5ª VARA CIVEL DE DUQUE DE CAXIAS
Apelante: BANCO BS2 S A
Apelada: DERRON ENGENHARIA LTDA
Relator: DES. MILTON FERNANDES DE SOUZA

ACÓRDÃO

DIREITO DO CONSUMIDOR. OBTENÇÃO DE DADOS BANCÁRIOS MEDIANTE FRAUDE. CONDUTA DA VÍTIMA. 1-Correntista que recebe mensagens por correio eletrônico e aplicativo visando o fornecimento de seus dados bancários e, mesmo desconfiado, decide por responder uma das mensagens recebidas, fato que viabilizou a invasão de seu dispositivo, a obtenção de seus dados bancários e, em consequência, a realização de transferência bancária em favor de terceiro, sem seu conhecimento

2-Fraude cibernética denominada "Phishing" que consiste em técnicas persuasivas direcionadas a consumidores visando a obtenção de senhas bancárias, dados pessoais, seja pelo fornecimento espontâneo da própria vítima ou por intermédio de arquivos maliciosos (malware) que retiram do dispositivo da vítima seus dados sigilosos.

3-Ausência de nexo causal com a atividade bancária, pois a obtenção dos dados se deu em decorrência de ato espontâneo da vítima, sem qualquer indício de que a transação estaria inadequada ao perfil do correntista.

Vistos, relatados e discutidos estes autos de **Apelação nº 0824290-12.2022.8.19.0021,** em que é apelante **BANCO BS2 S A** e é apelada **DERRON ENGENHARIA LTDA,**

Acordam os Desembargadores que compõem a Quarta Câmara de Direito Privado do Tribunal de Justiça, por **unanimidade** de votos, em **DAR PROVIMENTO** ao recurso para julgar improcedente a pretensão. Invertidos, em consequência, os encargos da sucumbência, com honorários advocatícios em 10% do valor da causa.

Cuida-se de ação ajuizada por DERRON ENGENHARIA LTDA em face de BANCO BS2 S.A, em razão de transação bancária realizada sem seu consentimento, fruto de ação de terceiro mediante fraude.

Narra a petição inicial que o autor recebeu email da empresa que cuida da sua contabilidade, solicitando atualização de dados bancários, mas ignorou, mas continuou a receber mensagens desse tipo por parte da instituição bancária, também as ignorando.

Todavia, resolveu responder a uma dessas mensagens informando que não se sentia seguro em realizar a operação.

No entanto, ao utilizar o aplicativo da instituição bancária foi identificado o início do procedimento de atualização e o autor foi redirecionado a uma conversa eletrônica, mas nela também não deu prosseguimento no pedido de atualização dos seus dados bancários.

Ocorre que apesar de não ter concluído o procedimento mencionado, foi realizada uma transferência via PIX, no valor de R$ 11.000,00 (onze mil reais), em favor de terceiro, desconhecido do autor e por ele não autorizada, motivo do ajuizamento da ação diante da negativa da instituição-ré em reembolsar o valor debitado.

Em contestação, a instituição argumenta, em resumo, pela ocorrência de culpa exclusiva da vítima, inexistindo danos morais a serem compensados.

A sentença recorrida contém o seguinte dispositivo:

> Por tudo o que foi exposto, **JULGO PARCIALMENTE PROCEDENTES** os pedidos autorais, resolvendo o mérito na forma do art. 487, I, do Código de Processo Civil, para condenar o Réu a:
>
> **1. restituir** à parte Autora, **na forma simples**, o montante de R$ 11.000,00 (onze mil reais), incluindo juros e encargos cobrados, incidindo sobre o valor juros de 1% (um por cento) ao mês desde a data da citação e correção monetária segundo os índices oficiais da E. Corregedoria de Justiça deste Tribunal desde o desembolso, devendo, para tanto, tais valores serem apurados em fase de liquidação de sentença;
>
> **2. indenizar** à parte Autora a quantia de **R$ 5.000,00 (cinco mil reais)** em favor da parte autora, para compensar os danos morais experimentados, observando-se também o caráter punitivo-pedagógico da condenação, com juros de 1% (um por cento) ao mês desde a citação e correção monetária desde a sentença.

A sentença recorrida adotou, basicamente, a seguinte fundamentação:

> Destaco que é rotineira a constatação que a utilização de meios magnéticos para efetivação de compras tem se prestado a todo tipo de

> fraude, sendo praticamente impossível ao consumidor realizar a prova negativa das suas alegações.
>
> O fato de ter a transação sido realizada eletronicamente, que só se concluiu com o fornecimento de dados pessoais, por si só não permite concluir que a parte Autora foi descuidada quanto ao seu uso e guarda. A notória engenhosidade e habilidade dos estelionatários milita contra essa assertiva, sendo certo que mesmo uma pessoa extremamente cuidadosa pode ser vítima de ardil de evento como o descrito nos autos.
>
> Nesta seara, é evidente ainda que a instituição financeira dispõe de outros recursos para verificar que estão sendo realizadas compras e transações, em curto espaço de tempo, que não condizem com o perfil do cliente, capazes de impedir este tipo de crime, restando caracterizado o fato de terceiro, considerado fortuito interno, risco inerente a própria atividade desenvolvida pelo réu, que não tem o condão de afastar sua responsabilidade.

A instituição bancária recorre argumentando, em resumo, que: (1) a sentença é nula por não observar o litisconsórcio passivo necessário, incluindo-se o beneficiário da transação questionada; (2) é parte ilegítima para responder a pretensão, foi identificado o beneficiário da transação; (3) houve culpa exclusiva do correntista ao clicar em link falso.

A parte autora apresentou contrarrazões prestigiando a sentença recorrida.

É o relatório.

Presentes os requisitos de admissibilidade recursal.

A hipótese dos autos cuida da fraude cibernética denominada “Phishing”[1], que consiste em técnicas persuasivas direcionadas a consumidores visando a obtenção de senhas bancárias, dados pessoais, seja pelo fornecimento espontâneo da própria vítima ou por intermédio de arquivos maliciosos (malware) que retiram do dispositivo da vítima seus dados sigilosos.

Isso porque denota-se dos autos que o correntista recebeu mensagens por correio eletrônico e aplicativo visando o fornecimento de seus dados bancários e, mesmo desconfiado, decidiu por responder uma das mensagens recebidas, fato que viabilizou a invasão do seu dispositivo, a obtenção de seus dados bancários e, em consequência, a transferência realizada em favor de terceiro, sem seu conhecimento.

Compete-nos, assim, perquirir se a instituição bancária tem responsabilidade civil em decorrência desses fatos.

Sobre a controvérsia o Superior Tribunal de Justiça concluiu que:

---

1 https://www.tjrj.jus.br/phishing#:~:text=O%20phishing%20%C3%A9%20um%20golpe,e%20dados%20confidenciais%20da%20v%C3%ADtima.

Vazamento de dados bancários. Golpe do boleto. Tratamento de dados pessoais sigilosos de maneira inadequada. Art. 43 da LGPD. Facilitação da atividade criminosa. Fato do serviço. Dever de indenizar. Súmula 479/STJ.

E, no Informativo 791, de 18 de outubro de 2023, discorreu-se da seguinte forma:

Nos termos do art. 14, § 1°, do CDC (Código de Defesa do Consumidor), o serviço é considerado defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração circunstâncias relevantes, como o modo de seu fornecimento, o resultado e os riscos que razoavelmente dele se conjecturam, e a época em que foi fornecido.

A prestação do serviço de qualidade pelos fornecedores abrange o dever de segurança, que, por sua vez, engloba tanto a integridade psicofísica do consumidor, quanto sua integridade patrimonial. Consabidamente, o CDC é aplicável às instituições financeiras (Súmula 297/STJ), as quais devem prestar serviços de qualidade no mercado de consumo.

No entendimento do Tema Repetitivo n. 466/STJ, que contribuiu para a edição da Súmula n. 479/STJ, as instituições bancárias respondem objetivamente pelos danos causados por fraudes ou delitos praticados por terceiros, como, por exemplo, abertura de conta corrente ou recebimento de empréstimos mediante fraude ou utilização de documentos falsos, porquanto tal responsabilidade decorre do risco do empreendimento, caracterizando-se como fortuito interno (REsp n. 1.197.929/PR, Segunda Seção, julgado em 24/8/2011, DJe 12/9/2011).

Especificamente nos casos de golpes de engenharia social, não se pode olvidar que os criminosos são conhecedores de dados pessoais das vítimas, valendo-se dessas informações para convencê-las, por meio de técnicas psicológicas de persuasão - como a semelhança com o atendimento bancário verdadeiro -, a fim de atingir seu objetivo ilícito.

Todavia, para sustentar o nexo causal entre a atuação dos estelionatários e o vazamento de dados pessoais pelo responsável por seu tratamento **é imprescindível perquirir, com exatidão, quais dados estavam em poder dos criminosos, a fim de examinar a origem de eventual vazamento e, consequentemente, a responsabilidade dos agentes respectivos.**

Assim, para se imputar a responsabilidade às instituições financeiras, no que tange ao vazamento de dados pessoais que culminaram na facilitação de estelionato, deve-se garantir que a origem do indevido tratamento seja o sistema bancário. Os nexos de causalidade e imputação, portanto, dependem da hipótese concretamente analisada. Isso porque os dados sobre operações financeiras são, em regra, presumivelmente de tratamento exclusivo pelas instituições financeiras.

> Portanto, dados pessoais vinculados a operações e serviços bancários são sigilosos e cujo tratamento com segurança é dever das instituições financeiras. Desse modo, seu armazenamento de maneira inadequada, a possibilitar que terceiros tenham conhecimento dessas informações e causem prejuízos ao consumidor, configura falha na prestação do serviço (art. 14 do CDC e 43 da LGPD). (grifos nossos)..

Sob essa perspectiva e observando que os dados do correntista foram obtidos mediante ação espontânea do próprio, por intermédio da qual terceiro obteve seus dados pessoais, não há como se estabelecer o nexo de causalidade necessário para se imputar à instituição bancária o dever de reparar o dano sofrido.

Logo, o vazamento dos dados não seu por conta de conduta da instituição bancária.

Nesse sentido:

> APELAÇÃO CÍVEL. AÇÃO INDENIZATÓRIA. ALEGAÇÃO DE FALHA NA PRESTAÇÃO DO SERVIÇO. INSTITUIÇÃO FINANCEIRA. PAGAMENTOS POR INTERNET BANKING NÃO RECONHECIDOS. ACESSO A SITE FALSO PELA CONSUMIDORA ATRAVÉS DE LINK RECEBIDO POR SMS. FORNECIMENTO DE DADOS EM SUPOSTA "ATUALIZAÇÃO DE CADASTRO". SITE DO RÉU COM DIVERSAS ADVERTÊNCIAS ACERCA DE FRAUDES MEDIANTE LINKS FALSOS E COM DICAS DE SEGURANÇA. AUSÊNCIA DE FALHA NA PRESTAÇÃO DO SERVIÇO. CULPA EXCLUSIVA DA VÍTIMA. IMPROCEDÊNCIA QUE SE IMPÕE. 1. Supondo estar fazendo uma "atualização de cadastro" junto ao banco réu, a autora acessou o link fornecido em seu celular, fez a "atualização" dos seus dados no site falso do banco, e logicamente para isso precisou digitar os dados da agência e conta e fornecer sua senha eletrônica ou token, e tais informações já são suficientes para que fraudadores acessem o aplicativo ou site do banco e façam as mais diversas operações, inclusive pagamentos, como foi o caso. 2. A par disso, além de o réu ter disponibilizado vídeos no YouTube sobre como evitar fraudes como as ocorridas nestes autos e outras semelhantes, consta do seu site, em consulta às dicas de segurança, que o Santander não envia links para atualizações através de SMS ou e-mail. 3. Forçoso é o reconhecimento, no caso, de que o apelante tomou todas as cautelas devidas para alertar os clientes acerca da fraude de que foi vítima a autora, a afastar completamente a falha na prestação do serviço. 4. O consumidor, ao utilizar um serviço como o de internet banking ou mobile banking, deve ficar atento às recomendações da instituição financeira para garantia da segurança em sua utilização. 5. Culpa única e exclusiva da apelada pelo dano sofrido. 6. Provimento do apelo para julgar improcedentes os pedidos. (0066304-54.2016.8.19.0021 - APELAÇÃO. Des(a). GILBERTO CLÓVIS FARIAS MATOS - Julgamento: 09/09/2021 - VIGÉSIMA SEGUNDA CÂMARA CÍVEL)

DECISÃO MONOCRÁTICA. CIVIL - DIREITO DAS OBRIGAÇÕES, PROCESSUAL CIVIL E DIREITO DO CONSUMIDOR. APELAÇÃO. AÇÃO INDENIZATÓRIA. DANO MATERIAL E MORAL. ALEGAÇÃO DE FALHA DO SERVIÇO. INSTITUIÇÃO FINANCEIRA. EMPRÉSTIMOS E PAGAMENTOS NÃO RECONHECIDOS. ACESSO A LINK FALSO PELO CONSUMIDOR, QUE FORNECEU OS DADOS DO SEU CARTÃO DE SEGURANÇA PARA OPERAÇÕES ON LINE. FALHA NA SEGURANÇA BANCÁRIA QUE NÃO SE VERIFICA. CULPA EXCLUSIVA DA VÍTIMA. VERBETE SUMULAR N.º 330 TJRJ. IMPROCEDÊNCIA DO PEDIDO. ACERTO DO JULGADO. RECURSO NÃO PROVIDO.

Embora tivesse omitido da narrativa inicial, admite a autora, em sede de recurso, que acessou um link falso de e-mail para suposta atualização do cartão de segurança, por meio do qual ela digitou as 50 (cinquenta) posições do token, mas que não teria fornecido o seu login ou a sua senha de acesso ao internet banking.

A fraude ocorreu por culpa única e exclusiva da apelante, que não atentou para as dicas de segurança amplamente divulgadas no site pelos réus.

Dever de guarda das informações de sigilo que não foi observado pela correntista, vítima de golpe do recadastramento bancário, o que afasta a responsabilidade da instituição financeira, a teor da inteligência do artigo 14, § 3º, II do CDC.

Culpa exclusiva da apelante pelo dano sofrido.

Recurso conhecido, mas não provido, nos termos do art. 932, IV, alínea "a", do CPC, deferindo-se à apelante a gratuidade de justiça tendo em vista o documento de arquivo 289. Majoração da verba honorária de sucumbência arbitrada na sentença para 12% (doze por cento) sobre o valor da causa, observada a gratuidade de justiça deferida. (0013383-11.2017.8.19.0207 - APELAÇÃO. Des(a). LINDOLPHO MORAIS MARINHO - Julgamento: 10/08/2020 - DÉCIMA SEXTA CÂMARA CÍVEL)

APELAÇÃO CÍVEL. AÇÃO INDENIZATÓRIA. DANO MATERIAL E MORAL. ALEGAÇÃO DE FALHA DO SERVIÇO. INSTITUIÇÃO FINANCEIRA. TRANSFERÊNCIAS NÃO RECONHECIDAS. ACESSO A LINK FALSO PELO CONSUMIDOR, QUE FORNECEU OS DADOS DO SEU CARTÃO DE SEGURANÇA PARA OPERAÇÕES ON LINE. SITE DO RÉU COM DIVERSAS ADVERTÊNCIAS ACERCA DE FRAUDES MEDIANTE LINKS FALSOS E COM DICAS DE SEGURANÇA. AUSÊNCIA DE FALHA NA PRESTAÇÃO DO SERVIÇO. CULPA EXCLUSIVA DA VÍTIMA. IMPROCEDÊNCIA QUE SE IMPÕE. 1. Conforme conversa gravada trazida aos autos pelo réu, o autor reconheceu a um preposto do banco, ao telefone, na entrevista acerca da fraude comunicada, que acessou um site falso para suposta atualização do cartão de segurança, e que informou a numeração do respectivo cartão e do código de segurança on line. 2. A par disso, o réu comprova que disponibilizou vídeo no YouTube avisando previamente sobre o golpe

> sofrido pelo autor, e de como não cair no engodo. Consta do site, inclusive, em consulta às dicas de segurança, que o banco não envia links para atualizações através de SMS ou e-mail. 3. Forçoso é o reconhecimento, no caso, de que o réu tomou todas as cautelas devidas para alertar os clientes acerca da fraude de que foi vítima o autor, a afastar completamente a falha na prestação do serviço. 4. Culpa exclusiva do apelado pelo dano sofrido. 5. Provimento do apelo para julgar improcedentes os pedidos. (0008174-45.2018.8.19.0007 - APELAÇÃO. Des(a). GILBERTO CLÓVIS FARIAS MATOS - Julgamento: 23/06/2020 - DÉCIMA QUINTA CÂMARA CÍVEL)

Por estes motivos, **DÁ-SE PROVIMENTO** ao recurso para julgar improcedente a pretensão. Invertidos, em consequência, os encargos da sucumbência, com honorários advocatícios em 10% do valor da causa.

Rio de Janeiro, na data da sessão de julgamento.

DESEMBARGADOR MILTON FERNANDES DE SOUZA
Relator