jurisprudência.pt

Tribunal da Relação do Porto
Processo nº 747/12.9TJPRT.P1

Relator: ANA LUCINDA CABRAL
Sessão: 07 Outubro 2014
Número: RP20141007
Votação: UNANIMIDADE
Meio Processual: APELAÇÃO
Decisão: CONFIRMADA

HOME BANKING **CONTRATO DE CONTA BANCÁRIA**

RESPONSABILIDADE CIVIL DO BANCO SACADO

Sumário

I - O phishing, numa primeira etapa, consiste na apropriação de informações de outra pessoa (como nome, informações de conta e senha bancária), para serem utilizadas fraudulentamente nas fases seguintes da trama (transferências de numerários de contas correntes e aplicações financeiras.
O pharming é um ataque de phishing mais sofisticado sem o uso da "isca" (o e-mail com a mensagem enganosa). O vírus reescreve arquivos do PC que são utilizados para converter os endereços de Internet (URL´s) em números que formam os endereços IP (números decifráveis pelo computador.
Assim, um computador com esses arquivos comprometidos leva o internauta para o site falso, mesmo que este digite corretamente o endereço do site intencionado.
A mais sofisticada e perigosa forma de pharming é conhecida como "DNS (Domain Name System) poisoning" (traduzindo para o português, seria algo como "envenenamento do DNS"), por possibilitar um ataque em larga escala. Nessa modalidade, o ataque é dirigido a um servidor DNS, e não a um computador de um internauta isoladamente.
II - A factualidade em causa emerge da existência de um contrato de conta bancária (ou abertura de conta) celebrado entre o banco, ora Apelante, e o Apelado e um contrato de homebanking, telebanking ou e-Banking, o qual sendo autónomo do contrato de conta bancária com ele tem uma íntima ligação
Através deste segundo contrato o Autor passou a poder movimentar a sua

conta por meios de comunicação à distância e foi alvo de uma fraude electrónica – phishing - acima conceptualizada, da qual resultou a subtracção da quantia € 4.480,00 da sua conta bancária.
O Decreto-Lei nº 317/2009, de 30 de Outubro, que aprovou o Regime jurídico que regula o acesso à actividade das instituições de pagamento e a prestação de serviços de pagamento e resultou da transposição para a ordem jurídica interna da Directiva nº 2007/64/CE, do Parlamento Europeu e do Conselho, de 13 de Novembro, relativa aos serviços de pagamento no mercado interno, entrou em vigor em 1 de Novembro de 2009.
Tendo os factos ocorrido depois da entrada em vigor deste diploma é este o quadro legal do caso.
III - Pode-se afastar, sem qualquer hesitação, o dolo ou intencionalidade no comportamento do Apelado e mesmo uma negligência consciente ou culpa grave.
Também não incumpriu o Apelado os deveres que a lei ou contato lhe impunham, tendo ficado provado que, logo que teve conhecimento da fraude, comunicou-a ao Apelante.
No caso, era necessário que o Apelado fosse uma pessoa muito experiente e muito conhecedora do meio de navegação em ambiente eletrónico para que pudesse desconfiar do isco que lhe foi lançado nas circunstâncias provadas.
Ora o banco Apelante quando acorda com os cliente o serviço homebanking não lhes exige essas aptidões.

Texto Integral

Processo nº 747/12.9TJPRT
Juízos Cíveis do Porto 3ª Juízo Cível

Acordam no Tribunal da Relação de Lisboa

I - Relatório
Autor: B…, residente na Rua …, N.º .., ….-… Vila Nova de Gaia
Réu: C…, com sede na …, N.º .., ….-… Porto.
Pedido: condenação do Réu a pagar ao Autor a quantia de € 4.480,00 (quatro mil quatrocentos e oitenta euros) acrescidos de juros de mora legais desde a data em que o Autor se encontra desapossado indevidamente de tal quantia, ou seja, de 11 de Julho de 2011 e até efectivo e integral pagamento e de € 1.500,00 (mil e quinhentos euros) pelos danos não patrimoniais, acrescidos de juros desde a data da citação até efectivo e integral pagamento.

Foi proferida sentença com o seguinte dispositivo: “Nestes termos, julgo parcialmente procedente por provada a acção intentada por B… contra o C… e, consequentemente, condeno este a pagar ao Autor a quantia de € 4.480,00 (quatro mil quatrocentos e oitenta euros) acrescido de juros de mora, à taxa legal, contados desde 11 de Julho de 2011, até efectivo e integral pagamento.”

O C…, SA interpôs recurso, concluindo:
1. Deverão ser julgados provados os factos alegados pelo Recorrente nos arts. 22º e 23º da Contestação, o que deverá suceder em função da análise de toda a prova produzida nos autos, em especial pelo depoimento da testemunha D… a 22-01-2013 a partir das 14:19:21h, em especial a partir do sexto e sétimo minuto daquele.
2. Deverá ser julgado provado o facto alegado pelo Recorrente no art. 31º da Contestação, o que deverá suceder em função do depoimento da testemunha D… 22-01-2013, a partir das 14:19:21h, em especial a partir do 10º e 11ºminuto do seu depoimento.
3. Deverá ser alterado o teor do facto nº 35º da sentença recorrida que deverá passar a conter a seguinte redacção: "Desde Janeiro de 2011 o Banco avisou os seus clientes, através da página de Internet que nunca efectuava qualquer pedido de instalação de software pela internet e que não alterava os procedimentos de acesso sem prévio aviso aos clientes, bem como que nunca solicitava o código de multicanal, o nº de contribuinte ou qualquer outro documento de identificação na sua totalidade, nos termos constantes do documento junto aos autos a fls. 68- 69, cujo teor aqui se dá por inteiramente reproduzido”, o que é imposto pelo depoimento da testemunha D… a 22-01-2013, a partir das 14:19:21h, em especial a partir do 13º minuto do mesmo.
4. A ordem de transferência em discussão nos autos foi efectuada através da aposição de todos os códigos secretos de que só o Autor tinha conhecimento, pelo que ao executá-la o Banco Recorrente limitou-se a cumprir o que havia sido acordado e convencionado com o Autor no contrato de "utilização de meios de comunicação à distância", não existindo, nem tendo sido demonstrado, qualquer facto ilícito contratual ou legal, nem tão pouco qualquer acto culposo que possibilite a condenação do Recorrente.
5. Em função do convencionado entre Autor e Recorrente, demonstrando-se que a transferência bancária foi executada pela aposição dos códigos secretos do Autor de que apenas ele tinha conhecimento, é sobre o Autor que deve recair o ónus probatório de alegar e demonstrar que a mesma deveu-se a acto culposo do Banco e não a incúria sua.
6. O Autor instalou programas de dados nos seus dispositivos electrónicos, o

que fez em contravenção com os avisos e recomendações que eram efectuados pelo Banco Recorrente.
7. A instalação de dados nos seus dispositivos electrónicos possibilitou a divulgação de parte dos seus códigos pessoais a terceiros.
8. Agiu, assim, com culpa que contribuiu decisivamente para o dano em que veio incorrer, responsabilizando-o pelo mesmo.
9. Violou a sentença recorrida o disposto nos arts. 570º e 799º do Código Civil.

10. Como tal, deverá a sentença ser revogada e o Recorrente inteiramente absolvido do pedido contra si formulado,
Tudo como acto de elementar Justiça e de sã aplicação do Direito.
B… apresentou contra-alegações, sintetizando:
A) O M.mº Juiz "a quo" não podia deixar de decidir, como decidiu, atento ao pedido formulado e aos respectivos fundamentos;
O âmbito do recurso é fixado em função das conclusões das alegações e circunscreve-se às questões aí equacionadas - arts. 639.° e 640.°, n.º I al. b) e n.º 2 al. a) do CPC;
B) Questão Prévia: O Apelante interpôs recurso e do cotejo da peça processual, entende-se claramente que quis o Apelante C…, S.A., dessa forma interpor o recurso da sentença, antes de mais, coloca em crise a decisão sobre matéria de facto, mas não especifica quais os concretos meios probatórios, constantes do processo ou de registo ou gravação nele realizada, que impunham decisão diversa sobre pontos da matéria de facto impugnados, limitando-se a referir-se ao depoimento da testemunha D…, sem contudo transcrever qualquer passagem desse mesmo depoimento;
C) Em ordem a obter a revogação da douta sentença, o recorrente, indica factos que presume provados, nomeadamente a existência de culpa do recorrido, invocando que este forneceu a terceiros todos os códigos de acesso ao serviço de homebanking e que não constam da matéria de facto dada como provada, nem de qualquer matéria alegada no recurso, tentando subverter o processado;
D) Pelo contrário, o Autor/Recorrido logrou provar que tomou todas as providências que lhe eram exigidas e exigíveis ao caso em concreto.
F) Senão vejamos:
Do depoimento de E…, companheira do Autor e que com ele já vivia à data dos factos, que foi prestado de forma clara e concisa, apesar de não ter conhecimento de todos os factos o que ao Tribunal se mostrou credível, a testemunha referiu que "o Autor usava o serviço da internet do Banco Réu tendo-o usado por diversas vezes. Sabia que, por motivos de segurança, o Autor usava um código de acesso, cujos números a testemunha desconhecia e

desconhece.. - Declarações prestadas na audiência do dia 22/01/2013 entre as 09h.32m.30ss. e as 09h.59m.47ss, documentadas no cd de gravação da audiência de discussão e julgamento.
G) A testemunha referiu ainda que "em certa altura e pretendendo o Autor fazer um carregamento de telemóvel, fazendo uso do seu portátil (computador por ele usado) entrou no site do banco e a certa altura referiu à testemunha que lhe estava a ser pedido o número e modelo do telemóvel, tendo-lhe solicitado que a mesma o informasse quanto a este último, que a testemunha fez não lhe parecendo estranho uma vez que pretendia o Autor fazer o carregamento, precisamente para o telemóvel. Declarações prestadas na audiência do dia 22/01/20l3 entre as 09h.32m.30ss. e as 09h.59m.47ss, documentadas no cd de gravação da audiência de discussão e julgamento.
H) Mais, a testemunha F…, técnico de informático que dá assistência ao computador do Autor, referiu que: "instalei o antivírus, a configuração do antivírus e configuração da firewall no computador portátil do Autor. O portátil do C… tem antivírus AVG, tem firewall do Windows Vista, original, através do código inscrito no autocolante que vem colado na parte de trás do computador e do CD Key." - Declarações prestadas na audiência do dia 22/01/2013 entre as 10h.l7m.35ss. e as 10h.24m.36ss, documentadas no cd de gravação da audiência de discussão e julgamento.
I) Questionada a mesma testemunha se tal sistema antivírus era adequado e fidedigno, respondeu: "Sim, tem aversão integral do AVG para uso pessoal, versão utilizada por milhões de utilizadores em todo o mundo. É atualizada frequentemente e tem ativada a firewall." - Declarações prestadas na audiência do dia 22/01/2013 entre as 10h.l7m.35ss. e as 10h.24m.36ss, documentadas no cd de gravação da audiência de discussão e julgamento.
J) Quanto à matéria de Direito, a recorrente não indica como seria mister, o preceituado nas alíneas b) e c) do art.º 639.°, n.º 2 do CPC;
L) Mais uma vez, ao arrepio de qualquer fundamento e unilateralmente, o recorrente, como já é seu hábito, invoca factos que não têm qualquer suporte probatório no processado;
K) O Recorrente alega no seu recurso que avisou os clientes para cuidados a terem quando acediam ao banco pela via eletrónica, nomeadamente com a indicação dos códigos pessoais a terceiros e dizemos nós ainda bem que o fez, mas perguntamos, o que releva para os autos?
M) Ora, a verdade é que o comportamento pedido ao Autor, no site oficial do Recorrente, era distinto da introdução de um qualquer código ou do fornecimento deste a terceiro, ao Autor foi pedido que realizasse um download, tendo fornecido apenas a marca e modelo do seu telemóvel, o que atendendo a que o mesmo pretendia fazer um carregamento de dinheiro no

mesmo, não podia ao comum utilizador de um site bancário, parecer estranho, obrigando-o a conduta distinta da que adoptou.
N) Desta forma, dúvidas não restam que o recorrente labora em erro, tentando com o seu logro induzir o tribunal a concluir conforme lhe convém, para assim obter benefício patrimonial indevido, eximindo-se ao pagamento do que deve e muito bem sabe que deve ao Apelado, que se vê desapossada de milhares de euros há vários anos a esta parte, colocando as suas finanças, já depauperadas com toda a crise que afecta o nosso país, em situação extremamente difícil.
O) Em suma, o recurso apresentado pela recorrente deve ser liminarmente rejeitado por não preencher os requisitos legais.
P) A sentença recorrida encontra-se bem estruturada e fundamentada, apreciando correctamente as questões que se lhe impunha conhecer, decidindo em conformidade com o Direito aplicável, merecendo o acolhimento da recorrida, não merecendo pois, qualquer censura.
Nestes termos e nos melhores de Direito, não dando provimento ao recurso e mantendo-se a decisão recorrida, V. Exas. Farão, como sempre, JUSTIÇA.

Nos termos da lei processual civil são as conclusões do recurso que delimitam o objecto do mesmo e, consequentemente, os poderes de cognição deste tribunal.
Assim, a questão a resolver consiste em saber se, no caso, o Banco deve reembolsar o Apelado da quantia que lhe foi subtraída por fraude electónica ao utilizar o serviço homebanking

II – Fundamentação de facto.
A) O tribunal recorrido deu como provados os seguintes factos:
1.O Réu é uma instituição bancária que exerce profissionalmente a actividade bancária e dessa actividade aufere lucros;
2. O Autor celebrou com o Réu um contrato de depósito ao qual foi associada uma conta bancária com o n° ……., sediada num dos balcões do Réu na cidade do Porto, denominada agência ….
3. A 27 de Setembro de 2006, Autor e o Réu acordaram a utilização de meios de comunicação à distância, nos termos constantes do documento junto aos autos a fls. 91 a 93, cujo teor se dá aqui por integralmente reproduzido.
4.Para tal o Réu atribui ao Autor um elemento de identificação secreto e um código também secreto.
5.Adicionalmente sempre que o Autor pretendesse realizar um pagamento ou transferência remotamente, esta só se realizava após a introdução de um apelidado "Código de Autorização" composto por 6 (seis dígitos) que seria

enviado por mensagem escrita pelo Réu, onde constava também um breve descritivo do movimento a efectuar, para o número de telemóvel do Autor.
6.Para os efeitos do artigo anterior o Autor disponibilizou ao Réu o seu número de telemóvel.
7.No dia 8 de Julho de 2011 o Autor utilizando o seu computador portátil entrou no site oficial do Réu onde acedeu à área reservada relativa à sua conta utilizando para o efeito o elemento de identificação secreto e o código também secreto que o Réu lhe disponibilizou.
8.Com o intuito de efectuar um carregamento de saldo do seu telemóvel.
9.Durante a supra citada operação surgiu no ecrã uma mensagem que indicava que o Autor deveria efectuar o download de uma aplicação para o telemóvel, e onde faltava preencher dois campos relativos à marca e modelo do telemóvel, os quais o Autor preencheu com a informação correspondente.
10.Posteriormente o Autor recebeu no seu telemóvel uma mensagem escrita com vista a efectuar um download".
11.O Autor efectuou o download da aplicação.
12.Uns dias depois, o Autor utilizando o seu computador portátil entrou novamente no site oficial do Réu onde acedeu à área reservada relativa à sua conta e verificou que tinha sido feita uma transferência bancária no valor de €4.480,00 (quatro mil quatrocentos e oitenta euros) nesse mesmo dia.
13.Transferência que não autorizou e nunca teve intenção de fazer. 14.0 Autor contactou de imediato o número de assistência ao cliente do Réu expondo a situação e solicitando de imediato a devolução da quantia, tendo sido informado não ser possível o cancelamento da transferência.
15.No dia 13 de Julho de 2011, o Autor apresentou no Banco Réu a pedido junto aos autos a fls. 13, cujo teor se dá aqui por integralmente reproduzido.
16.A 14 de Julho de 2011, o Autor apresentou no balcão do Padrão do Banco Réu a reclamação de fls. 15 e 16, cujo teor se dá aqui por integralmente reproduzido.
17.Na Polícia Judiciária, Directoria do Norte, foi registado inquérito com o n° NUIPC: 299/11-7 GFVNG, em que foi participante o ora Autor, relativo a crime informático sobre a conta bancária n° ..... do Banco ora Réu.
18.A falta da quantia referida em 12) acarretou para o Autor algumas dificuldades económicas, tendo de pedir dinheiro a terceiros.
19.O Autor ficou transtornado.
20.O Autor, através do serviço referido em 27) desfrutou de um acesso mais continuado, mais rápido e mais fácil com disponibilidade acrescida de fundos e a possibilidade de realização de outras operações, bem como obtenção de uma gama mais vasta de serviços de forma mais cómoda.
21.0 Banco assegura, como não podia deixar de ser, a segurança do serviço de

Internet prestado, assegurando a fiabilidade da sua página de internet e a confidencialidade e segurança dos dados e património dos seus clientes, no que se refere aos seus servidores e componentes informáticos.
22.Tem sido difundidas nos órgãos de comunicação nacional notícias da ocorrência de fraudes e crimes a ocorrerem na internet em data anterior e posterior à celebração do contrato alegado pelo Autor.
23.Quem utiliza internet deve instalar antivírus e firewall no seu computador.
24.O Banco, já antes do ano de 2011, recomendava no seu sítio de Internet, com o endereço www.C....pt que os utilizadores desses serviços de Banca na Internet deviam: "Ao aceder a C....pt, introduza os Códigos Pessoais, apenas em zonas encriptadas do site. Esta zona é definida pela indicação https://www.C....pt na barra de endereço do browser, antes do nome da página que está a aceder, e pela existência de um "cadeado".
25.O Banco em Outubro de 2010, publicou no seu sítio da internet, as regras de segurança inscritas no documento junto aos autos a fls. 52, cujo teor se dá aqui por integralmente reproduzido.
26.O Banco avisava ainda os seus clientes que: "C....pt nunca lhe solicitará, em situação alguma, em simultâneo mais de 3 dígitos do seu Código Multicanal, pelo que qualquer pedido nesse sentido constitui uma tentativa de fraude e deverá ser reportada para: .....", que "nunca forneça a terceiros os códigos de autorização recebidos por SMS ou obtidos via ..." e que "em caso de dúvida, confirme a origem do certificado digital - duplo clique sobre o cadeado - e verifique se corresponde efectivamente ao C...".
27. O Banco avisou os seus clientes, em altura precedente a Junho de 2011, da existência de fraudes na Internet através da solicitação indevida dos códigos de acesso pessoais por terceiros em computadores infectados.
28.Bem como, da necessidade dos seus clientes instalarem um antivírus e actualizá-lo, utilizar uma firewall e instalar restantes actualizações de segurança.
29.O Banco elaborou a newsletler junta aos autos a fls. 60 a 66, cujo teor se dá aqui por integralmente reproduzido.
30.No dia 11 de Julho de 2011 foi efectuada transferência por débito da conta depósitos à ordem do Autor no valor de € 4.480,00 a favor do NIB ..... em nome de G....
31.A referida operação bancária foi efectuada através da utilização das credenciais do Autor, nomeadamente do código de utilizador "....", três posições do código multi canal que lhe havia sido exclusivamente atribuído e validada com código de autorização, previamente enviado por SMS para o telemóvel associado com o n° ..... que o Autor havia fornecido ao Banco.
32.Todos os dados pessoais acima referidos foram obtidos pelo Autor junto do

Banco mediante a subscrição do acordo referido em 3), sendo do seu exclusivo conhecimento.
33.A partir daquele momento só o cliente, no caso o Autor, poderia alterar o código de utilizador como o multicanal no sítio de internet do Banco.
34.O Banco cumpriu a ordem recebida e certificada pela aposição daqueles códigos.
35.Em Maio de 2012, o Banco avisou os seus clientes, através da página de Internet que nunca efectuava qualquer pedido de instalação de software pela internet e que não alterava os procedimentos de acesso sem prévio aviso aos clientes, bem como que nunca solicitava o código de multicanal, o n° de contribuinte ou qualquer outro documento de identificação na sua totalidade, nos termos constantes do documento junto aos autos a fls. 68- 69, cujo teor se dá aqui por integralmente reproduzido.
B) Impugnação da matéria de facto
Diz a Apelante que deverão ser julgados provados os factos alegados nos arts. 22º e 23º da sua contestação, o que deverá suceder em função da análise de toda a prova produzida nos autos, em especial pelo depoimento da testemunha D… a 22-01-2013 a partir das 14:19:21h, em especial a partir do sexto e sétimo minuto daquele.
Também deverá ser julgado provado o facto do art. 31º da sua contestação, o que deverá suceder, defende, em função do depoimento da testemunha D… a 22-01-2013, a partir das 14:19:21h, em especial a partir do 10º e 11ºminuto do seu depoimento.
Mais, aduz, deverá ser alterado o teor do facto nº 35 da sentença recorrida que deverá passar a conter a seguinte redacção: "Desde Janeiro de 2011 o Banco avisou os seus clientes, através da página de Internet que nunca efectuava qualquer pedido de instalação de software pela internet e que não alterava os procedimentos de acesso sem prévio aviso aos clientes, bem como que nunca solicitava o código de multicanal, o nº de contribuinte ou qualquer outro documento de identificação na sua totalidade, nos termos constantes do documento junto aos autos a fls. 68- 69, cujo teor aqui se dá por inteiramente reproduzido, o que é imposto pelo depoimento da testemunha D… a 22-01-2013, a partir das 14:19:21h, em especial a partir do 13º minuto do mesmo.
Vejamos os artigos da contestação:
22. O Banco e a sua página de internet não foram infectados com qualquer vírus ou outro programa malicioso que tenha dado origem aos factos descritos na petição inicial, em especial sob os arts. 4 e ss. Petição.
23. O Banco e a sua página de internet não tiveram qualquer quebra de segurança, nem foram infectados com qualquer tipo de programa malicioso no

dia 08.07.2011 ou 11 de Julho do mesmo ano, ou em qualquer outro, que permitisse que os dados e informações do Autor ficassem disponíveis para terceiros.
31 - Como se verifica do que o Autor alega, previamente ao dia 11/07/2011 e à transferência descrita na Petição, o Autor - inadvertidamente ou não - cedeu os dados e códigos pessoais e intransmissíveis acima referidos a terceiros e instalou software malicioso no seu telemóvel.
Quanto à matéria dos artigos 22º e 23º da contestação, verteu-se na motivação de facto da sentença que a testemunha D… disse que o Banco nunca foi alvo de pirataria pois que o alvo de pirataria são os clientes quando usam computadores e software malicioso. No entanto, a mesma não conseguiu demonstrar que, no caso sub judice, o Autor não tivesse as cautelas necessárias ao introduzir os dados que lhe foram pedidos.
Ora, esta é uma conclusão que se retira de uma análise às técnicas de obtenção não autorizada de elementos de identificação do utilizador de homebanking: normalmente, como no caso, não é a loja virtual do Banco que é o alvo de pirataria mas sim os clientes e o seu software.
Como conclusão dedutiva não deve constar da factualidade considerada provada.
No que concerne ao artigo 31º da contestação, se o Autor, inadvertidamente ou não, cedeu os dados e códigos pessoais e intransmissíveis acima referidos a terceiros e instalou software malicioso no seu telemóvel, é matéria conclusiva a extrair da descrição factos concretos.
A propósito da pretendida alteração do ponto 35º da sentença, dir-se-á que os factos em causa constam dos pontos 24º a 29º da sentença.
Não há, pois, motivo para modificar a matéria de facto da sentença.

III – Fundamentação de direito.
O discurso dos acontecimentos pode resumir-se assim:
O Autor, no âmbito dos serviços de homebanking contratados com o réu, iniciou uma operação de carregamento do saldo do seu telemóvel. Durante essa operação surgiu no ecrã do seu computador uma mensagem que indicava que que deveria efectuar o download de uma aplicação para o telemóvel, e onde faltava preencher dois campos relativos à marca e modelo do telemóvel, os quais o Autor preencheu com a informação correspondente. Posteriormente o Autor recebeu no seu telemóvel uma mensagem escrita com vista a efectuar um download e efectuou o download da aplicação.
Os conceitos de que agora nos vamos ocupar encontram-se bem definidos e com clareza invulgar no estudo do juiz brasileiro, Demócrito Reinaldo Filho, A responsabilidade dos bancos pelos prejuízos resultantes do phishing, acessível

em jus.com.br/artigos/11481/a-responsabilidade-dos-bancos-pelos-prejuizos-resultantes-do-phishing.
Seguiremos, pois, de perto este estudo.
O termo phishing, uma derivação do verbo inglês fishing (pescar), é utilizado para designar alguns tipos de condutas fraudulentas que são cometidas na rede.
O phishing, numa primeira etapa, consiste na apropriação de informações de outra pessoa (como nome, informações de conta e senha bancária), para serem utilizadas fraudulentamente nas fases seguintes da trama (transferências de numerários de contas correntes e aplicações financeiras). O criminoso apodera-se da informação de outra pessoa, sem o conhecimento desta, que é enganada de forma fraudulenta. Nesse sentido, o phishing pode ser enquadrado naquilo que se designa "furto de identidade" (identity theft), que é a expressão utilizada para denominar de forma genérica o crime de maior tendência ao crescimento nos tempos actuais. O furto de informações pessoais pode ser realizado com as mais diversas finalidades, tanto para imigração ilegal, espionagem, terrorismo ou mesmo para fins aparentemente menos ilícitos, como o marketing e publicidade dirigida. As estratégias para a apropriação dos dados pessoais também podem variar, com a utilização de meios tecnológicos ou não. Os dados podem ser obtidos em sites e bancos de dados informáticos ou em qualquer arquivo físico ou fichário. Mas consiste sempre numa exploração dos meios de identificação de uma pessoa para finalidades ilegais. O phishing, como espécie de furto de identidade, apenas tem a peculiaridade de ser realizado em ambientes de redes informáticas (Internet) e objetivar o furto de informações específicas (dados bancários), para finalidades também específicas (transferência de numerário existente em contas bancárias). Diversos esquemas inteligentes são empregados para burlar a vítima do phishing (e apoderar de suas informações bancárias) - que pode ter o seu computador invadido-, a ser levada a ingressar em site falseado através de link em mensagem eletrónica recebida ou porque o seu programa navegador está infectado (levando-a a um endereço diverso do site legítimo, mesmo sem receber qualquer tipo de e-mail). São muito comuns as mensagens eletrónicas (e-mails) onde são feitas propagandas de pechinchas comerciais, não solicitadas. Geralmente, o destinatário é convidado a clicar sobre um link que aparece no corpo da mensagem ou a abrir um arquivo anexo e, ao fazê-lo, acciona o download de um programa malicioso que vai penetrar no seu computador e capturar informações sensíveis. Ocorre também que, ao clicar no link sugerido, é enviado para um site falso, com as mesmas características de apresentação gráfica de um site popularmente conhecido (por exemplo do site um grande banco ou um site de comércio eletrónico). Ao chegar ao site

falseado, a pessoa é instada a inserir informações pessoais (número de cartão de crédito ou de conta bancária) e, uma vez de posse dessas informações, o fraudador utiliza-as para fazer saques e movimentações.
O phishing é, portanto, uma modalidade de spam, em que a mensagem além de indesejada é também fraudulenta (scam).
Outra modalidade de ataque que não é perpetrada através do envio de mensagens de e-mail é o pharming. Trata-se de um tipo de golpe que redireciona os programas de navegação (browsers) dos internautas para sites falsos.
O pharming opera pelo mesmo princípio do phishing, ou seja, fazendo os internautas pensarem que estão a aceder a um site legítimo, quando na verdade não estão. Mas ao contrário do phishing, o qual uma pessoa mais atenta pode evitar simplesmente não respondendo ao e-mail fraudulento, o pharming é praticamente impossível de ser detectado por um utilizador comum da Internet, que não tenha maiores conhecimentos técnicos. Nesse novo tipo de fraude, os agentes criminosos valem-se da disseminação de softwares maliciosos que alteram o funcionamento do programa de navegação (browser) da vítima. Quando esta tenta aceder a um site de um banco, por exemplo, o navegador infectado redireciona-a para o spoof site (o site falso com as mesmas características gráficas do site verdadeiro). No site falseado, então, ocorre a recolha das informações privadas e sensíveis da vítima, tais como números de cartões de crédito, contas bancárias e senhas.
No crime de pharming**,** a vítima não recebe um e-mail fraudulento como passo inicial da execução, nem precisa clicar num link para ser levada ao site falso, uma vez infectado o seu computador pelo vírus, mesmo teclando o endereço correto do site a que pretende aceder, o navegador leva-o diretamente para site falseado**.**
O pharming é, pois, um ataque de phishing mais sofisticado sem o uso da "isca" (o e-mail com a mensagem enganosa). O vírus reescreve arquivos do PC que são utilizados para converter os endereços de Internet (URL´s) em números que formam os endereços IP (números decifráveis pelo computador Assim, um computador com esses arquivos comprometidos leva o internauta para o site falso, mesmo que este digite corretamente o endereço do site intencionado.
A mais sofisticada e perigosa forma de pharming é conhecida como "DNS poisoning" (traduzindo para o português, seria algo como "envenenamento do DNS"), por possibilitar um ataque em larga escala. Nessa modalidade, o ataque é dirigido a um servidor DNS, e não a um computador de um internauta isoladamente
O sistema DNS (Domain Name System) funciona como uma espécie de

diretório de endereços da Internet. Toda navegação na Internet (no seu canal gráfico, a World Wide Web) tem que passar por um servidor DNS. Quando um internauta digita um determinado endereço web na barra do seu navegador, o seu computador pessoal comunica com o servidor do seu provedor local de acesso à Internet, em busca do número IP que corresponde àquele determinado endereço. Se o endereço procurado estiver armazenado no cache do servidor do provedor local, então ele mesmo direciona o programa de navegação para o endereço almejado ou, caso contrário, transfere a requisição para o servidor de um provedor maior, e assim por diante, até encontrar aquele que reconheça o endereço procurado e faça a correspondência.
Um hacker pode invadir o servidor DNS de um provedor de acesso à Internet e alterar endereços arquivados na memória cache. Se o servidor é "envenenado", alteradas as configurações relativas a um determinado endereço web, os internautas podem ser direcionados para um site falso mesmo teclando o endereço (URL) correcto. O ataque, assim praticado, produz resultados em muito maior escala do que a outra forma de pharming, em que os "pharmers" vitimam uma pessoa de cada vez, infectando os seus PC´s com vírus. O ataque ao servidor DNS de um provedor de Internet pode atingir inúmeros usuários de uma única vez.
Premonitório destas subversões dos sistemas cibernéticos foi o filme “A rede” (The Net) de 1995 – Dirigido por Irwin Winkler com Sandra Bullock, Jeremy Northam, L. Scott Caldwell - primeiro suspense de Hollywood sobre internet.
Todas estas actuações são criminosas e são objecto da Lei nº. 109/91, de 17 de Agosto, Lei da criminalidade informática, estando previstas e puníveis no artigo 7º, epigrafado “Acesso ilegítimo.”
Como se observa no citado estudo, os perpetradores directos das fraudes (phishers) não são facilmente identificáveis, pela razão de que utilizam técnicas de "anonimização" e, como regra, estão situados em territórios não submetidos à jurisdição do país da vítima.
Tem-se discutido a possibilidade da responsabilização de outros intermediários da cadeia informática, por exemplo dos provedores de hospedagem de conteúdo na Internet (sites e páginas eletrónicas).
Sustenta-se nesse estudo que o provedor não tem uma "obrigação geral de vigilância" sobre as informações que os utilizadores do sistema transmitem ou armazenam, bem como não tem uma "obrigação geral de procurar activamente factos ou circunstâncias que indiciem ilicitudes". Simplesmente actua provendo a infra-estrutura técnica para acesso à rede de comunicação, serviço que não acarreta uma co-obrigação de controlo de conteúdo, de zoneamento visando à exclusão de informação ou material ilícito. Assim, prevalece um princípio geral de irresponsabilidade do provedor por material

ilícito, depositado pelos utilizadores ou que de qualquer forma transita em seu sistema informático

Acresce que, em regra, os phishers não deixam as spoofed webpages hospedadas por longo tempo; é somente o suficiente para aplicar o golpe em algumas vítimas, o que pode ser questão de dias ou de horas. Assim, o provedor, em se tratando desse tipo de golpe, na prática, nem sequer pode ser acusado de inércia na remoção do conteúdo ilícito (site), pois são os próprios criminosos quem toma a iniciativa de remover o material, logo após a execução das tentativas do golpe.

Também se opina no estudo que em relação aos serviços de e-mail, não se pode exigir que o provedor tenha uma obrigação de triagem das mensagens. No caso de simples spams, o provedor não pode ser obrigado a indemnizar por perdas e danos, mesmo quando as mensagens indesejadas conduzam vírus (em arquivos anexos), a menos que o contrato com o usuário contenha cláusula expressa nesse sentido, com a promessa de uso de sistemas especiais e infalíveis de filtragem (firewall e outros sistemas de bloqueio). A única medida que parece razoável exigir por parte dos provedores de serviços de e-mail, em matéria de phishing e, de um modo geral, em relação a qualquer prática fraudulenta via spam, é que prestem informações aos seus utilizadores sobre essa prática, deixando bem claro até onde se responsabilizam e como configurar seu servidor de e-mail, indicando as medidas e a tecnologia para minimizar suas consequências.

As tecnologias disponíveis permitem um grau limitado de impedimento de chegada das mensagens fraudulentas à caixa postal dos utilizadores. Em geral, os prestadores de webmail divulgam um compromisso de combater o spam, através da utilização de filtros e outras ferramentas que se utilizam de inteligência artificial para apagar ou bloquear automaticamente mensagens não solicitadas. Outra técnica também bastante difundida é a de possibilitar que os próprios utilizadores bloqueiem certos endereços de e-mail.

No estudo seguido propugna-se ser necessário identificar outros meios para se oferecer resposta eficaz para a pessoa que sofre o dano, pois o Direito não pode tolerar que ofensas fiquem sem reparação. Se o interesse em restabelecer o equilíbrio violado pelo dano é a fonte geradora da responsabilidade civil, nada impede que se visualize a responsabilidade de outro intermediário da comunicação eletrónica, para atender a uma necessidade moral, social e jurídica de garantir a restauração do património da vítima violado pelo acto lesivo. E, realça-se, que, dentre os demais partícipes da cadeia de comunicação telemática, é o banco (prestador dos serviços de Internetbanking) quem está mais visivelmente posicionado de forma a interferir e impedir os efeitos da acção do phisher. Por ser a parte que

controla tecnicamente o acesso ao serviço de Internetbanking, pode prevenir os ataques de forma mais eficaz do que qualquer outro agente intermediário da cadeia eletrónica de comunicação. E é justamente por isso, por ser o agente intermediário que tem o maior controle tecnológico para evitar a consecução da fraude, que pode ser chamado à responsabilização, para reparar os efeitos patrimoniais do ilícito. Além disso, nenhum outro intermediário da cadeia de comunicação informática está tão ligado à vítima de phishing do que o seu próprio banco, com quem mantém uma relação contratual para prestação de serviços deInternetbanking.
Diz-se estudo que os bancos rejeitam a razoabilidade desta teoria, já que não podem ser responsabilizados por falha de segurança, nesses casos, uma vez que são os próprios utilizadores do sistema que fornecem (ainda que involuntariamente) as senhas aos infratores. No caso de phishing, sustentam, não há propriamente nenhuma invasão ao sistema informático dos bancos. Os phishers, mediante artifícios enganosos, apossam-se previamente das senhas dos verdadeiros usuários, e de posse delas acedem livremente ao sistema do banco, como se fossem legítimos utilizadores. Sob essa óptica, o ataque não é cometido contra o sistema informático do banco, que permanece invulnerável em termos de segurança.
Note-se que é precisamente esta a tese do Apelante.
Sobre isto avança-se no estudo em questão que essa tentativa de se colocar exclusivamente nas mãos do próprio usuário a responsabilidade de se precaver desse tipo específico de fraude não é satisfatória, quando se tem em vista as características dinâmicas do ciberespaço e o papel que os bancos desempenham no mercado de serviços on line. Por mais bem informado que possa ser o internauta, em termos de noções básicas de navegação segura e utilização de programas de protecção, não se tem como eliminar completamente a probabilidade de ser vítima da fraude. As técnicas de phishing estão cada vez mais sofisticadas. Portanto, o senso comum que as pessoas têm nos ambientes físicos, quando se protegem de ardis e esquemas fraudulentos, não é aplicável ao ambiente do ciberespaço. Uma coisa é a pessoa ser abordada em casa, no meio da rua ou mesmo no interior de uma agência bancária por um burlão, outra situação completamente diferente é a da navegação em ambiente eletrónico, onde a ausência de conhecimentos técnicos e a natural falta de aptidão para lidar com inovações tecnológicas, somadas às características dinâmicas da Internet, que permitem o aparecimento de variadas formas e a sofisticação das fraudes eletrónicas, colocam o utilizador em situação de ainda maior fragilidade. Essa diferenciação de situações impede que se tome de empréstimo de forma absoluta os padrões de conduta dos ambientes físicos para construção de

analogias com o ciberespaço, quando se trata de alocar os riscos financeiros da utilização de sistemas de pagamento e transações on-line. Os riscos devem ser alocados às partes mais capazes de lidar com eles e que, no caso em questão, são justamente os bancos.
Mais se explicita que a visão de que o phishing é um ataque que se executa de forma completamente externa ao sistema do banco, também não é apropriada. Na verdade, os computadores pessoais dos clientes são uma extensão do sistema de Internetbanking. Os bancos poderiam fornecer computadores dotados de programas actualizados de protecção contra golpes cibernéticos, mas optaram por utilizar os próprios computadores pessoais dos clientes como um recurso disponível. Essa deliberada opção tem o condão de vinculá-los a um mais elevado grau de riscos e perdas. As perdas decorrentes das fraudes financeiras devem integrar os custos do sistema escolhido já que os bancos escolheram permitir aos utilizadores a utilização dos seus computadores pessoais para, através da rede mundial, fazer conexão com o Internetbankig pelo que toda a rede nesse caso se considera como uma extensão do sistema. Encarada a questão por este ângulo, equipara-se a fraude electrónica à fraude dirigida ou cometida contra o cliente no interior de uma agência bancária ou caixa eletrónica. Essa é a analogia mais perfeita e que pode justificar a responsabilização do banco pela não adopção de dispositivos eficientes de protecção contra o phishing.
A solução preconizada por este autor, em termos de ressarcimento da vítima, passa pelo recurso ao Código de Defesa do Consumidor brasileiro, àquilo que chama de responsabilidade especial, dependente de parâmetros impostos nas previsões legais específicas (art. 20 e seu § 2º.). "O legislador criou um padrão de responsabilidade peculiar, que impõe a obrigação de liberar no mercado de consumo somente serviços isentos de vícios, não importando perquirir a culpa pelos danos causados em função do serviço viciado (…). Na definição do dever de reparação do fornecedor de serviços (bancários), o importante é um dado objetivo: se o serviço (de Internetbanking) é falho, no sentido de que não protege o usuário contra golpes de phishing".
Explica que são vícios de insegurança que atingem o consumidor (ou terceiro) na sua integridade física ou psíquica. O defeito de segurança provoca danos à esfera da saúde física ou psíquica da pessoa, causando o acidente de consumo.
Enquadremos agora o caso no nosso jure constituto.
A factualidade descrita emerge da existência de um contrato de conta bancária (ou abertura de conta) celebrado entre o banco, ora Apelante, e o Apelado e um contrato de homebanking, telebanking ou e-Banking, o qual sendo autónomo do contrato de conta bancária com ele tem uma íntima ligação

Através deste segundo contrato o Autor passou a poder movimentar a sua conta por meios de comunicação à distância.
Tendo Apelado sido alvo de uma fraude electrónica – phishing - acima conceptualizada, da qual resultou a subtacção da quantia € 4.480,00 da sua conta bancária, a questão decidenda consiste em saber se o Banco o deve reembolsar.
A jurisprudência tem vindo a entender, nesta matéria, que os riscos da falha do sistema informático utilizado, bem como dos ataques cibernautas ao mesmo, correm por conta do banco, por a tal conduzir o disposto no artigo 796º, nº1 do CCivil, desde que não se prove a culpa do cliente/utilizador. (vide Ac. do STJ de 18/12/2013, proc. nº 6479/09.8TBBRG.G1.S1 in www.dgsi.pt).
Isto embora alguma doutrina venha alertando, a propósito do contrato de depósito, que o dinheiro hoje em dia é escritural e que em bom rigor não há depósito porque não há guarda, nem há entrega. (v. g. Carlos Ferreira de Almeida acessível em http://www.justicatv.com/index.php?p=4235).
Também se tem utilizado o instituto da responsabilidade civil contratual, fazendo-se recair a presunção de culpa, prevista do artigo 799º, nº 1do C.Civil, sobre o banco por causa das deficiências de segurança no serviço homebanking.
Tem-se chamado ainda à colação o Regime das Cláusulas contratuais legais.
Na verdade, é sabido que o contrato de homebanking á partida comporta risco e esse risco tem de ser repartido de uma forma equitativa, tendo em conta os. direitos e deveres contratuais e os que emergem do quadro normativo existente.
O Decreto-Lei nº 317/2009, de 30 de Outubro que aprovou o Regime jurídico que regula o acesso à actividade das instituições de pagamento e a prestação de serviços de pagamento e resultou da transposição para a ordem jurídica interna da Directiva nº 2007/64/CE, do Parlamento Europeu e do Conselho, de 13 de Novembro, relativa aos serviços de pagamento no mercado interno, entrou em vigor em 1 de Novembro de 2009.
Ora, tendo os factos ocorrido depois da entrada em vigor deste diploma cremos ser este o quadro legal do caso.
Importa, assim, atentar nas seguintes disposições deste diploma
Artigo 67.º
Obrigações do utilizador de serviços de pagamento associadas aos instrumentos de pagamento
1 - O utilizador de serviços de pagamento com direito a utilizar um instrumento de pagamento tem as seguintes obrigações:
a) Utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização; e

b) Comunicar, sem atrasos injustificados, ao prestador de serviços de pagamento ou à entidade designada por este último, logo que deles tenha conhecimento, a perda, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento.
2 - Para efeitos da alínea a) do número anterior, o utilizador de serviços de pagamento deve tomar todas as medidas razoáveis, em especial ao receber um instrumento de pagamento, para preservar a eficácia dos seus dispositivos de segurança personalizados.
Artigo 68.º
Obrigações do prestador de serviços de pagamento associadas aos instrumentos de pagamento
1 - O prestador de serviços de pagamento que emite um instrumento de pagamento tem as seguintes obrigações:
a) 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, sem prejuízo das obrigações do utilizador do serviço de pagamento estabelecidas no artigo anterior;
b) Abster-se de enviar instrumentos de pagamento não solicitados, salvo quando um instrumento deste tipo já entregue ao utilizador de serviços de pagamento deva ser substituído;
c) Garantir a disponibilidade, a todo o momento, de meios adequados para permitir ao utilizador de serviços de pagamento proceder à notificação prevista na alínea b) do nº 1 do artigo anterior ou solicitar o desbloqueio nos termos do nº 4 do artigo 66.º;
d) O prestador do serviço de pagamento deve facultar ao utilizador do serviço de pagamento, a pedido deste, os meios necessários para fazer prova, durante 18 meses após a notificação prevista na alínea b) do nº 1 do artigo anterior, de que efectuou essa notificação; e
e) Impedir qualquer utilização do instrumento de pagamento logo que a notificação prevista na alínea b) do nº 1 do artigo anterior tenha sido efectuada.
2 - O risco do envio ao ordenante de um instrumento de pagamento ou dos respectivos dispositivos de segurança personalizados corre por conta do prestador do serviço de pagamento.
Artigo 70.º
Prova de autenticação e execução das operações de pagamento
1 - Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi correctamente efectuada, incumbe ao respectivo prestador do serviço de pagamento fornecer prova de que a operação de pagamento foi autenticada,

devidamente registada e contabilizada e que não foi afectada por avaria técnica ou qualquer outra deficiência.
2 - Caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, por si só, não é necessariamente suficiente para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 67.º
Artigo 71.º
Responsabilidade do prestador do serviço de pagamento por operações de pagamento não autorizadas
1 - Sem prejuízo do disposto no artigo 69.º, em relação a uma operação de pagamento não autorizada, o prestador de serviços de pagamento do ordenante deve reembolsá-lo imediatamente do montante da operação de pagamento não autorizada e, se for caso disso, repor a conta de pagamento debitada na situação em que estaria se a operação de pagamento não autorizada não tivesse sido executada.
2 - Sempre que o ordenante não seja imediatamente reembolsado pelo respectivo prestador de serviços de pagamento nos termos do número anterior, são devidos juros moratórios, contados dia a dia desde a data em que o utilizador de serviços de pagamento haja negado ter autorizado a operação de pagamento executada, até à data do reembolso efectivo, calculados à taxa legal, fixada nos termos do Código Civil, acrescida de 10 pontos percentuais, sem prejuízo do direito à indemnização suplementar a que haja lugar.
Artigo 72.º
Responsabilidade do ordenante por operações de pagamento não autorizadas
1 - No caso de operações de pagamento não autorizadas resultantes de perda, de roubo ou da apropriação abusiva de instrumento de pagamento, com quebra da confidencialidade dos dispositivos de segurança personalizados imputável ao ordenante, este suporta as perdas relativas a essas operações dentro do limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, até ao máximo de € 150.
2 - O ordenante suporta todas as perdas resultantes de operações de pagamento não autorizadas, se aquelas forem devidas a actuação fraudulenta ou ao incumprimento deliberado de uma ou mais das obrigações previstas no artigo 67.º, caso em que não são aplicáveis os limites referidos no nº 1.
3 - Havendo negligência grave do ordenante, este suporta as perdas resultantes de operações de pagamento não autorizadas até ao limite do saldo disponível ou da linha de crédito associada à conta ou ao instrumento de

pagamento, ainda que superiores a € 150, dependendo da natureza dos dispositivos de segurança personalizados do instrumento de pagamento e das circunstâncias da sua perda, roubo ou apropriação abusiva.
4 - Após ter procedido à notificação a que se refere a alínea b) do nº 1 do artigo 67.º, o ordenante não suporta quaisquer consequências financeiras resultantes da utilização de um instrumento de pagamento perdido, roubado ou abusivamente apropriado, salvo em caso de actuação fraudulenta.
5 - Se o prestador de serviços de pagamento não fornecer meios apropriados que permitam a notificação, a qualquer momento, da perda, do roubo ou da apropriação abusiva de um instrumento de pagamento, conforme requerido pela alínea c) do nº 1 do artigo 68.º, o ordenante não fica obrigado a suportar as consequências financeiras resultantes da utilização desse instrumento de pagamento, salvo nos casos em que tenha agido de modo fraudulento.
Artigo 74.º
Pedidos de reembolso de operações de pagamento iniciadas pelo beneficiário ou através deste
1 - O ordenante tem direito a apresentar o pedido de reembolso, referido no artigo 73.º, de uma operação de pagamento autorizada, iniciada pelo beneficiário ou através deste, durante um prazo de oito semanas a contar da data em que os fundos tenham sido debitados.
2 - No prazo de 10 dias úteis a contar da data da recepção de um pedido de reembolso, o prestador de serviços de pagamento reembolsa o montante integral da operação de pagamento, ou apresenta uma justificação para recusar o reembolso, indicando os organismos para os quais o ordenante pode remeter a questão, ao abrigo dos artigos 92.º e 93.º, se não aceitar a justificação apresentada.
3 - O direito do prestador do serviço de pagamento de recusar o reembolso nos termos do número anterior não é aplicável no caso a que se refere a nº 4 do artigo 73.
Desta literalidade se pode retirar a ideia de que o risco deve ser suportado sobretudo pelos bancos, o que é de bom senso por tudo o que já se disse.
Temos aqui que a regra é a do reembolso pelo prestador de serviços em relação a uma operação de pagamento não autorizada.
E, se o utilizador de serviços de pagamento negar ter autorizado uma operação de pagamento executada, ou alegar que a operação não foi correctamente efectuada, é ao prestador do serviço de pagamento que compete provar que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afectada por avaria técnica ou qualquer outra deficiência.
Neste caso a utilização do instrumento de pagamento registada pelo prestador

de serviços de pagamento não basta para provar que a operação de pagamento foi autorizada pelo ordenante, que este agiu de forma fraudulenta ou que não cumpriu, deliberadamente ou por negligência grave, uma ou mais das suas obrigações decorrentes do artigo 67.º
O texto destes preceitos é complexo e de difícil interpretação talvez porque resulta da transposição de directivas comunitárias em que é tudo muito negociado.
De qualquer forma, e tendo presente o disposto no nº 3 do artigo 9º do C.Civil, ou seja, que "Na fixação do sentido e alcance da lei, o intérprete presumirá que o legislador consagrou as soluções mais acertadas e soube exprimir o seu pensamento em termos adequados", julga-se ser de valia a tradicional doutrina de Antunes Varela Antunes Varela, (in Das Obrigações em Geral, Vol. I, 6.ª edição, Almedina, Coimbra, pág. 495), sobre os pressupostos da responsabilidade civil: a) a ocorrência de um facto; b) que esse facto deve ser considerado ilícito; c) que o facto ilícito possa ser imputado a um determinado sujeito; d) que por virtude desse facto ilícito praticado por uma pessoa ocorra um dano, patrimonial ou não patrimonial, na esfera jurídica de outrem; e) e que exista um nexo de causalidade entre o facto e o dano.
No citado artigo 72º preveem-se as situações de responsabilidade do ordenante por operações de pagamento não autorizadas
Quando se fala em imputação (nº1 do preceito) trata-se normalmente, e em termos de responsabilidade civil, como atrás se viu, de imputação subjectiva, sendo que esta pode revestir as modalidades de dolo, mera culpa ou negligência.
Na negligência podem abarcar-se as situações em que há a omissão de um dever de cuidado que uma atenta avaliação do caso poderia e deveria ter prevenido e as situações de imprudência ou imperícia, sendo que a primeira ocorrerá quando o agente age por precipitação, por falta de previdência, de atenção no cumprimento de determinado acto, e a imperícia quando o agente acredita estar apto e possuir conhecimentos suficientes pratica acto para o qual não está preparado por falta de conhecimento aptidão capacidade e competência.
Na mera culpa ou negligência é comum distinguirem-se os casos em que o agente prevê a produção do resultado lesivo como possível, mas, por leviandade, precipitação, desleixo ou incúria, crê na sua não verificação (representa um puro vício de vontade), daqueles em que, por inconsideração, descuido, imperícia ou ineptidão, o agente não concebe a possibilidade do resultado lesivo se verificar, podendo e devendo prevê-lo e evitar a sua verificação (representa um vício de representação e de vontade).
No primeiro caso fala-se de negligência consciente, no segundo de negligência

inconsciente. A par das apontadas modalidades de negligência, é tradicional a distinção entre negligência grave, leve e levíssima, em função da intensidade ou grau da ilicitude (a violação do cuidado objectivamente devido) e da culpa (a violação do cuidado que o agente é capaz de prestar segundo os seus conhecimentos e capacidades pessoa
Partindo destas premissas parece-nos que a norma do nº1 do artigo em causa prevê a negligência ou culpa leve ou levíssima, a do nº 2 prevê o dolo, a intencionalidade e a do nº 3 prevê a negligência consciente ou culpa grave.
A esta conclusão se também chegou no Ac. do Tribunal da Relação de Lisboa, de 17/6/2014, proc. nº 131/11.2TJLSB.L1-1 in www.dgsi.pt.
Vendo a factualidade descrita podemos afastar, sem qualquer hesitação, o dolo ou intencionalidade no comportamento do Apelado e mesmo uma negligência consciente ou culpa grave.
Resta apurar se actuou com negligência ou culpa leve.
Terá havido descuido, precipitação na consideração da situação ou falta da competência exigível para com ela lidar?
O Apelado acedeu à sua conta, através de homebanking, para efectuar um carregamento de saldo do seu telemóvel e durante a operação surgiu no ecrã uma mensagem que indicava que deveria efectuar o download de uma aplicação para o telemóvel, onde faltava preencher dois campos relativos à marca e modelo do telemóvel, os quais o Autor preencheu com a informação correspondente. Posteriormente recebeu no seu telemóvel uma mensagem escrita com vista a efectuar um download, o que fez. Uns dias depois verificou que tinha sido feita uma transferência bancária no valor de €4.480,00.
Esta factualidade tem de conjugar-se com a seguinte:
Para utilização do serviço homebanking o Apelante forneceu ao Apelado um elemento de identificação secreto e um código também secreto.
Adicionalmente sempre que o Apelado pretendesse realizar um pagamento ou transferência remotamente, esta só se realizava após a introdução de um apelidado "Código de Autorização" composto por 6 (seis dígitos) que seria enviado por mensagem escrita pelo Apelante, onde constava também um breve descritivo do movimento a efectuar, para o número de telemóvel do Autor.
Ora, tendo em conta que o banco sempre tinha de lhe enviar uma mensagem para o telemóvel com um código de autorização e com um descritivo do movimento a efectuar e tendo ainda em conta que pretendia proceder a um carregamento de saldo de telemóvel, não pode censurar-se a conduta do Apelado ao efectuar o download nas circunstâncias descritas.
Não incumpriu o Apelado os deveres supra enunciados, tendo ficado provado que, logo que teve conhecimento da fraude, comunicou-a ao Apelante.

Era necessário que o Apelado fosse uma pessoa muito experiente e muito conhecedora do meio de navegação em ambiente eletrónico para que pudesse desconfiar do isco que lhe foi lançado nas circunstâncias mencionadas.
Ora o Apelante quando acorda com os cliente o serviço homebanking não lhes exige essas aptidões.
Por tudo que se deixou explanado não se podem acolher as razões do Apelante
Pelo exposto, delibera-se julgar totalmente improcedente a Apelação, confirmando-se a sentença recorrida.

Conclusões.
I - O phishing, numa primeira etapa, consiste na apropriação de informações de outra pessoa (como nome, informações de conta e senha bancária), para serem utilizadas fraudulentamente nas fases seguintes da trama (transferências de numerários de contas correntes e aplicações financeiras.
O pharming é um ataque de phishing mais sofisticado sem o uso da "isca" (o e-mail com a mensagem enganosa). O vírus reescreve arquivos do PC que são utilizados para converter os endereços de Internet (URL´s) em números que formam os endereços IP (números decifráveis pelo computador.
Assim, um computador com esses arquivos comprometidos leva o internauta para o site falso, mesmo que este digite corretamente o endereço do site intencionado.
A mais sofisticada e perigosa forma de pharming é conhecida como "DNS (Domain Name System) poisoning" (traduzindo para o português, seria algo como "envenenamento do DNS"), por possibilitar um ataque em larga escala. Nessa modalidade, o ataque é dirigido a um servidor DNS, e não a um computador de um internauta isoladamente.
II - A factualidade em causa emerge da existência de um contrato de conta bancária (ou abertura de conta) celebrado entre o banco, ora Apelante, e o Apelado e um contrato de homebanking, telebanking ou e-Banking, o qual sendo autónomo do contrato de conta bancária com ele tem uma íntima ligação
Através deste segundo contrato o Autor passou a poder movimentar a sua conta por meios de comunicação à distância e foi alvo de uma fraude electrónica – phishing - acima conceptualizada, da qual resultou a subtracção da quantia € 4.480,00 da sua conta bancária.
O Decreto-Lei nº 317/2009, de 30 de Outubro, que aprovou o Regime jurídico que regula o acesso à actividade das instituições de pagamento e a prestação de serviços de pagamento e resultou da transposição para a ordem jurídica interna da Directiva nº 2007/64/CE, do Parlamento Europeu e do Conselho, de 13 de Novembro, relativa aos serviços de pagamento no mercado interno,

entrou em vigor em 1 de Novembro de 2009.
Tendo os factos ocorrido depois da entrada em vigor deste diploma é este o quadro legal do caso.
III - Pode-se afastar, sem qualquer hesitação, o dolo ou intencionalidade no comportamento do Apelado e mesmo uma negligência consciente ou culpa grave.
Também não incumpriu o Apelado os deveres que a lei ou contato lhe impunham, tendo ficado provado que, logo que teve conhecimento da fraude, comunicou-a ao Apelante.
No caso, era necessário que o Apelado fosse uma pessoa muito experiente e muito conhecedora do meio de navegação em ambiente eletrónico para que pudesse desconfiar do isco que lhe foi lançado nas circunstâncias provadas.
Ora o banco Apelante quando acorda com os cliente o serviço homebanking não lhes exige essas aptidões.

Custas pelo Apelante.
Porto, 7 de Outubro de 2014
Ana Lucinda Cabral
Maria do Carmo Domingues
José Carvalho