2022
AGOSTO/OUTUBRO
Ed. 39 - Vol. 4. Págs. 71-90

JNT - FACIT BUSINESS AND TECHNOLOGY JOURNAL ISSN: 2526-4281 - QUALIS B1

A RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES BANCÁRIAS POR DANOS SOFRIDOS NO GOLPE DO PIX

THE CIVIL RESPONSIBILITY OF BANKING INSTITUTIONS FOR DAMAGES SUFFERED IN THE PIX COUP

Ana Jasmim Barbosa da SILVA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: anajasmyym_9707@outlook.com

Pollyanna Marinho Medeiros CEREWUTA
Centro Universitário Tocantinense Presidente Antônio Carlos (UNITPAC)
E-mail: pollyanna.cerewuta@unitpac.edu.br

RESUMO

O presente artigo aborda a responsabilidade civil das instituições bancárias por danos sofridos pelas vítimas no golpe do PIX, cujo objetivo é demonstrar as nuances da responsabilidade civil aplicada às fraudes envolvendo o PIX, tendo em vista a constante ocorrência das fraudes e a possibilidade de responsabilização das instituições bancárias. O estudo foi desenvolvido com uso da metodologia exploratória, com a finalidade de esclarecer, desenvolver ou até mesmo modificar conceitos e ideia, através da análise de documentos, relatos de casos reais e decisões jurídicas e tendo como método de pesquisa o hipotético-dedutivo. Para tanto, fez-se uma discussão acerca do Golpe do PIX, seguida de uma análise sobre o estelionato virtual e por fim a responsabilização objetiva nessa modalidade de fraude. Com isso, foi constatado que diariamente os tribunais têm se posicionado a considerar interpretações sobre a temática, mas que se trata ainda de uma questão recente, que vem evoluindo nos últimos anos, proporcionando maior segurança jurídica no ordenamento jurídico brasileiro no sentido de aplicar a responsabilização às instituições bancárias pela ocorrência do golpe do PIX.

Palavras-chave: Crimes cibernéticos. Estelionato virtual. Golpe do PIX. Responsabilidade civil objetiva.

ABSTRACT

This article addresses the civil liability of banking institutions for damages suffered by victims in the PIX scam, whose objective is to demonstrate the nuances of civil liability applied to fraud involving the PIX, in view of the constant occurrence of fraud and the possibility of liability for banking institutions. The study was developed using the exploratory methodology, with the purpose of clarifying, developing or even modifying concepts and ideas, through the analysis of documents, reports of real cases and legal decisions and using the indirect inductive research method. To this end, a discussion was held about the PIX coup, followed by an analysis of virtual embezzlement and, finally, objective accountability in this type of fraud. With this, it was verified that the courts have positioned themselves daily to be considered understood on the subject, but that it is still a recent issue, which has been evolving in recent years, providing greater legal certainty in

the Brazilian legal system in the sense of applying the accountability to banking institutions for the occurrence of the PIX coup.

Keywords: Cybercrimes. Virtual fraud. PIX coup. Objective civil liability.

INTRODUÇÃO

O presente artigo científico estuda a possibilidade da responsabilização civil das instituições bancárias pelo golpe do PIX no ordenamento jurídico brasileiro, suas particularidades, em observância as mais recentes normatizações e decisões judiciais sobre essa questão.

Com isso, a problemática do presente trabalho está voltada para a análise se da ocorrência dessas fraudes seria passível de responsabilização civil objetiva ou subjetiva, especialmente considerando a jurisprudência brasileira.

Entretanto, devido à facilidade em se transferir dinheiro sem a necessidade de dados, como agência, conta corrente ou poupança, se tornou necessária apenas a chave PIX, o que facilitou o crescimento de fraudes. Dito isso, o Golpe do PIX acontece quando o criminoso, com amplo acesso à internet, encaminha páginas e arquivos falsos para roubar dados, bem como a ocorrência da falha do PIX, o WhatsApp clonado e outras formas.

Assim, dada a relevância do tema, este trabalho buscou demonstrar as nuances da responsabilidade civil aplicada as fraudes envolvendo o PIX, tendo como objetivos específicos expor os aspectos gerais do golpe do PIX para em seguida compreender o crime de estelionato virtual e, assim, abordar sobre as possíveis responsabilizações.

Inicialmente, foram abordadas as formas do golpe do PIX existentes no Brasil, os dados alarmantes e as legislações pertinentes sobre essa temática. Em seguida tratou-se de expor acerca do estelionato de modo geral e no ambiente virtual.

Posteriormente, para melhor elucidar sobre a problemática, fez-se uma análise sobre a responsabilidade das instituições bancárias sobre o golpe do PIX, demonstrando as formas de fraude, a engenharia social e o phishing, bem como as modalidades de responsabilização.

Logo, para a realização do trabalho, fora utilizada a pesquisa exploratória, objetivando o esclarecimento de conceitos e ideias, através da análise de documentos, entrevistas, relatos de casos reais e decisões jurídicas. Além disso, foi utilizado na pesquisa o método hipotético-dedutivo, que submete as hipóteses principais para determinada teoria com um teste de falseabilidade, tendo por base pesquisas exploratórias.

Por fim, o presente tema tem relevância, devido a crescente incidência dos golpes do PIX no Brasil, bem como na exposição das correntes doutrinárias e jurisprudenciais acerca da aplicação da responsabilidade civil objetiva ou subjetiva nos casos concretos.

GOLPE DO PIX

Inicialmente, se sabe que o PIX começou a ser desenvolvido no ano de 2018, através da portaria nº 97.909 que tratava sobre pagamentos instantâneos (BRASIL, 2018). Posteriormente, no ano de 2019, foram divulgados como seria o PIX. Logo, no ano de 2020, dispondo de modalidades de transferências sem custo ao titular, foi implementado o PIX.

É importante estabelecer acerca do conceito de PIX, que é uma ferramenta que transformou as questões bancárias, especialmente nos casos de emissões de boleto, como uma forma de pagamento instantâneo vinculado ao Banco Central (SCHAAL; QUINELATO; GOULART, 2021). Assim, desde o lançamento através da Resolução do Banco Central Brasileiro, de nº 1, o PIX se tornou possível a realização de transações de forma rápida, segura, simples e barata (BRASIL, 2020).

Segundo o site oficial do Banco Central, o PIX seria a ferramenta instantânea de pagamento, em que se transferem recursos em segundos, a qualquer hora ou dia. Essa ferramenta ainda aumenta a velocidade dos pagamentos ou transferências que são realizados e recebidos (BANCO CENTRAL DO BRASIL, 2021).

Sabe-se que os pilares do PIX são: a governança, formas de participação, infraestrutura centralizada de liquidação, serviços de conectividade, provimento de liquidez, e base única e centralizada de dados de endereçamento (SCHAAL; QUINELATO; GOULART, 2021).

As características dessa ferramenta bancária está no fato de as transações serem concluídas rapidamente, com recursos disponíveis e receber em tempo real, efetiva nas 24 horas do dia e sete dias por semanas, com facilidade para o usuário e gratuidade para pessoa física. Além disso, existem mecanismos de segurança nas transações, haja vista a sua versatilidade e a ampla participação que possibilita os pagamentos entre instituições diferentes (BANCO CENTRAL, 2021).

Outro ponto importante está no fato de que não só os bancos tradicionais, como fintechs[1] e cooperativas de crédito também possuem acesso a plataforma PIX. Ainda assim, plataformas com mais de 500 mil contas ativas, tem sua participação obrigatória (SCHAAL; QUINELATO; GOULART, 2021).

Contudo, os pagamentos do PIX são realizados por intermédio de chaves, como o CPF ou CNPJ, número de telefone, e-mail, ou código aleatório que é gerado pela instituição bancária. Uma pessoa natural pode ter até 5 chaves e a pessoa jurídica até 20. Em casos de requerimento de exclusão de chave, é necessário que seja direcionado a instituição participante a pedido do usuário, com exceção das hipóteses previstas no Regulamento n. 1 do BACEN, na tentativa de fraude e inatividade por até 12 meses (BRASIL, 2020).

Ainda assim, se sabe que quando a chave PIX, está vinculada a uma pessoa natural, esta é considerada como sendo um dado pessoal, mesmo se for um código aleatório, haja vista estar vinculado ao usuário indiretamente. Logo, segundo a Lei Geral de Proteção de Dado em seu artigo 5º inciso I, dado pessoal é compreendido como sendo qualquer informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2018).

Sabe-se que a base legal do tratamento de dados pessoais relacionados a essas transações, é o consentimento, que tem que ser colhido na hora do cadastramento das chaves do titular na instituição, consoante artigo 7º, inciso I da LGPD (BRASIL, 2018). Uma questão relevante é a possibilidade de que seja utilizado os dados provenientes das transações para outras destinações não compatíveis com o consentimento original, o que implica a necessidade de o controlador informar o titular sobre essas mudanças de finalidade para que se possa revogar seu consentimento caso discorde (SCHAAL; QUINELATO; GOULART, 2021).

Entretanto, se sabe que as facilidades advindas do cenário digital devem ser acompanhadas com questões de segurança. Assim, com a chegada do PIX, não seria diferente, devendo as instituições tomarem medidas para se protegerem de possíveis fraudes.

Os golpes do PIX funcionam de diversas maneiras, sendo a primeira chamada de capturador de sessões. Nessa espécie de fraude, o golpista encaminha um pdf ou e-mail para a vítima que se aberto o arquivo infecta o dispositivo com o vírus que avisa o

1 Fintechs: Trata-se de uma união da palavra financial e tecnology, correspondendo a tecnologia e inovação que são aplicadas na solução de serviços financeiros.

criminoso quando o aplicativo do banco é aberto, permitindo assim, que se se capture as credenciais de acesso da conta bancária da vítima (BRANCO, 2021).

Ainda assim caso seja necessário a autenticação por token[2], o criminoso necessita clonar o número do celular da vítima para que seja possível o acesso ao código. Dessa forma, o invasor se associa com funcionários da operadora de telefonia, que bloqueia o chip da vítima e o recadastram com a posse direcionada ao criminoso (BRANCO, 2021).

Além dessa captura de sessões, existe ainda os golpes de *phishing*, simples ou complexos. Os básicos são aqueles em que os golpistas criam páginas falsas que podem ser acessadas por um link de falsa oferta. Já em se tratando do mais complexo, envolve o Domain Name System do usuário, que ao digitar seu endereço de IP, direciona o navegador a um ambiente já esperado. Logo, o invasor, modifica a configuração, fazendo com que a vítima acesse sites falsos, pensando que são verdadeiras (BRANCO, 2021)

É importante fazer uma ressalva, a respeito da dificuldade ao acesso a internet que várias pessoas possuem, de modo a não possuírem conhecimento e acabarem por se evolver em golpes, por não terem noção de que um simples aceite de e-mail, poderá ensejar em um perigo.

Esse acesso ao DNS do aparelho da vítima é um processo difícil, onde os criminosos dependem da infecção do computador do alvo para que se possam realizar a chance de modificação das configurações. Ainda assim, mesmo que consigam realizar esse golpe, as páginas dos bancos com as medidas de segurança, não são afetadas pelos constantes avanços na segurança, tornando esse método pouco popular entre os criminosos (BRANCO, 2021).

Outro golpe realizado pelos criminosos, é o do SMS emergencial, que dispara milhares de mensagens automáticas solicitando que sejam realizadas uma transferência via PIX, para a solução do problema financeiro (BRANCO, 2021).

As transações ora estudadas, contam com os mesmos mecanismos já utilizados no DOC e TED, tais como a mensageria e a criptografia e são protegidos pela Lei do Sigilo Bancário, nº 105 de 2001 (BRASIL, 2001). O PIX ainda possui uma função de notificação em casos de fraudes, sendo que as chaves envolvidas nestas fraudes, são colocadas em uma lista negra, que é compartilhada com as demais instituições do programa PIX para que sejam evitadas possíveis golpes (SCHAAL; QUINELATO; GOULART, 2021).

2 Token: Trata-se de um dispositivo gerador de senhas.

Acontece que, a Resolução nº 1 em seu artigo 38, dispõe que a instituição deve rejeitar as transações quando houver suspeitas de fraude, mas não bastando se caso o fraudador for rápido e retire o dinheiro da conta (SCHAAL; QUINELATO; GOULART, 2021).

Logo, a vulnerabilidade do sistema está relacionada ao próprio usuário, em relação ao roubo do aparelho celular para a realização de transações, capturas da identidade de pessoas por intermédio de golpes de chaves, roubos de chaves de PIX e outros mecanismos. Dito isso, é evidente a importância da efetividade de canais de comunicação com o usuário, deixando claro que transações e cadastros somente são realizados por canais oficiais (SCHAAL; QUINELATO; GOULART, 2021).

Nesse sentido, os participantes da plataforma PIX, devem garantir que seus aplicativos atendam aos requisitos de segurança impostos pelo Banco Central, como é o caso da criptografia, verificação de identidade, assinatura digital, gestão de certificados digitais e o cumprimento das normativas da Lei Geral de Proteção de Dados nº 13.709 de 2018 (SCHAAL; QUINELATO; GOULART, 2021).

Contudo, mesmo o PIX possuindo mecanismos inibidores de fraudes, ainda se fazem necessários cuidados da parte pagadora e recebedora. Dito isso, existem algumas formas de prevenção dos golpes do PIX:

> Estabeleça um limite diário para transferência via Pix no app ou site oficial do seu banco; Realize transações somente no app ou site oficial do seu banco; Certifique-se que o site do banco ou da loja que você está navegando é o correto; Confira se o site di banco ou da loja que está navegando é o correto; Confira se o site em que está navegando é seguro clicando no cadeado que fica na barra de endereço do navegador; Não clique em links ou baixe arquivos de e-mails suspeitos, e sempre confira se o e-mail possui um domínio confiável; Não realize transações financeiras quando estiver conectado em redes públicas como de shoppings e restaurantes; Ao divulgar sua chave Pix para pessoas e empresas que você não tem relação de confiança, prefira informar a chave aleatória em vez da atrelada ao CPF; Ative a autenticação de duas etapas em todos os lugares onde ela está disponível (BRANCO, 2021, p. 17).

Nesse sentido, o referido autor trouxe soluções para que fossem evitadas as fraudes envolvendo o PIX, devido ao analfabetismo virtual presente no dia a dia da sociedade. Ações como: estabelecer limite diário, fazer transferências apenas através do banco e outras, são importantes para que não ocorram essas fraudes.

Em contrapartida, desde a introdução do PIX no Brasil no ano de 2020, se observa o número de 400 milhões de chaves já cadastradas. Ocorre que, como já fora mencionado,

com o advento dessa plataforma, surgiram os golpes, que no mês de setembro e março de 2021, foram registrados pelo Banco Central o vazamento de três dados de usuários que utilizaram o PIX. Sendo assim, 576.785 chaves no ano de 2021 foram expostas, mesmo que evolvam apenas informações cadastrais (NASSIF, 2022).

No ano de 2022, foram realizadas 844.821 tentativas de golpes que envolvem o PIX no período entre janeiro e junho deste ano. Essa modalidade de golpe ficou muito popular entre os brasileiros que cresceu o número de 275% no primeiro semestre de 2022, se comparado ao mesmo período do ano anterior (OLIVEIRA; BRAGA; LAFORÉ, 2022).

No Brasil, o senador Chico Rodrigues propôs o Projeto de Lei 133 de 2022 como a Lei de Segurança do PIX, que poderá gerar mecanismos para permitir a rápida recuperação de valores transferidos por intermédio das fraudes cometidas pelo pagamento instantâneo. Esse projeto ainda prevê a criação de um código de segurança para que sejam utilizados pelas vítimas nos casos de sequestro relâmpago e permitir a realização da transferência e ainda emitir um alerta ao banco (PINHEIRO, 2022).

Em suma, se observa que o golpe do PIX está presente no Brasil com números alarmantes, mas, que é fundamental a realização de novas medidas que implementem maior segurança nessa seara.

O ESTELIONATO NO AMBIENTE VIRTUAL

Primeiramente, o crime de estelionato está disposto no Código Penal no rol dos crimes contra o patrimônio, no capítulo VI, que trata sobre o estelionato e outras fraudes. Com a seguinte redação no artigo 171:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis (BRASIL, 1940, s/p).

Com isso, se sabe que esse delito deriva da palavra grega “stelio” referente a um lagarto que altera sua cor para enganar as presas. Logo, essa referência é bem explicativa, tendo em vista que, o estelionato condiz com uma conduta típica do criminoso em induzir a vítima ao erro, fazendo a utilização de artifícios fraudulentos para que seja possível o alcance dos seus objetivos. Sendo assim, esse crime é patrimonial, não sendo utilizado a violência ou grave ameaça, mas, meios fraudulentos para que seja obtida a vantagem ilícita, tutelando a inviolabilidade do patrimônio (SILVA; SANTOS, 2021).

Para a configuração desse delito se faz necessário que sejam atendidos quatro requisitos, sendo eles: obtenção de vantagem ilícita; prejuízo para outra pessoa; a utilização de meio ardil; e que seja demonstrado a intenção do autor em enganar a vítima ou induzi-la ao erro de forma a que a vítima tenha uma percepção equivocada (SILVA; SANTOS, 2021).

Ademais, esse crime faz com que o agente manipule, iluda e engana a vítima, induzindo a entregar bens ou objetos, que, voluntariamente são entregues pelo fato de a vítima acreditar no criminoso, pensando estar agindo de boa-fé (SILVA; SANTOS, 2021).

Segundo Capez (2020), a expressão "vantagem ilícita" dispõe que está se trata do objeto material do delito e que caso o agente esteja agindo com uma vantagem devida, a conduta é considerada como exercício arbitrário das próprias razões, previsto no artigo Código Penal.

Consoante o artigo 171 do Código Penal, este delito pode ser cometido através de artificio, ou qualquer outro meio fraudulento. Dessa forma, Mirabete e Fabbrini (2021, p. 325) prelecionam:

> [...] o artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc.

Assim, para que a vítima seja enganada, o autor faz uso de algum artefato ou objeto para ludibria-la. Contudo com o Pacote Anticrime, a Lei nº 13.964 de 2019, foi alterada a natureza da ação penal no delito ora estudado, tornando-se pública incondicionada, com ressalva das exceções trazidas: "somente se procede mediante representação, se o crime previsto neste título é cometido em prejuízo: I do cônjuge desquitado ou judicialmente separado; II de irmão, legítimo ou ilegítimo; III de tio ou sobrinho, com quem o agente coabita", como assim dispõe o artigo 182 do Código Penal (BRASIL, 1940).

Em contrapartida, outro conceito importante a ser mencionado diz respeito aos crimes cibernéticos que se constituem como o cometimento de ilícitos através de computadores ou rede de internet, classificando de acordo com a sua forma de cometimento (WENDT; JORGE, 2012)

Com isso, no que diz respeito a natureza jurídica dos crimes cibernéticos, se observa a existência de várias correntes, mas, a que será adotada no presente trabalho é a de crimes cibernéticos próprios e impróprios. Sendo assim, os crimes próprios são aqueles

em que o agente ao cometer um delito necessita de um computador como meio de execução indispensável e possuindo como bens jurídicos afetados os dados em outra máquina ou rede. Já em se tratando dos impróprios, tem-se que são cometidos pela máquina, mas, que o bem jurídico tutelado não necessita ser afetado pelo computador (ORRIGO; FILGUEIRA, 2015).

Fazendo uma relação entre o conceito inicial do crime de estelionato e as noções de crimes cibernéticos, se estrai o estelionato virtual. Sendo assim, se sabe que o número de usuários da internet é grande, o que desencadeou um aumento considerável dos números de crimes virtuais. Justificado pela facilidade no manuseio dos meios virtuais e pela dificuldade em contemplar punições aos usuários, haja vista não ser fácil o encontro da identidade dos mesmos e ausência de normativas especificas nessa seara (SILVA; SANTOS, 2021).

Para tanto, há de se considerar que não é fácil de serem encontrados os autores dessa espécie de fraude o que vai em contraposição a facilidade de se cair nesses golpes, tendo em vista a existência do analfabetismo virtual.

Por isso, essa realidade não é diferente quanto ao estelionato, que vem fazendo inúmeras vítimas, agravando-se ainda mais com o surgimento da pandemia Covid19, pelo aumento dos usuários na internet. Diante disso, os criminosos criam páginas falas que oferecem oportunidades surreais, enviando em alguns casos mensagens via WhatsApp, que acabam enganando as vítimas mais vulneráveis (SILVA; SANTOS, 2021).

Acontece que o crime de estelionato sofreu uma recente atualização legislativa com o advento da lei nº 14.155 de 2021 acrescentando e alterando alguns parágrafos ao Código Penal. Sendo assim, o §2º passou a dispor de uma qualificadora do crime de estelionato, que não sendo praticado presencialmente, mas através da utilização de informações advindas das redes sociais, de contatos telefônicos, e-mail. Esse dispositivo ainda dispõe sobre a possibilidade da prática do crime de estelionato virtual (BRASIL, 2021).

Em se tratando do §2-Bº do artigo 171 do Código Penal, trouxe o aumento de pena de 1/3 para 2/3, nos casos em que o crime é praticado mediante a utilização de servidor estrangeiro, considerando a relevância do resultado gravoso e a dificuldade na localização e punição do agente. Outra importante alteração foi o § 4º do mesmo artigo que trouxe o aumento de pena no caso de estelionato contra idoso, sendo considerado como vulnerável.

Além disso, essa normativa ainda trouxe a alteração do artigo 70 do Código de Processo Penal sobre a competência para julgamento de alguns crimes de estelionato (BRASIL, 2021). Em suma, se observa que o critério para que seja estabelecido essa

competência, passa a ser o domicílio da vítima, determinado pela prevenção em caso de diversidade de vítimas. Portanto, em se tratando de estelionato mediante falsificação de cheque, a competência para julgamento será do juízo do local de obtenção do ilícito, assim como dispõe a súmula 48 do STJ (SILVA; SANTOS, 2021).

Portanto, em se tratando do âmbito criminal, é necessário que sejam realizadas perícias, mas que, na esfera civil, é necessária a discussão acerca da responsabilização das instituições financeiras, considerando a obrigatoriedade em garantir a segurança dos seus usuários.

RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES BANCÁRIAS

Com a crescente dos serviços prestados no âmbito digital, as fraudes pela Internet aumentaram. Assim, as migrações das pessoas para o mobile e internet banking, foram surgindo, dentre elas as pessoas que não tinham contato com nenhuma instituição financeira e que precisou no período da pandemia abrir contas digitais para conseguir receber o auxílio do governo, incluindo os idosos com uma dificuldade grotesca para compreender as tecnologias atuais, levando os criminosos a aumentarem as fraudes através da engenharia social, phishing e pharming (GONÇALVES, 2021).

Segundo os levantamentos realizados pela FEBRABAN (2020), foi constatado que neste ano as tentativas de fraudes financeiras pelo phishing contra brasileiros aumentaram em 80%. Acontece que, na maioria desses golpes não existe invasão, sendo uma atitude da própria vítima por ser enganada pelos fraudadores. Logo, apenas investir em segurança do setor de tecnologia de informação não é suficiente para evitar a ocorrência dessas fraudes, sendo necessário que sejam implementadas novas medidas de segurança.

Para tanto, com a finalidade de proteger o consumidor de futuras fraudes, o sistema do PIX, implementou em novembro de 2021 mecanismos de devolução de valores transferidos em casos de erros ou suspeitas de fraudes (GONÇALVES, 2021).

Contudo surgem questionamentos, tais como, essa atitude será suficiente para reduzir o número de fraudes bancárias relacionadas a transferências bancárias? O que será necessário para configurar uma suspeita de fraude pelos bancos?

Quando se fala em phishing, se sabe que o fraudador faz uso de características do banco na correspondência eletrônica que é enviada ao consumidor, que inocentemente preenche com seus dados pessoais e bancários voluntariamente. Assim, com os dados colhidos, os fraudadores acessam sua conta bancária livremente, inexistindo invasão ou

quebra no sistema do banco. Logo, como se fundamenta a fraude, se não ocorreu invasão ao sistema bancário?

Portanto, com esse crescimento exacerbado das tecnologias digitais, e em consequência as fraudes nessa seara é importante que sejam estudadas as responsabilizações das partes nessa relação de consumo.

A Responsabilidade Civil do Fornecedor no Direito do Consumidor

O Código de Defesa do Consumidor, Lei nº 8078 de 1990 reconhece a relação de consumo no setor bancário, definindo como uma instituição financeira, em seu artigo 3º, §2, como fornecedora de serviços (BRASIL, 1990). Porém, mesmo estando expresso neste diploma normativo, por muitos anos se perpetuou a dúvida sobre a incidência deste nos serviços bancários.

Hodiernamente esse entendimento já está pacificado na jurisprudência, onde o Superior Tribunal de Justiça, na disposição da Súmula 297 estabelece ser aplicável o CDC às instituições financeiras (BRASIL, 2011).

Sabe-se que a finalidade o Direito do Consumidor é eliminar as desigualdades existentes entre o fornecedor e o consumidor, de modo a estabelecer o equilíbrio entre as partes nessa relação de consumo (CAVALIERI FILHO, 2019). Ocorre que, a internet já dispunha de diversos modelos de contratos para oferta e compra de produtos e serviços, o que aumentou a vulnerabilidade do consumidor nos negócios jurídicos.

Logo, ao reconhecer a vulnerabilidade do consumidor, o CDC atribuiu alguns ônus ao fornecedor, para que fossem garantidos a segurança da relação de consumo e os direitos do consumidor. Nesse sentido o jurista Bruno Miragem (2014) compreende que a finalidade desse instituto está voltada a contemplar a vulnerabilidade do consumidor em relação ao fornecedor e que é responsável por responder os danos que decorrem dessa relação.

Já em se tratando das mudanças trazidas pelo CDC, nos casos envolvendo vício ou defeito do produto ou serviço nas relações de consumo, se observou que passou a deixar de incumbir ao consumidor o ônus de comprovar a culpa ou dolo do fornecedor para assim responsabilizar. Logo, o fornecedor passou a ter o ônus da prova sobre os danos causados, de modo que existem excludentes de responsabilização diante da inexistência do nexo de causalidade em relação ao defeito do produto ou dano sofrido (GONÇALVES, 2021).

Com isso, o artigo 12 do CDC dispõe em seu §3º os casos em que o fabricante, construtor, produtor ou importador não serão responsabilizados se comprovados alguns

requisitos. Assim, a responsabilidade objetiva traz menção a hipótese em que se presume a culpa do fornecedor, exigindo ainda o nexo de causalidade. Logo, nos casos de inexistência desse nexo, não há que se falar em responsabilidade do fornecedor (GONÇALVES, 2021).

Em suma, o caso fortuito externo é passível de exclusão da responsabilização, tendo em vista que o produto ou serviço estaria resguardado pela excludente do artigo 14 §3, I do CDC. Por fim, o fortuito interno mesmo sendo imprevisível e inevitável quando relacionado a atividade do fornecedor e o acontecimento, não exclui a responsabilidade do fornecedor com base no risco do empreendedorismo (GONÇALVES, 2021).

Portanto, se sabe que consoante o Código do Consumidor, existe a relação de consumo quanto a entidade bancária, além de possuir a responsabilização objetiva, devendo responder pelos prejuízos causados a terceiros, independente de culpa.

O Risco Proveito do Setor Bancário

O risco advindo da atividade empresarial, ou o chamado de risco proveito, é uma das teorias existentes que justificam a responsabilidade civil objetiva, no que diz respeito a todas as pessoas, podendo ser física ou jurídica, no exercício da atividade empresarial que visa o lucro e cria riscos de danos a terceiros (GONÇALVES, 2021).

Para Carlos Roberto Gonçalves (2021), a responsabilidade civil objetiva seria o dano, o fornecedor, ou responsável que é responsabilizado independente de culpa. Nessa teoria, substitui-se a culpa pelo risco, que é fundada no princípio de que o dano é reparável em consequência ao exercício das atividades empresariais lucrativas em benefício próprio.

No caso dos bancos, um exemplo a ser destacado são os assaltos a clientes dentro das agências bancária ou em qualquer de suas dependências, apesar de o fato gerador do dano ter sido por culpa exclusiva de terceiros ainda é reconhecida a falha na prestação dos serviços do banco na justificativa de que é papel deste garantir a privacidade e segurança dos seus clientes em suas transações (GONÇALVES, 2021).

No caso, a aplicação da teoria do risco da atividade é um entendimento subjetivo, devendo ser observado caso a caso. Um exemplo disso, é o entendimento do STJ em afastar a responsabilidade do banco nas transações financeiras que sejam realizadas por terceiros sem autorização através de seus cartões pessoais e utilizando suas senhas (GONÇALVES, 2021).

Nesse caso, a responsabilidade civil do banco é excluída diante da exclusiva culpa do consumidor. Tendo em vista caber ao correntista a tutela de maior segurança possível das senhas, que é pessoal e intransferível. Assim, ao facilitar o acesso a essa senha o

consumidor agravou o risco de dano, passando a assumir os riscos da sua conduta (GONÇALVES, 2021).

Nos dois casos, o ato causador foi realizado por terceiro, não sendo nem o fornecedor, nem o consumidor, evidenciando que inexiste uma divisão entre o fortuito interno e o externo, abrindo espaço para que exista uma interpretação da aplicação do caso fortuito no caso concreto. Sendo assim, fortuito interno seria a incidência durante o processo de confecção do produto, não sendo possível se eximir da responsabilidade civil o fornecedor. Já em se tratando do fortuito externo, se sabe que é devido a ser alheio ao processo de elaboração do serviço uma vez que exclui a responsabilidade (GOMES, 2008).

Logo, o STJ, através da Súmula 479 dispõe sobre as instituições financeiras que respondem objetivamente pelos danos causados por fortuito interno relativo a fraudes e delitos que sejam praticados por terceiros nas relações bancária (BRASIL, 2012).

Com isso, essa Súmula abre lacunas ao deixar de especificar as fraudes praticadas por terceiros, que atribuem aos bancos a responsabilidade da reparação ou a sua aplicação quanto às fraudes virtuais.

Por fraude se entende pela caracterização de um ato ilícito ou de má-fé com o objetivo de obter vantagens para si ou para outrem. Assim, para Davia, Coggins e Wideman (1992), a fraude seria um ato que envolva uma ou mais pessoas que agem com a intenção de privar outra pessoa de um valor para seu enriquecimento.

Logo, a fraude é caracterizada através do dolo ou má-fé do agente. Sendo o dolo praticado civil ou penal, conforme preleciona Wanderley (2009). Assim, o setor bancário é um alvo recorrente utilizado pelos fraudadores, em especial na versão online.

Sendo assim, essas fraudes financeiras causam diversos prejuízos aos fornecedores e consumidores se sabe ainda que existe uma deficiência na literacia digital pela população brasileira. Ocorre que, essa limitação facilita na aplicação de fraudes bancárias no mundo digital, como a engenharia social e phishing.

Por engenharia social se entende como sendo um ato por parte do criminoso com o objetivo de enganar pessoas de boa-fé que forneçam o acesso a informações ou sistemas não autorizados. Assim, para Basta, Basta e Brown (2014), essa engenharia é utilizada para se obter uma vantagem ilícita da vítima.

Logo, essa engenharia social é uma persuasão utilizada para manipular a vítima a entregar informações usadas sem sequer a vítima saber que está sendo alvo do golpe. Nesse sentido o TJ SP julgou a apelação sobre a emissão e um boleto falso enviado após o

contato pelo site com o banco, não eximindo esta dos danos causados ao consumidor (SÃO PAULO, 2021).

Com isso, se observa que a engenharia social pode ser utilizada da forma que bem entender, bastando apenas que o criminoso disponha da habilidade de persuasão, prejudicando a percepção da fraude.

Phishing, é um termo que advém do inglês, e significa “pescar”, utilizado para estipular condutas fraudulentas cometidas no ambiente digital. Dessa forma, esse tipo de fraude faz o uso da engenharia social para enganar a vítima e obter informações pessoais e confidenciais (PINHEIRO, 2022).

No mais, essa modalidade de fraude é realizada através do envio de mensagem de texto, em especial por e-mail, como se fossem enviadas por instituições financeiras, loja ou instituições do governo para que o receptor dessa mensagem sem desconfiar aceite-a e execute-a nos termos assim dispostos, que contêm um vírus (GONÇALVES, 2021)

Com isso, se observa a dificuldade em controlar essas fraudes, tendo em vista serem realizadas por vários meios e com diferentes conteúdos capazes de instigarem, a curiosidade do receptor. Logo, mesmo com a conscientização das agências bancárias e do Governo Federal, ainda não são suficientes para evitar os crescimentos das vítimas dessa fraude.

Desse modo, ao ter acesso aos dados da vítima o fraudador passa a acessar livremente o sistema do banco, como se este fosse o legítimo usuário. Não decorrendo a fraude de um ataque ou invasão do fraudador ao banco. Nos casos de engenharia social, phishing, são aplicáveis as teorias do risco-proveito, da culpa exclusiva do consumidor e a responsabilidade exclusiva de terceiros (GONÇALVES, 2021).

Ocorre que, nos casos em que não se utilizou o aplicativo bancário para consumar a fraude, a teoria adotada é a da culpa exclusiva da vítima, como por exemplo nos e-mail ou SMS enviados para pagamento de boleto, fundamentado pela ausência de cautela mínima para a realização do negócio jurídico (GONÇALVES, 2021)

Nos casos em que o consumidor disponibiliza seus dados bancários através da internet, sem que sejam tomadas as devidas precauções, e sejam realizadas transações por terceiros, se entende que a criação do risco é a mesma do caso anterior, tendo em vista que o consumidor facilitou a fraude ao disponibilizar dados pessoais e intransferíveis. Porém, nesse segundo exemplo já existe um entendimento pacificado pelo STJ que dispõe acerca da ausência de responsabilidade da instituição financeira pela falha na guarda dos dados (REINALDO FILHO, 2008).

Portanto, nos casos em que existe a culpa exclusiva do consumidor, seja por ineficiência na guarda dos seus dados bancários, não há que se falar em responsabilização, já nos casos envolvendo a engenharia social, phishing, são aplicáveis a teoria do risco proveito.

RESPONSABILIDADE DO BANCO NAS TRANSAÇÕES FEITAS POR INTERMÉDIO DO PIX

A regra é a de que o banco não possui a responsabilidade nos crimes cometidos pela utilização do PIX, isso se justifica pelo fato de que em um sequestro, por exemplo, a própria vítima coloca o *login* de acesso ao aplicativo do banco e faz a transferência. Assim, o banco não contribui com a fraude desse delito (SILVA, 2021).

Ocorre que as decisões relacionadas a essa temática atribuem aos bancos a responsabilidade em dois casos: o primeiro quando a vítima entrar em contato com a instituição financeira logo após o crime, requerendo o bloqueio imediato dos valores da sua conta, mas não foram atendidas; o segundo quando existe a suspeita de invasão do aplicativo. Ainda existe a possibilidade de conta fraudada criada pelo criminoso em nome de um terceiro, que não tenha conhecimento desta, configurando ainda a responsabilidade do banco, pelo fato de que a instituição permitiu a abertura da conta sem a devida análise documental (SILVA, 2021).

Logo, conforme mencionado anteriormente, a Súmula 479 traz a responsabilização objetiva das instituições financeiras pelos danos gerados por fortuitos internos relativos a estas modalidades de fraudes contra terceiros nas operações bancárias. Significando em tese, que os bancos arquem com os prejuízos em caso de invasão de hackers, fraudes no sistema e outros problemas (SILVA, 2021).

Com isso, mesmo o banco alegando não possuir culpa pelo ocorrido, normalmente não é possível comprovar processualmente sua afirmação. Assim, nesses casos de golpe do PX, se verifica a inobservância dos deveres de proteção e segurança que são trazidos pelo CDC em seu artigo 6º, inciso I e artigo 14, §1º, de forma que o banco se responsabiliza pelos danos suportados pelo autor, consoante a Súmula 479 do STJ (BLANCO, 2022).

Por sua vez, no que diz respeito as boas práticas e governança, disposta nos artigos 50 e 51 da LGPD, se sabe que os controladores e operadores, em relação a suas competências, no tratamento de dados pessoais, podem formular regras sobre boas práticas e de governança.

O que se entende por governança, é o sistema onde as empresas e demais organizações são dirigidas, monitoradas em relação aos relacionamentos entre sócios, conselho administrativo, diretoria e outras partes interessadas. Já no que se refere as boas práticas de governança, se sabe que são a conversão de princípios básicos que alinham interesses com a finalidade de preservar e otimizar o valor da empresa em longo prazo, de modo a facilitar seu acesso a recursos e a contribuição para a qualidade de uma gestão organizada (IBGC, 2018).

Sendo assim, o tratamento é realizado pelo controlador que é a pessoa natural e jurídica que decidirá sobre qualquer questão que envolva a manipulação de dados e operador de dados, pessoa natural ou jurídica que realizará este tratamento consoante o que o controlador definir (BRASIL, 2018).

Sendo assim, ambos poderão ser responsabilizados quando causares danos a outra pessoa no exercício da atividade, consoante o artigo 42 da LGPD. Além disso, se sabe que não existe um entendimento pacificado quanto a responsabilidade do controlador e do operador, mas que segundo Mazon (2021), existe uma responsabilização sui generis, valendo a análise da responsabilidade objetiva que é protetiva do CDC e que é aplicada nos casos em que houverem danos sofridos pelo titular dos dados na relação consumerista.

Ainda assim, a falha na aplicação da segurança resulta em dano moral à parte autora, devido ao prejuízo patrimonial, sem qualquer apoio da instituição financeira. Ainda assim, essa indenização possui o viés de prestação pecuniária, servindo para compensar a lesão no direito de personalidade da vítima e caráter pedagógico para que sejam evitadas futuras fraudes como as ocorridas (BLANCO, 2022).

Nessa margem o Tribunal de Justiça do Estado de São Paulo julgou a agência bancária como sendo responsável pelos danos sofridos pelo autor no golpe do PIX. Dispondo ainda que o banco teria prestado serviço com defeito (SÃO PAULO, 2021).

Portanto, observa-se que a agência bancária tem responsabilidade nos casos do golpe do PIX, devendo ainda em alguns casos indenizar o autor como foi demonstrado em uma recente decisão do Tribunal de Justiça do Estado de São Paulo. Além disso, se verifica que os golpes se tornaram mais eficientes e burlam sistemas de segurança de modo a enganar as vítimas e tendo como solução que sejam promovidas uma educação digital, bem como o contato direto com o correntista, haja vista os avisos sobre boas práticas e segurança.

CONSIDERAÇÕES FINAIS

Inicialmente o PIX surgiu para dinamizar as operações bancárias de transferências de valores entre contas e pagamentos instantâneos, vinculado ao Banco Central tornando possível que fossem realizadas transações de forma rápida, segura, simples e barata. Além disso, se observou que o golpe do PIX se faz presente no Brasil com números alarmantes, sendo fundamental a realização de novas medidas para atribuir maior segurança.

Não obstante, restou evidente o crime de estelionato está voltado no fato de o agente manipular, iludir e enganar a vítima, induzindo a entregar bens ou objetos, que, voluntariamente são entregues pelo fato de a vítima acreditar no criminoso, pensando estar agindo de boa-fé. Além disso, foi constatada a natureza jurídica dos crimes cibernéticos em própria e imprópria, o que se verifica no Golpe do PIX.

Posteriormente, restou apurado com a fusão dos conceitos de crime de estelionato e as noções de crimes cibernéticos, se estrai o estelionato virtual. Logo, tornou-se uma realidade com maior frequência após o surgimento da pandemia Covid-19, devido ao aumento dos usuários na internet.

Nesse sentido, foi constatado através da análise do Código do Consumidor, de súmulas do STJ e leis que é possível a responsabilização civil objetiva das instituições bancárias sobre o golpe do PIX, nos casos em que as vítimas entrem em contato com a agencia lodo após o delito e quando a suspeita de invasão dos aplicativos.

Contudo, verificou-se diariamente que os tribunais têm se posicionado a ofertar melhores interpretações sobre a temática, mas que se trata de uma questão ainda é recente, mas que vem evoluindo nos últimos anos, proporcionando maior segurança jurídica. Portanto, ainda é necessário que sejam ofertadas decisões mais severas na responsabilização civil objetiva, para que assim seja possível maiores investimentos em segurança.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. **Sistema de Pagamentos Brasileiro**. Gov.br. 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pix. Acesso em: 11 out. 2022.

BASTA, A. BASTA, N. BROWN, M. **Segurança de Computadores e teste de invasão**. 2 ed. São Paulo: Saraiva, 2014.

BLANCO, K. **Banco é responsabilizado no caso de Golpe do PIX**. 2022. Disponível em: 14 out. 2022.

BRANCO, D. C. **Golpes no Pix: veja como funcionam as duas principais abordagens dos criminosos**. 2021.

BRASIL. **Decreto Lei nº 2.848**, de 7 dezembro de 1940. Código Penal. Brasília: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 13 out. 2022.

BRASIL. **Lei nº 8078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 14 out. 2022.

BRASIL. **Lei complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm. Acesso em: 7 nov. 2022.

BRASIL. Superior Tribunal de Justiça (Segunda Seção). **Súmula n. 297**. O Código de Defesa do Consumidor é aplicável às instituições financeiras. RSSTJ, a. 5, (23): 243-314, outubro 2011.

BRASIL. Superior Tribunal de Justiça (Segunda Seção). **Súmula n. 479**. RSSTJ vol. 43 p. 179, 2012.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília: Presidência da República, 2018. Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 7 nov. 2022.

BRASIL. **Portaria nº 97.909, de 3 de maio de 2018**. Institui grupo de trabalho temático, no âmbito do Fórum AIP, de que trata a Portaria nº 85.478, de 23 de junho de 2015. Diário oficial da União: Publicado em: 7 mai. 2018, ed. 86, s. 2, p. 46. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/13152573/Imprns_Nacional. Acesso em: 7 nov. 2022.

BRASIL. **Resolução BCB nº 12, agosto de 2020**. Institui o arranjo de pagamentos PIX e aprova o seu regulamento. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=1. Acesso em: 07 nov. 2022.

BRASIL. **Lei nº 14.155 de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 13 out. 2022.

CAPEZ, F. **Parte especial arts. 121 a 212**: coleção curso de direito penal. 20. ed. São Paulo: Saraiva Educação, 2020.

CAVALIERI FILHO, S. **Programa de direito do consumidor**. 5. ed. São Paulo: Atlas, 2019.

DAVIA, H. R.; COGGINS, P. C.; WIDEMAN, J. C. **Management accountant`s guide to fraud discovery and control**. Nova York: Wiley, 1992.

FEBRABAN - Federação Brasileira de Bancos. **Observatório FEBRABAN dezembro 2020.** Disponível em: https://www.google.com/url. Acesso em: 14 out. 2022.

GOMES, L. F. **Qual a diferença entre caso fortuito externo e interno**. JusBrasil. 2008. Disponível em: Acesso em: 07 nov. 2022.

GONÇALVES, C. R. **Direito civil brasileira responsabilidade**. 16. ed. São Paulo: Saraiva Educação, 2021.

IBGC - Instituto Brasileiro de Governança Corporativa. **Código das melhores práticas de governança corporativa**. 2018. p. 20. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138. Acesso em: 16 nov. 2022.

MAZON, F. A. **Responsabilidade civil do controlador/ operador de dados pessoais no âmbito da lei 13709 de 2018**. 2021. Disponível em: http://45.4.96.19/bitstream/aee/18223/1/Filipe%20Augusto%20Mazon.pdf. Acesso em: 16 nov. 2022.

MIRABETE, J. F.; FABBRINI, R. N. **Manual de direito penal. Parte especial**: arts. 121 a 234-B do CP. 36. ed. São Paulo: Atlas, 2021.

MIRAGEM, B. **Curso de direito do consumidor**. 5. ed. São Paulo: Revista dos Tribunais, 2014.

NASSIF, T. **Golpistas cruzam chaves vazadas de Pix com outros dados para aplicar novas fraudes.** CNN Brasil. 2022. Disponível em: https://www.cnnbrasil.com.br/business/golpistas-cruzam-chaves-vazadas-de-pix-com-outros-dados-para-aplicar-novas-fraudes/. Acesso em: 11 out. 2022.

OLIVEIRA, B. BRAGA, D. LAFORÉ, B. **Tentativas de golpes com PIX aumentam quase 1.200 % no 1º semestre, aponta pesquisa**. CNN Brasil. 2022. Disponível em: https://www.cnnbrasil.com.br/business/tentativas-de-golpes-com-pix-aumentamquase-1-200-no-1o-semestre-aponta-pesquisa/. Acesso em: 11 out. 2022.

ORRIGO, G. M. A. FILGUEIRA, M.H.B. **Crimes cibernéticos: uma abordagem jurídica sobre os crimes realizados no âmbito virtual**. Jus. 2015. Disponível em: https://jus.com.br/artigos/43581/crimes-ciberneticos-uma-abordagem-juridica-sobreos-crimes-realizados-no-ambito-virtual. Acesso em: 12 de out. 2022.

PINHEIRO, R. **PL institui a "Lei de segurança do PIX".** Senado Notícias. 2022. Disponível em: https://www12.senado.leg.br/noticias/audios/2022/02/pl-institui-a-201clei-de-seguranca-do-pix201d. Acesso em: 13 out. 2022.

REINALDO FILHO, D. A responsabilidade dos bancos pelos prejuízos resultantes do "phishing". **Revista Jus Navigandi**, Teresina, ano 13, n. 1836, 11 jul. 2008. Disponível em: https://jus.com.br/artigos/11481. Acesso em: 14 out. 2022.

SÃO PAULO. Tribunal de Justiça (2ª Turma Recursal Cível e Criminal). **RI 55.2021.8.26.0278**. Relator Eduardo Calvert. Data do julgamento: 31/05/2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1225665110. Acesso em: 15 out. 2022.

SCHAAL, F.M.M. QUINELATO, P.D. GOULART, M. **Pix- Lgpd, marcas, disputas e cenário financeiro digital**. 2021. Disponível em: https://muradpma.com/wpcontent/uploads/2021/03/pix_news.pdf. Acesso em: 11 out. 2022.

SILVA, O. J. da. **Responsabilidade dos bancos nas transações realizadas por meio do PIX**. JusBrasil, 2021. Disponível em: https://orlandojsilva.jusbrasil.com.br/artigos. Acesso em: 14 out. 2022.

SILVA, F. J. SANTOS, R.J. M. **Estelionato praticado por meio da internet: Uma visão acerca dos crimes virtuais**. Anima educação, 2021. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/18080/1/TCC%2001.12.21%20dep%C3%B3sito%20final.pdf. Acesso em: 13 out. 2022.

SÃO PAULO. Tribunal de Justiça (22ª Câmara de Direito Privado). **Apelação Cível 102397051.2020.8.26.0506**. Relator (a): Ana de Lourdes Coutinho Silva da Fonseca; Órgão Julgador: 13ª Câmara de Direito Privado; Foro de Ribeirão Preto 4ª Vara Cível; Data do Julgamento: 23/09/2021; Data de Registro: 24/09/2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1360644563. Acesso em: 14 out. 2022.

WANDERLEY, M. O. M. **Fraude à norma de incidência**: reflexões jurídico tributárias. São Paulo: EdIBET, 2009.

WENDT, E.; JORGE, H. V. N. **Crimes cibernéticos**: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012. p 10.