitas nas recorrentes e, consequentemente, recusariam a aludida validação.

tt) Tais sistemas de segurança mostram-se por isso, indispensáveis para impedir operações idênticas àquelas de que as recorrentes foram vítimas.

uu) Os referidos factos, s.m.o., instrumentais deveriam ter sido considerados e compatibilizados com "... toda a matéria de facto adquirida ..." (art.º 607.º nº 4 do C.P.C.) para a sua análise critica que deveria ter conduzido à conclusão da falta de viabilidade do sistema de segurança implementado pela recorrida C.G.D.

vv) Atento o disposto no art.º 799.º nº 1 do Cód. Civil "*Incumbe ao devedor provar que a falta de cumprimento ou o cumprimento defeituoso da obrigação não procede de culpa sua.*"

ww) Entendeu o douto tribunal *a quo* que a recorrida C.G.D. havia ilidido a referida presunção já que se provou que a recorrente BB tinha revelado *"... na internet a totalidade das combinações de três algarismos que compõem o seu cartão matriz*" (23. Dos Factos Provados) o que, segundo o tribunal *a quo*, foi suficiente para desresponsabilizar a C.G.D.

xx) Decorre das regras de experiência comum que, jamais a recorrente BB, ou qualquer pessoa, forneceria dados pessoais de acesso às suas contas bancárias sem a convicção de que o fazia de forma segura.

yy) O sistema de segurança implementado e gerido pela recorrida C.G.D. apresentava falhas cuja colmatação posterior, pela criação de processos ulteriores como a validação via sms, veio reforçar.

zz) A existência de tais processos teria impedido o ilícito de que as recorrentes foram vítimas.

aaa) A publicação de que, *"... os serviços de Internet Banking da Caixa dispõe de sistemas de monitorização permanente que previnem e detetam tentativas de fraude ..."* e que a *"... utilização destes sistemas de verificação e prevenção de fraudes permite identificar actividades online suspeitas, ajudando-nos a*

proteger online as contas dos clientes", traduz uma falsidade pois os movimentos ilícitos e ofensivos das contas da recorrente não podiam deixar de suscitar fortes suspeitas.

bbb) Em 2008 - dados dos factos - a C.G.D. não fazia a monitorização online permanente das contas e actividades suspeitas, permitia transferências somente com matriz de valor dez vezes superior ao que passou a permitir a partir de 2009 e não possuía o sistema de validação por sms.

ccc) Tais factos, devida e cabalmente provados mas não considerados na douta sentença ora sindicada, são suficientemente demonstrativos da culpa da C.G.D. ou pelo menos, quando assim não se entenda, impedem que esta ilida a presunção que sob ela impende atento o referido 799.º nº 1.

ddd) Não deveria o douto tribunal *a quo* ter concluído pela ilisão da presunção de culpa da C.G.D.

eee) A mera e singela transferência para os utilizadores da adopção de comportamentos de segurança não pode corresponder ao complexo de segurança que deve salvaguardar os interesses e direitos desses mesmos utilizadores.

fff) A ser assim sempre se deveria perguntar qual seria, nesta matéria de segurança do sistema, a prestação da C.G.D.?

ggg) Se era somente sobre os titulares das contas e utilizadores do sistema *homebanking* que impendia o ónus de proteger as suas contas, não revelando dados pessoais, qual seria então, em concreto, a obrigação da C.G.D.?

hhh) Evidentemente que tais obrigações haveriam de transcender a mera veiculação das cautelas a ter pelos utilizadores.

iii) Foi que a própria C.G.D. que criou, *a posteriori*, mecanismos que permitiram tornar o sistema de segurança eficaz.

jjj) Mecanismos esses que, para além do programa de gestão de fraudes, consistiram na singela medida de reduzir para dez vezes menos a possibilidade de transferência somente com os dados do cartão matriz e na adoção de um sistema de validação por sms para operações de valor superior aos 500,00 €.

kkk) Se tais processos já estivessem em vigor e se a monitorização das contas fosse efectivamente realizada, os "ataques" de que as recorrentes foram vítimas não tinham produzido qualquer resultado.

III) Não se vislumbra, por isso, acertado a desresponsabilização da C.G.D. com fundamento na ilisão da presunção de culpa que sob ela impende.

Nestes termos e nos mais de Direito que V. Exas. não deixarão de doutamente suprir, alterando a matéria de facto conforme o proposto e considerando toda aquela que foi desconsiderada, deverá revogar-se a sentença ora recorrida, substituindo-a por outra que condene a recorrida Caixa Geral de Depósitos nos termos peticionados, assim se fazendo a costumada JUSTIÇA!»

A Ré contra-alegou, formulando as seguintes conclusões [transcrição]:

«1. Os nºs 37 e 38 da douta decisão de facto deverão ser corrigidos pelo Tribunal recorrido ao abrigo do preceituado no art. 614º nº 1 do CPC de forma que passem a ter a seguinte redacção: ***37.*** *À A. BB foram ainda entregues as condições gerais de fls. 70 e ss.* ***38.*** *A A. BB tinha conhecimento das condições gerais que lhe foram entregues aquando da adesão ao serviço homebanking, idênticas aquelas juntas a fls. 70 e ss.*;

2. Foi correctamente julgada a matéria constante dos pontos **7, 8, 37** e **38** da douta fundamentação de facto inexistindo qualquer fundamento válido para alterar a decisão; com efeito, as apelantes transcreveram apenas parte do depoimento da testemunha EE sendo que da restante parte do seu depoimento resulta que a apelante BB não poderia deixar de ter levado consigo as **condições gerais** porquanto é nelas que consta impresso o **número do contrato**, elemento este que é um dos elementos necessários para se poder aceder ao serviço Caixa Directa *on line*;

3. Ou seja: Sem o sobredito **número do contrato** a apelante não poderia nunca ter acedido à utilização do serviço Caixa Directa *on line*, e para dispôr desse elemento tiveram forçosamente que lhe ser entregues as **condições gerais**;

4. Sem embargo, mesmo que à apelante BB não tivessem sido entregues as **condições gerais** nunca a mesma poderia alegar desconhecer a **regra de segurança** nos termos da qual a CGD avisa que **não devem ser fornecidos mais do três digitos do cartão matriz e apenas para validar operações** (e não para mais nenhuma outra finalidade), regra esta que foi precisamente aquela que resultou violada pela apelante, atendendo à matéria que resultou

provada no ponto nº 6 da fundamentação de facto, que não foi impugnada pelas apelantes;

5. Carece de fundamento a argumentação segundo a qual "*a recorrida foi incapaz de apresentar nos autos as cláusulas contratuais gerais devidamente assinadas pela recorrente BB*", pretendendo-se daí concluir que as **condições gerais** do serviço Caixa Directa *on line* seriam inoponíveis à dita apelante; Com efeito, no ponto nº **38** da decisão de facto considerou-se provado que: A Ré tinha conhecimento das condições gerais que lhe foram entregues aquando da adesão ao serviço de **homebanking**, idênticas aquelas juntas a fls.70 e segs.;

6. Ou seja, a apelada fez prova que foram entregues à apelante BB as **condições gerais** do contrato Caixa Directa **on line**, e que as **condições gerais** que lhe foram entregues são idênticas àquelas que constam de fls. 70 e ss. dos autos;

7. Não assiste igualmente razão às apelantes quando invocam que não foi considerado pelo Tribunal que *as duas transferências em causa nestes autos, pelos seus elevados e invulgares montantes e pela proximidade das datas deveriam ter suscitado fundadas suspeitas que, consequentemente, deveriam ter levado a apelada a recusar a realização de tais movimentos* porquanto ficou demonstrado que as duas transferências em causa **apenas** foram efectuadas porquanto a apelante BB negligenciou à partida **regras de segurança** elementares à boa utilização do serviço Caixa Directa *on line*, que eram/deviam ser do seu conhecimento e que, não fora essa negligência jamais as transferências teriam sido concretizadas;

8. Por outro lado, ficou provado no nº **22** da douta fundamentação de facto - e este número da decisão de facto **não foi impugnado** pelas apelantes - que à data as transferências não se afigurariam como suspeitas para a Ré, pelo que aos sistemas de detecção da apelada nada pode ser imputado, pelo que há que concluir que o Tribunal analisou e decidiu esta matéria nada lhe havendo assim a censurar, mormente nos termos e para os efeitos previstos no art. 608º nº 2 do CPC.

9. Ao contrário do que vem defendido pelas apelantes a alegação de que a introdução do sistema SMS TOKEN como regra de segurança suplementar ao serviço Caixa Directa *on line* constituiu **não** um *facto meramente instrumental* mas sim um *facto essencial* à sua pretensão, em ordem a lograrem demonstrar que aquele serviço não oferecia à altura das efectivação das transferências todas as garantia de segurança aos utentes;

10. Cabia-lhes assim no cumprimento do **princípio dispositivo** alegar em sede própria - i.e. nos articulados - tal matéria, e não aguardar pela interposição deste recurso para agora vir alegar que o Tribunal *a quo* não considerou (como *facto meramente instrumental*) que se o SMS TOKEN tivesse sido introduzido pela apelada no serviço Caixa Directa *on line* à data das transferências estas não teriam sido concretizadas;

11. Depois, também não resulta sequer da prova testemunhal produzida - mormente das testemunhas mencionadas pelas apelantes no seu recurso - que este mecanismo suplementar de segurança (SMS TOKEN) já existisse à data da ocorrência das transferências; de facto todas elas foram unânimes em reconhecer que tal sistema **não existia** à data em que ocorreram as transferências em causa nestes autos, pelo que não existindo não poderia ser implementado pela apelada no serviço; o facto de as actuais medidas de segurança terem evoluído desde a data da ocorrência das transferências em causa não pode obviamente servir para avaliar ou aferir da bondade do sistema nem das regras de segurança que à altura a apelada disponibilizava aos utentes.

12. Não resultaram, assim, violados os preceitos normativos consignados nos artigos 5º nº 2, 6 e 602º nº 1 todos do CPC;

13. Incumbia às apelantes o ónus de alegar e demonstrar que foi por causa do alegado mau/deficiente funcionamento do serviço Caixa Directa *on line* providenciado pela apelada que as transferências a débito ocorridas nas suas contas se efectivaram;

14. Ora, o que resultou da prova produzida foi exactamente o inverso, conforme se constata dos pontos nºs 5, 6, 7, 9, 21, e 22 a 35 da douta decisão de facto, nos quais resultou provada matéria que inequivocamente aponta no sentido de a apelante BB ter violado regras básicas de segurança do serviço Caixa Directa *on line*;

15. Por força da subscrição do serviço Caixa Directa *on line* a apelante BB obrigou-se a manter a confidencialidade do seu número de cliente, do código de acesso (vulgo, *password*) e ainda do seu cartão de matriz, tendo resultado provado o incumprimento destas obrigações da apelante enquanto utilizadora do *homebanking*;

16. Provou-se assim que a apelante reproduziu integralmente a matriz do cartão porque tanto lhe foi pedido ao entrar no sítio da *internet* da apelada,

tendo igualmente resultado provado que esta jamais solicita seja em que circunstâncias for mais do que três dígitos desse cartão, e, ainda que o cumprimento deste elementar dever era/devia ser do conhecimento da aludida apelante porquanto seja no **guia de utilizador**, seja nas **condições gerais** do serviço seja nos **alertas** e **recomendações de segurança** disponíveis à apelante logo aquando do acesso ao serviço eram anunciadas/publicitadas tais regras de segurança;

17. Por outro lado as apelantes não lograram assim demonstrar que "A introdução da matriz do cartão resultou de deficiências de funcionamento do sistema que a Ré utiliza para prestar o serviço de *homebanking*, conforme decorre da **alínea d)** dos factos não provados.

Nesta conformidade deverá a douta sentença ser mantida na íntegra.

Assim se fará Justiça!»

O recurso foi admitido por despacho de fls. 315.

Colhidos os vistos legais, cumpre decidir.

II. FUNDAMENTAÇÃO

O objecto do recurso é delimitado pelas conclusões das respectivas alegações, sem prejuízo das questões de conhecimento oficioso, tendo por base as disposições conjugadas dos artºs 608º, nº. 2, 635º, nº. 4 e 639º, nº. 1 todos do Novo Código de Processo Civil (NCPC), aplicável “in casu” por a decisão sob censura ter sido proferida depois de 1/09/2013 (artº. 7º, nº. 1 da Lei nº. 41/2013 de 26/6).

Nos presentes autos, o objecto do recurso interposto pelas Autoras, delimitado pelo teor das suas conclusões, circunscreve-se à apreciação das seguintes questões:

I) - Questão prévia:

- Rectificação do erro material existente nos **pontos 37 e 38 da matéria de facto provada** da sentença recorrida;

II) - Impugnação da decisão sobre a matéria de facto:

1. Erro na apreciação da prova produzida;

2. Desconsideração de matéria de facto alegada e fundamental para a decisão da causa;

3. Desconsideração de factos instrumentais apurados no julgamento;

III) – Do afastamento da presunção de culpa estabelecida no artº. 799º, nº. 1 do Código Civil.

Na sentença recorrida foram considerados provados os seguintes factos [transcrição]:

«**1.** A Ré é uma instituição bancária que exerce profissionalmente a actividade bancária e dessa actividade aufere lucros.

2. A Autora BB é filha de CC.

3. A Autora BB é titular da conta de depósito à ordem n.º 2...930, aberta na agência da Ré de Santarém.

4. A Autora CC é titular da conta poupança n.º 0...365, igualmente titulada pela Autora BB.

5. A Autora BB aderiu ao serviço denominado "Caixadirecta Online", celebrando para o efeito o respectivo contrato de "*home banking*".

6. Tendo-lhe sido entregue o "*guia de utilizador*"*,* pré elaborado e não susceptível de negociação prévia, junto a fls. 15 e segs., e que se dá aqui por integralmente reproduzido.

7. Do guia consta a seguinte recomendação de segurança "*Nunca forneça mais de 3 dígitos do cartão matriz,* e *apenas para validar operações por si solicitadas dentro dos serviços mobile ou internet Banking da Caixa*".

8. Tal serviço permitia à Autora BB aceder a operações bancárias sobre as suas contas de depósito, nomeadamente, transferências, pagamentos, consultas, simulações, pedidos; tudo através da utilização de meios informáticos mormente da internet.

9. Para o efeito a Ré atribuiu à Autora BB um cartão matriz de coordenadas com um elemento de identificação e um código secretos.

10. A 22/08/2008, pelas 22:18, através do serviço "Caixadirecta online", a conta à ordem com o n.º 2...930, titulada em nome da Autora BB, foi movimentada a débito sob a designação "TRF CXDOL" (transferência caixa directa online), na quantia de € 5.000,00.

11. A 23/08/2008, pelas 1:10, através do serviço "Caixadirecta online", a conta de poupança com o número 0...365, titulada em nome da Autora CC, foi movimentada a débito sob a designação "TRF CXDOL" (transferência caixa directa online), na quantia de € 4.900,00.

12. Tais movimentos foram realizados com o desconhecimento e contra a vontade das Autoras, nunca por elas tendo sido autorizados, ordenados, ratificados ou consentidos.

13. Sendo as transferências realizadas por alguém cuja identidade ou identidades as Autoras desconheciam.

14. A Autora BB contactou por via telefónica a Ré em 25 de Agosto de 2008, pelas 18:35, avisando a Ré da realização de operações não consentidas.

15. No seu site a Ré anuncia que "*os serviços de Internet Banking da Caixa dispõe de sistemas de monitorização permanente que previnem* e *detectam tentativas de fraude*" e "*... utilização destes sistemas de verificação* e *prevenção de fraudes permite identificar actividades online suspeitas, ajudando-nos a proteger online as contas dos clientes.*"

16. Do site da Ré consta ainda: "*... os serviços de Internet Banking da CGD utilizam mecanismos de segurança através das tecnologias mais avançadas existentes no mercado.*"

17. A Autora BB é funcionária pública, detendo básicos conhecimentos de informática.

18. A verba referida em 10. corresponde a vários anos de poupanças da Autora.

19. A Autora CC é reformada, sem quaisquer conhecimentos de informática.

20. O acto ilícito de que foram vítimas as Autoras causou-lhes mágoa, angústia e insegurança

21. As transferências efectuadas só foram possíveis porquanto foram prévia e correctamente introduzidos no sistema todos os elementos de segurança

respeitantes à utilização do serviço Caixa Directa *on line,* designadamente número de contrato, password, e uma combinação aleatória de três números do cartão matriz.

22. À data as transferências não se afigurariam como suspeitas para a Ré.

23. Em data não concretamente apurada, mas por volta de Junho de 2008, a Autora BB revelou na internet a totalidade das combinações de três algarismos que compõem o seu cartão matriz.

24. A Autora procedeu a essa reprodução na sequência de solicitação que lhe surgiu quando pretendia aceder ao sítio da internet da Ré.

25. A Ré não efectuou tal solicitação à Autora.

26. A Ré tem vários alertas de segurança no seu sítio da internet advertindo os utilizadores para não reproduzirem os elementos da matriz do cartão.

27. Esses avisos já existiam aquando dos factos descritos em **23., 10. e 11..**

28. Foi a revelação referida em **23.** que permitiu o acesso de terceiros às contas debitadas.

29. Aquando da subscrição do serviço Caixa Directa online foi fornecido à A. na activação deste serviço um número de contrato, bem como um código de acesso (que são os elementos necessários para entrar no serviço Caixa Directa através de um computador - login -) e também um cartão matriz com um conjunto único de 64 combinações de números de 3 algarismos cada uma, que funciona como um elemento de segurança adicional para as operações realizadas no serviço Caixa Directa online.

30. Qualquer destes três itens (número de contrato, código de acesso e cartão matriz) são absolutamente pessoais, secretos, e intransmissíveis.

31. A CGD divulgava e divulga no seu site www.cgd.pt e que estão disponíveis ao utilizador imediatamente antes do acesso ao serviço e sempre em cada utilização deste.

32. Nas Recomendações de Segurança, acessíveis a qualquer utilizador do Caixa Directa online logo que faça o login e sob o título de "*MANTENHA A CONFIDENCIALIDADE DOS SEUS DADOS PESSOAIS*" consta expressamente que: "*... Mantenha sempre os seus códigos de acesso ao Caixa Directa on-line reservados. Não os divulgue nem mesmo* se *solicitado por pessoas que* se *identifiquem como colaboradores da CGD: Não os escreva de forma a poderem*

ser consultados por terceiros, nem os envie por correio electrónico (nem mesmo para si próprio) ..."

33. Ainda em sede das mesmas Recomendações de Segurança e sob o título de "*PROTEJA E PRESERVE* O *SEU CARTÃO MATRIZ*" a CGD avisa os utentes deste serviço que devem: "*Preservar a confidencialidade dos números contidos no cartão*" e ainda que: "*Deve ter sempre presente que a Caixa nunca solicita dados de segurança (códigos de acesso* e *cartão matriz) ou outro tipo de informação confidencial através de mensagens de e-mail, telefone, ou outro tipo de contacto. Nunca* se *deve responder a este tipo de solicitação porque* se *trata de fraude.*

Para ter a certeza de que está a aceder ao site Caixadirecta on-line, deve sempre aceder através do endereço https/caixadirecta.cgd.pt e *nunca através de links contidos em mensagens de email mesmo que estas tenham alegadamente origem na Caixa*".

34. Para que o utente do serviço Caixa Directa on-line, possa efectuar operações na(s) sua(s) conta(s) após fazer o login (mediante a introdução do nº de contrato e do código de acesso) é-lhe solicitada aleatoriamente pelo sistema uma (e apenas uma) das 64 possíveis combinações de 3 números que compõem o cartão matriz.

35. E só com tal indicação precisa e correcta se consegue validar a operação que se pretende realizar e realizá-la.

36. As duas transferências tiveram como destino a conta bancária titulada por DD, sendo a conta da Caixa Geral de Depósitos com o n.º 0...600.

37. À Ré foram ainda entregues as condições gerais de fls. 70 e segs.

38. A Ré tinha conhecimento das condições gerais que lhe foram entregues aquando da adesão ao serviço de *homebanking,* idênticas aquelas juntas a fls. 70 e segs.

39. Nos autos n.º 857/08.7TBSTR, do 1.º Juízo Criminal do Tribunal Judicial de Santarém, foi proferido acórdão de 25/09/2012, já transitado em julgado no qual o aí arguido KK foi condenado, pela prática de dois crimes de burla informática agravada, previsto e punido pelo art. 221.º, n.º l e 5, al. a), do Código Penal, na pena de (1) um ano e seis (6) meses de prisão por cada um, em cúmulo jurídico numa pena única de dois (2) anos de prisão.

40. No referido acórdão ficaram provados, entre outros, os seguintes factos:

"*1. Em Agosto de 2008,* o *arguido KK, por forma não apurada, obteve* os *códigos e credenciais de acesso, através do serviço Caixa Directa da Caixa Geral de Depósitos, relativos à conta bancária n.º 2...930, titulada por BB e FF, e relativos à conta n.º 0...365, titulada por BB e CC, ambas na Caixa Geral de Depósitos, agência de Santarém.*

2. Com tais informações, o *arguido decidiu aceder ao serviço disponibilizado na internet da Caixa Directa da Caixa Geral de Depósitos, e por essa via aceder às contas bancárias acima referidas utilizando para* o *efeito* os *respectivos códigos de acesso de que era conhecedor.*

3. Ainda em Agosto de 2008, o *arguido solicitou a DD que aceitasse receber na sua conta bancária cerca de 10 000,00* e, *referindo-lhe que iria receber tal quantia do seu pai que se encontrava no Brasil, e que posteriormente deveria levantar e proceder à sua entrega ao arguido.*

4. DD anuiu ao pedido formulado pelo arguido, e forneceu a este os *elementos bancários da conta com* o *n.º 0...600, de que é titular na Caixa Geral de Depósitos.*

5. *Na posse de tais elementos, no dia* 22 *de Agosto de 2008, às* 22 *horas e* 18 *minutos, em local não apurado,* o *arguido logrou aceder, pela internet e através do endereço IP número* 8...9, *pertencente ao "ISP (internet service provider) Telepac - Comunicações Interactivas, S.A.", ao serviço Caixa Directa da Caixa Geral de Depósitos e, por essa via, à conta bancária com* o *n.º 2...930, titulada por BB e FF na Caixa Geral de Depósitos, utilizando para* o *efeito* os *respectivos códigos secretos de acesso ao serviço.*

6. Na sequência desse acesso, o *arguido efectuou uma transferência no valor de* 5 *000,00 €, por débito da referida conta bancária e para crédito da conta bancária n.º 0...900, titulada por DD, utilizando uma vez mais* os *códigos que permitem debitar aquela conta bancária em tal montante.*

7. No mesmo dia o *arguido solicitou a DD que* o *acompanhasse e levou-o ao casino de Lisboa, onde DD, utilizando* o *cartão de débito da conta bancária de que é titular, procedeu ao levantamento da quantia total de 4 710,00 € que entregou ao arguido.*

8. No dia 23 *de Agosto de 2008, à 01 hora e 10 minutos, em local não apurado, o arguido logrou aceder, pela internet e através do endereço IP número 1...2, pertencente ao ISP (internet service provider) telesp celular, com sede no Brasil, ao serviço Caixa Directa da Caixa Geral de Depósitos e, por essa via, à*

conta bancária com o *n.º 0…365, titulada por BB e CC, na Caixa Geral de Depósitos, utilizando para* o *efeito* os *respectivos códigos secretos de acesso ao serviço.*

9. Na sequência desse acesso, o *arguido efectuou uma transferência no valor de 4 900,00 €, por débito da referida conta bancária e para crédito da conta bancária n.º 0…900, titulada por DD, utilizando uma vez mais* os *códigos que permitem debitar aquela conta bancária em tal montante.*

10. Na noite desse mesmo dia o *arguido solicitou a DD que* o *acompanhasse e levou-o ao casino de Lisboa, onde DD, utilizando* o *cartão de débito da conta bancária de que é titular, procedeu ao levantamento da quantia total de* 5 *190,00 € que entregou ao arguido, recebendo deste 50,00 € de gratificação.*"»

Por outro lado, na decisão recorrida foram considerados não provados os seguintes factos [transcrição]:

«**A.** A A. CC aderiu ao serviço denominado "Caixadirecta Online".

B. A quantia ilicitamente retirada da sua conta corresponde a mais de um terço de uma vida de poupanças.

C. As duas transferências a que se alude na p.i. tiveram como beneficiário o Sr. DD.

D. A introdução da matriz do cartão resultou de deficiências de funcionamento do sistema que a Ré utiliza para prestar o serviço de *homebanking.*»

*

Apreciando e decidindo.

I) - Questão prévia:

- Da rectificação do erro material existente nos **pontos 37 e 38 da matéria de facto provada** da sentença recorrida:

Como questão prévia à apreciação de fundo da primeira questão supra enunciada, e porque está correlacionada com a matéria de facto dada como provada pelo Tribunal “a quo”, afigura-se-nos existir nos “factos provados” constantes da sentença recorrida os seguintes lapsos de escrita, que se tornam manifestos em face da metodologia seguida pela Mª Juíza “a quo” na enunciação dos mesmos no capítulo da “fundamentação de facto” e que foram

assinalados pelas ora recorrentes nas suas alegações e pela recorrida nas suas contra-alegações, lapsos esses que importará corrigir, nos termos dos artºs 613º, nº. 2 e 614º "ex vi" do artº. 666º todos do NCPC, por forma a haver consonância entre a factualidade dada como provada e a motivação de facto inserida na sentença recorrida:

a) – no ponto 37 dos "factos provados", onde se refere *"À Ré foram ainda entregues as condições gerais de fls. 70 e segs."*, deverá constar "À A. BB foram ainda entregues as condições gerais de fls. 70 e segs.";

b) - no ponto 38 dos "factos provados", onde se refere *"A Ré tinha conhecimento das condições gerais que lhe foram entregues aquando da adesão ao serviço de homebanking, idênticas aquelas juntas a fls. 70 e segs."*, deverá constar "A A. BB tinha conhecimento das condições gerais que lhe foram entregues aquando da adesão ao serviço de *homebanking*, idênticas aquelas juntas a fls. 70 e segs.".

Tal evidência resulta do facto de ser desprovido de sentido que à Ré fossem entregues as condições gerais que ela própria criou e das quais obviamente tem de ter conhecimento por esse mesmo facto.

Por outro lado não ficou demonstrado que a A. CC tivesse aderido ao serviço "Caixadirecta Online", pelo que estes factos apenas se podem reportar à A. BB e não a ambas as AA. ora recorrentes.

Deverão, pois, na sentença recorrida, ser corrigidos os lapsos de escrita constantes dos pontos da matéria de facto provada acima enunciados e nos termos explanados.

*

Apreciemos, agora, a primeira questão suscitada no recurso interposto pelas Autoras.

I) - Impugnação da decisão sobre a matéria de facto:

(…)

2. Da desconsideração de matéria de facto alegada:

(…)

3. Da desconsideração de factos instrumentais apurados no julgamento:

Argumentam, também, as recorrentes que não foram considerados pelo Tribunal “a quo” factos instrumentais relevantes para a descoberta da verdade e boa decisão da causa, apurados no decurso da audiência de julgamento, mais concretamente com relevância para o apuramento da robustez ou eficácia do sistema de segurança implementado e gerido pela Ré CGD, a saber: o ter resultado provado que, a partir de Novembro de 2009, esta introduziu regras de segurança que incidem sobre as transferências e impõem que estes movimentos com valor superior a € 500,00 sejam validados pelo titular da conta através de um sms via telemóvel (o sistema “SMS TOKEN”).

Consideram as recorrentes que tais factos resultaram provados em face dos depoimentos das testemunhas GG, HH e JJ, dos quais transcrevem pequenos excertos, pretendendo dos mesmos concluir que, à data dos factos em apreço, a Ré CGD não possuía ainda os procedimentos de segurança, que veio a implementar em 2009, e que lhe permitiriam, caso os utilizasse, impedir as transferências ilícitas, não só porque o valor em si a isso obstava, mas também porque, para os valores em questão, tais operações ficariam dependentes de validação por sms o que, obviamente, despertaria suspeitas nas recorrentes que, assim, recusariam tal validação, considerando tais factos instrumentais em relação a toda a matéria de facto adquirida nos autos.

Conforme se alcança da “fundamentação de facto” constante da sentença recorrida, o Tribunal “a quo” fez uma correcta apreciação e análise crítica dos depoimentos das supra mencionadas testemunhas, conjugada com as regras da experiência comum, nos termos que passamos a transcrever:

«A convicção do Tribunal baseou-se ainda nos depoimentos, coerentes e espontâneos, das testemunhas GG e JJ.

A testemunha GG, funcionário da Ré, confirmou que das averiguações que efectuou a única causa que permitira o sucesso da operação de transferência foi a divulgação integral dos códigos e da matriz.

A testemunha JJ, Eng.º Informático da Ré, prestou um depoimento marcado por um profundo conhecimento técnico. Esta testemunha referiu que naquele período foram acompanhados vários sistemas de phising tradicional. A testemunha explicitou que o modo de funcionamento quer do phising quer do pharming dispensam qualquer contaminação do prestador de serviços, no caso a Ré, funcionando no computador do utilizador.

O modo de funcionamento do sistema de *homebanking*, resultou dos depoimentos das testemunhas, sendo unânimes em considerar que o sistema não funcionaria sem a introdução do número de contrato, do código de acesso e da combinação de três algarismos como operação de validação.

Neste particular, a testemunha JJ depôs ainda sobre os actuais sistemas de confirmação das operações, aos quais acresce a confirmação por código enviado por mensagem escrita para o telemóvel.

De facto, no caso a conclusão da causalidade mais próxima e adequada para que os códigos chegassem a KK (condenado do processo crime) será necessariamente a divulgação dos mesmos pela Autora BB. A proximidade temporal aliada à ausência de outra explicação plausível (furto, extravio ou problemas informáticos da Ré) levaram o Tribunal a considerar como provado que foi essa reprodução que permitiu as operações não autorizadas.

(…)

No que respeita aos avisos e alertas de segurança […] A testemunha HH, funcionária da Ré, prestou um depoimento coerente e espontâneo, merecedor da confiança do Tribunal. Esta testemunha, que desde de Maio de 2007 que exerce as funções de direcção de canais electrónicos, identificou os alertas de fraude disponíveis no site da Caixa Directa, que já existiam à data das transferências em causa nos presentes autos, e supra referidos.

A testemunha JJ, já descrita como credível, explicou que, para além da evolução do sistema de confirmação das operações, a Ré criou um sistema para evitar fraudes. Este sistema, criado em finais de 2008, permite automaticamente identificar operações suspeitas pelo seu montante, pelas horas a que são ordenadas, ou pelo local (IP) donde são emitidas as ordens de pagamento. À data dos factos a testemunha confirmou que as operações não suscitariam suspeita».

Ora, ouvida a gravação dos depoimentos destas testemunhas, constata-se que as mesmas confirmaram que a partir de determinada altura no ano de 2009 – em mês que não souberam precisar com exactidão - a Ré CGD adoptou o sistema SMS TOKEN como regra suplementar de segurança, tendo todas elas sido unânimes em reconhecer que tal sistema não existia à data em que ocorreram as transferências em causa nestes autos.

É um facto do conhecimento geral que as condições de segurança na utilização deste tipo de serviço evoluem no tempo à medida que as fraudes se

vão descobrindo e à medida que os contornos das mesmas se vão revelando, sendo certo que, por mais sofisticadas que as mesmas possam ser, nunca afastam a necessidade, por parte do utilizador, do estrito cumprimento de regras de segurança.

Aliás, foi referido pela testemunha GG, inspector no departamento de auditoria interna da CGD (e instrutor/analista do processo de averiguações que foi aberto na sequência da reclamação apresentada pelas AA.), que o sistema "Caixadirecta Online" existente em 2008 era seguro e que, não obstante estar actualmente implementado o sistema de SMS TOKEN, não existe nenhum sistema de segurança que funcione quando o próprio cliente não cumpre com as regras de utilização do serviço, como aconteceu com a A. BB neste caso concreto.

Confirmou, ainda, esta testemunha que foi a própria A. BB que lhe disse, no âmbito da investigação que levou a cabo que, para além do número do contrato e do código de acesso (password), a mesma terá facultado todos os dígitos constantes do seu cartão matriz na autenticação de acesso ao serviço (facto este, aliás, admitido por aquela A. na carta que dirigiu à Ré CGD em 26/08/2008 e junta a fls. 68 dos autos), o que levou a que a CGD concluísse ter havido incumprimento das normas de segurança estabelecidas para o serviço.

Assim, o facto das actuais medidas de segurança terem evoluído desde a data da ocorrência das transferências em causa não pode servir para avaliar ou aferir da bondade do sistema nem das regras de segurança que à altura a Ré disponibilizava aos clientes utilizadores do serviço.

Aliás, não se vislumbra que este facto possa ser qualificado como facto instrumental, como pretendem as recorrentes.

Tal facto sempre seria de considerar como um facto essencial para a demonstração da tese defendida pelas recorrentes, que é a da responsabilidade contratual da Ré/recorrida.

Com efeito, cabia às AA./recorrentes alegar em sede própria – isto é, nos articulados - e, posteriormente, em sede de produção de prova, demonstrar que a Ré não implementou todos os sistemas de segurança que à data dos factos já poderia ter implementado no serviço "Caixadirecta Online" que disponibilizava aos seus clientes.

Contudo, as AA. não cumpriram tal ónus, sendo certo que vigora, em sede de direito processual civil, o princípio do dispositivo segundo o qual cabe às

partes alegar os factos essenciais que constituem a causa de pedir e aqueles em que se baseiam as excepções invocadas (artº. 5º, nº. 1 do NCPC).

Assim, ponderando o conjunto de elementos probatórios constantes dos autos e enunciados na sentença recorrida, e considerando tudo o que atrás se deixou explanado, entendemos que bem andou o Tribunal "a quo" ao dar como provados os pontos 7, 8, 37 e 38 e ao fixar a matéria de facto nos termos que constam da sentença, contrariamente ao defendido pelas recorrentes, considerando-se definitivamente fixada a matéria de facto provada e não provada.

*

III) – Do afastamento da presunção de culpa estabelecida no artº. 799º, nº. 1 do Código Civil:

Insurgem-se as recorrentes contra o facto do Tribunal "a quo" ter considerado que a Ré CGD havia ilidido a presunção de culpa que sobre ela impendia por força do disposto no artº. 799º, nº. 1 do Código Civil (cfr, pontos 23 e 24 dos factos provados) e, por via disso, ter desresponsabilizado aquela pelo que aconteceu nas contas das recorrentes.

Partilhamos o entendimento da sentença recorrida ao considerar que o serviço de *home banking* prestado pela Ré e a que a A. BB aderiu, envolve obrigações recíprocas: por um lado, o Banco tem o dever de garantir a segurança na implementação do sistema informático e de informar o cliente das regras de segurança a seguir na utilização do serviço e, por outro, o cliente utilizador obriga-se a cumprir determinadas condições de segurança na utilização daquele serviço, designadamente a manter a confidencialidade do número do contrato, do código e do cartão matriz.

No que se refere ao contrato denominado de *home banking*, as operações de transferência electrónica de fundos realizadas através de um sistema de banca ao domicílio mostram-se actualmente reguladas no DL 317/2009 de 30/10, estabelecendo-se nos seus artºs 67º e 68º as obrigações do utilizador e do prestador do serviço.

Ora, considerando a complexidade dos sistemas bancários de *home banking*, concebidos e controlados pelos Bancos, assim como a grande exigência dos mecanismos relacionados com a segurança das operações bancárias através deles realizadas, a par da propriedade do Banco sobre os valores depositados

pelos seus clientes, em ambiente contratual, deverá funcionar “in casu” a regra da presunção de culpa estabelecida no artº. 799º, nº. 1 do Código Civil, nos termos da qual recai sobre o Banco depositário o ónus da prova de que a falta de cumprimento ou o cumprimento defeituoso da obrigação (correspondente a avarias técnicas ou outras deficiências que levaram à utilização fraudulenta daqueles meios) não procede de culpa sua.

Ou seja, a lei faz recair sobre o Banco o ónus da prova de que as operações de pagamento (nas quais se inserem as transferências bancárias) não foram afectadas por avarias técnicas ou por quaisquer outras deficiências, não bastando o registo da operação para, por si só, provar que a operação foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das obrigações decorrentes do artº. 67º no DL 317/2009 de 30/10.

E isto é assim pela simples razão de que o utilizador não podia ser colocado na necessidade de fazer prova sobre o funcionamento de um sistema informático complexo da entidade bancária e que não domina (cfr. acórdão da RL de 5/11/2013, proc. nº. 9821/11.8T2SNT, acessível em www.dgsi.pt).

Em todo o caso, avultando neste tipo de contractos de *home banking* a obrigação de utilização correcta do serviço por parte do utente, o qual assenta em boa parte na não divulgação dos seus elementos de segurança e códigos de acesso, o Banco pode elidir aquela presunção, afastando a sua culpa ou demonstrando mesmo a culpa do cliente pela deficiente utilização daqueles meios expeditos, designadamente, alegando e provando que o cliente beneficiário violou o contrato, divulgando na internet dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de *hackers* (cfr. acórdão da RG de 23/10/2012, proc. nº. 305/09.5TBCBT, acessível em www.dgsi.pt).

No caso em apreço não se provou qualquer incumprimento das obrigações da Ré. Ao invés, resultou provado o incumprimento das obrigações da A. BB, enquanto utilizadora do serviço de *home banking*. De facto, provou-se que a mesma reproduziu integralmente na internet a totalidade das combinações de 3 algarismos que compõem o seu cartão matriz, na sequência de solicitação que lhe surgiu quando pretendia aceder ao site da Ré na internet, tendo sido essa reprodução que permitiu o acesso de terceiros às contas das AA. e que levou à concretização das transferências bancárias.

Como é sabido, 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.

Na definição das técnicas utilizadas nesses ataques é particularmente útil o aresto do STJ de 18/12/2013, proferido no processo nº. 6479/09.8TBBRG, disponível em www.dgsi.pt:

"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, nº 41, 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 página 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".

Acolhemos a posição defendida na sentença recorrida no sentido de que, atentas as definições supra descritas e a factualidade provada, estamos perante um caso de *pharming*.

De facto, a situação surgiu à A. BB quando esta tentou abrir a página de internet da Ré, sendo a reprodução dos elementos confidenciais e a subsequente apropriação efectuadas em página da Web falsa e não através de email ao qual tenha respondido ou através do qual tenha acedido a um link.

Como é referido no supra mencionado acórdão do STJ de 18/12/2013, os riscos da falha do sistema informático utilizado, bem como dos ataques cibernautas ao mesmo, têm de correr por conta do Banco, por a tal conduzir o disposto no artº. 796º, nº. 1 do Código Civil, desde que não tenha resultado provado que houve culpa por parte do cliente utilizador.

Acontece que, contrariando o que deve ser tido por elementares regras de procedimento no acesso ao serviço *de home banking* e, em particular, à "Caixadirecta Online", resultou provado que a A. BB forneceu todas as combinações dos algarismos do seu cartão matriz de acesso às aludidas contas bancárias, por tal lhe ter sido pedido quando tentou abrir a página de internet da Ré.

Por outro lado, provado se mostra que a Ré jamais pediria tal informação na prestação daquele seu serviço, pois que a ser assim não faria sentido o fornecimento e a utilização do cartão matriz, que só existe para que se introduzam no serviço on line, a partir dele, determinadas variáveis, caso a caso, ou operação a operação, como é próprio daquele serviço e da segurança que lhe deve ser inerente. Aliás, como vimos, constitui contrapartida contratual do acesso ao serviço, que o aderente garanta a segurança dos elementos de identificação que lhe são fornecidos com confidencialidade, a título pessoal e intransmissível, o que implica que se coloque a salvo de todos os terceiros, incluindo os funcionários daquela ou de qualquer outra instituição de crédito.

Ao divulgar na internet a totalidade das combinações de 3 algarismos que compõem o seu cartão matriz, como se não existisse pirataria informática – apesar dos vários alertas de segurança no site da Ré na internet, advertindo os utilizadores para não reproduzirem os elementos do cartão matriz, e de ter tomado conhecimento das Recomendações de Segurança constantes do *"guia de utilizador"* que lhe foi entregue e que também se encontram acessíveis no mencionado site - a A. BB actuou ao arrepio do contrato de *home banking* a que aderiu e em violação de regras básicas de segurança nele previstas para a utilização do serviço "Caixadirecta Online", regras essas acessíveis à Autora, o que permitiu que terceiros se apoderassem dos seus elementos de segurança e assim lograssem aceder às contas bancárias tituladas pelas recorrentes e efectuar as transferências bancárias em causa nestes autos.

Com efeito, por força da subscrição do serviço "Caixadirecta Online", a recorrente BB obrigou-se a manter a confidencialidade do número do contrato, do código de acesso (vulgo, *password*) e ainda do seu cartão matriz, tendo, no entanto, resultado provado que a mesma reproduziu integralmente as combinações de 3 algarismos que compõem o seu cartão matriz, na sequência de pedido feito quando pretendia entrar no site da Ré na internet, tendo igualmente se provado que a Ré nunca solicita, seja em que circunstâncias for, mais do que 3 dígitos daquele cartão, devendo o cumprimento destas elementares regras de segurança ser do conhecimento da recorrente BB, quer através do **guia de utilizador**, quer das **Condições Gerais** do serviço, quer dos **alertas** e **Recomendações de Segurança** disponíveis aos utilizadores logo aquando do acesso ao serviço onde são anunciadas/publicitadas tais regras de segurança.

Tal como se sublinhou na sentença recorrida "*... A Autora não podia ignorar que não podia reproduzir integralmente a matriz, sendo esse o aviso de segurança mais frequente. Ao ser-lhe solicitado, o que aliás configurou com certeza uma operação demorada, o utilizador medianamente diligente recorria às linhas de apoio ou ao atendimento presencial"*.

Relacionado com esta matéria, o acórdão da RG de 25/11/2013, proferido no proc. nº. 2869/11.4TBGMR (acessível em www.dgsi.pt) concluiu que: "***Age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador"***.

Nesta conformidade, teremos de concluir que o comportamento da A. BB foi negligente, sendo censurável pois a mesma violou regras de segurança impostas pelo contrato de *home banking*, tendo sido este comportamento causa directa da movimentação das aludidas contas bancárias por terceiros.

A Ré, ao provar a culpa da A. BB na transmissão da totalidade dos dados do seu cartão matriz a terceiros, ilidiu a presunção de culpa prevista no artº. 799º, nº. 1 do Código Civil, aplicável a este contrato, sendo esta também a posição assumida (a nosso ver, bem) na sentença recorrida.

Assim sendo, não é a Ré responsável pela movimentação das contas de forma fraudulenta, porquanto a mesma se deveu a culpa exclusiva da A. BB, que não teve o cuidado devido ao executar o contrato a que estava vinculada, traduzida no fornecimento da totalidade dos dados do cartão matriz a terceiros.

Nestes termos, improcede o recurso de apelação interposto pelas Autoras, devendo manter-se a sentença recorrida.

III. DECISÃO

Em face do exposto e concluindo, acordam os Juízes da Secção Cível do Tribunal da Relação de Évora em julgar improcedente o recurso de apelação interposto pelas Autoras **BB** e **CC** e, em consequência, confirmar a sentença recorrida.

Custas pelas recorrentes.

Évora, 25 de Junho de 2015
(Maria Cristina Cerdeira)
(Maria Alexandra Moura Santos)
(António Manuel Ribeiro Cardoso)