A RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS EM CASOS DE FRAUDES DECORRENTES DE *PHISHING* E *PHARMING*

Midiã Vitória Chaves, Fernanda Frois Faria.

Universidade do Vale do Paraíba/ Faculdade de Direito, Praça Cândido Dias Castejón, Centro – 12245-914 - São José dos Campos-SP, Brasil, midia.vchaves@gmail.com, ffrois@univap.br.

Resumo

O presente artigo analisa a responsabilidade civil das instituições financeiras nos casos de fraudes eletrônicas de *Phishing* e *Pharming*, fenômeno intensificado pela crescente digitalização dos serviços bancários e pelo surgimento de golpes cibernéticos, o que suscita novos desafios jurídicos. O estudo investiga a aplicação da legislação consumerista, da LGPD e da jurisprudência pátria, com destaque para a Súmula 479 do STJ, no intuito de delimitar os contornos da responsabilidade dos Bancos em tais hipóteses. A metodologia utilizada foi a pesquisa bibliográfica, legislativa e jurisprudencial. Os resultados demonstraram que, nos casos de *Phishing*, a responsabilização do Banco tende a ser afastada quando comprovada culpa exclusiva da vítima, devido à natureza do ataque. Contudo, no *Pharming*, dada a imperceptibilidade da fraude, a responsabilidade recairá sobre a instituição financeira, sobretudo quando verificada a falha na adoção de medidas preventivas eficazes. Conclui-se que, embora a responsabilidade objetiva prevaleça nas relações de consumo, essa deve ser relativizada conforme a conduta da vítima, a segurança da plataforma e a complexidade do ataque.

Palavras-chave: Responsabilidade Civil. Fraude. *Phishing. Pharming*. Instituição financeira.

Área do Conhecimento: Ciências Jurídicas. Direito Privado.

Introdução

A contemporaneidade é marcada pela ascensão vertiginosa das tecnologias digitais, fenômeno que transformou as formas de comunicação, consumo e, especialmente, a prestação de serviços financeiros, consolidando o internet banking como ferramenta essencial para a vida moderna. Contudo, esse mesmo avanço tecnológico serviu de terreno fértil para o surgimento de práticas fraudulentas sofisticadas, como o *Phishing* e o *Pharming*. Tais modalidades de fraude digital se destacam por explorar vulnerabilidades humanas e técnicas, visando a subtração de dados sensíveis e movimentações indevidas, o que amplifica a complexidade da responsabilização pelos danos enfrentados pelos clientes.

Para Silva (2021), o *Phishing* por sua vez, é caracterizado por sua menor sofisticação e maior flexibilização. A prática consiste no envio de comunicações eletrônicas, como e-mails, que imitam com alta similaridade a identidade visual e o domínio das Instituições Financeiras. O mecanismo de ataque se desenvolve em duas etapas complementares: a primeira consiste no envio da mensagem com um link embutido e, a segunda, na ação consciente do usuário que, ao acessar o link, insere dados sensíveis (como números de cartão e documentos pessoais), momento em que os fraudadores adquirem os meios necessários para invadir a conta da vítima.

Já o *Pharming* configura-se como uma modalidade de fraude eletrônica de elevada complexidade, atuando de forma imperceptível ao usuário. Ao contrário do *Phishing*, sua eficácia independe da interação consciente com conteúdo suspeito, operando de maneira automatizada mediante a inserção de softwares maliciosos ou arquivos ocultos no dispositivo. A técnica modifica elementos do sistema do computador e redireciona o usuário, mesmo quando este digita corretamente o endereço oficial, para um site fraudulento visualmente idêntico ao portal bancário. Essa perfeita simulação, que não apresenta sinal aparente de irregularidade, revela o caráter insidioso do *Pharming* e sua capacidade de enganar até mesmo usuários cautelosos (Silva, 2021, p.47).

Diante desse cenário, a discussão reside na delimitação dos deveres de segurança e informação por parte das Instituições Bancárias, e na aplicação das normas do Código de Defesa do Consumidor

(CDC), notadamente quanto à responsabilidade objetiva nas relações de consumo. Além disso, é crucial analisar as implicações da Lei Geral de Proteção de Dados (LGPD) na prevenção de fraudes e na proteção de dados sensíveis dos clientes. Dessa forma, o presente artigo tem como objetivo examinar, sob uma abordagem doutrinária, legislativa e jurisprudencial, a responsabilidade civil dos Bancos diante das fraudes por *Phishing* e *Pharming*, refletindo sobre os limites da imputação de responsabilidade às instituições financeiras e os critérios jurídicos para sua eventual responsabilização.

Metodologia

A metodologia adotada neste estudo baseia-se em uma abordagem exploratória, fundamentada na análise abrangente, incluindo o exame de processos judiciais, a consulta de doutrina especializada, o exame da legislação vigente, além de estudos contemporâneos sobre responsabilidade civil das instituições financeiras em ambientes virtuais. A análise processual permitiu a identificação de precedentes e a aplicação prática das normas envolvidas. A doutrina foi selecionada para um embasamento teórico consistente e orientar as interpretações jurídicas. A legislação vigente foi analisada criticamente, com destaque para o Código Civil (Lei nº 10.406/2002), o Código de Defesa do Consumidor (Lei nº 8.078/1990) a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), em especial os artigos que tratam da responsabilidade por danos, proteção de dados e fraudes. Além disso, foram consultadas decisões recentes do Superior Tribunal de Justiça (STJ) para verificar o entendimento predominante dos tribunais superiores quanto à aplicabilidade da responsabilidade objetiva e aos critérios para exclusão do dever de indenizar.

Resultados

A análise da responsabilidade civil das instituições financeiras frente às fraudes cibernéticas, em especial o *Phishing* e o *Pharming*, revela um cenário jurídico de grande complexidade e crescente debate. As decisões judiciais e os posicionamentos doutrinários indicam que a imputação de responsabilidade aos Bancos depende da identificação da natureza do dano, da conduta das partes envolvidas e do nexo causal entre o serviço prestado e o prejuízo suportado pelo consumidor.

Verificou-se que os tribunais superiores, em especial o STJ, têm adotado o entendimento que condiciona a responsabilização das instituições financeiras à comprovação de falha na prestação de serviço ou à ausência de segurança adequada nas operações eletrônicas. No caso de *Phishing*, em que o consumidor interage diretamente com uma comunicação fraudulenta, algumas decisões têm afastado a responsabilidade da instituição quando comprovada culpa exclusiva da vítima.

Já nos casos de *Pharming*, nos quais o redirecionamento malicioso independe de ação do usuário apresentando maior sofisticação técnica e reduzida perceptibilidade por parte do usuário, o que torna sua identificação extremamente difícil, mesmo por clientes diligentes, a atuação da vítima raramente contribui para o resultado danoso, motivo pelo qual a responsabilização do Banco demanda um exame probatório mais rigoroso e criterioso, a equiparação entre essas duas modalidades não se revela adequada, tendo em vista o distinto grau de complexidade de cada uma, bem como os diferentes níveis de atenção exigidos dos usuários para detectar a fraude virtual a que foram submetidas (Silva, 2021, p.60)

A pesquisa também identificou que, mesmo nos casos em que as instituições bancárias disponibilizam orientações em seus sites e canais de atendimento, tal iniciativa, isoladamente, não é suficiente para eximi-las da obrigação de indenizar, especialmente quando não forem adotadas medidas preventivas concretas, como autenticação em múltiplas etapas, notificações automáticas de transações suspeitas ou bloqueio de movimentações atípicas.

Sob a ótica da legislação consumerista, os Bancos são considerados fornecedores de serviços, e os clientes, consumidores, relação esta regida pelo Código de Defesa do Consumidor (Brasil, 2025a) que impõe responsabilidade objetiva por falha na segurança dos serviços. A Súmula 297 do STJ reforça essa condição, estendendo a aplicação do CDC às Instituições financeiras (Brasil, 2025e). No entanto, julgados ainda mais recentes demonstram a mera ocorrência do prejuízo não gera automaticamente o dever de indenizar, sendo indispensável a análise do comportamento do consumidor e das medidas de segurança adotadas pela instituição.

Por outro lado, a Lei Geral de Proteção de Dados (LGPD) tem ampliado os parâmetros para responsabilização dos agentes de tratamento de dados, incluindo os Bancos, especialmente nos casos

em que a vulnerabilidade na guarda de informações pessoais contribui para a efetivação do ilícito. A falta de transparência sobre o tratamento de dados e a ausência de mecanismos de proteção podem ser interpretados como violação dos princípios de boa-fé, segurança e prevenção previstos na LGPD (Brasil, 2025c).

Assim, apesar dos crimes de *Phishing* e *Pharming* serem praticados por terceiros, a posição privilegiada dos Bancos na relação contratual e seu domínio técnico sobre as plataformas digitais justificam a imposição de um dever reforçado de diligência. O reconhecimento de sua responsabilidade, ainda que não absoluta, decorre do risco da atividade e da necessidade de proteger o consumidor diante da assimetria técnica e informacional que caracteriza as transações bancárias eletrônicas.

Discussão

O crescente volume de fraudes eletrônicas envolvendo *Phishing* e *Pharming* no âmbito bancário coloca em discussão os limites da responsabilidade civil das instituições financeiras, exigindo do ordenamento jurídico respostas compatíveis com a nova realidade digital. Ao explorar esse cenário, torna-se evidente que a aplicação da responsabilidade objetiva, nos termos do Artigo 14 do CDC (Brasil, 2025a), é o ponto crucial do debate, sobretudo em razão da hipossuficiência técnica e informacional do consumidor frente aos riscos inerentes às operações eletrônicas.

Além disso, a responsabilização do Banco, o intermediário na relação jurídica, é essencial, tendo em vista que identificação e punição do criminoso autor da fraude são, na prática, inviáveis. Assim, a definição clara das responsabilidades das instituições financeiras e demais atores envolvidos torna-se um pilar para garantir a segurança dos usuários, conforme ressalta Reinaldo Filho (2020).

A responsabilidade objetiva, aquela que independe de culpa, exigindo somente a comprovação da conduta, do nexo de causalidade e do dano, foi concebida para equalizar o desequilíbrio estrutural entre fornecedor e consumidor. Nesse sentido, o Banco, enquanto fornecedor de serviços essenciais, deve responder pelos riscos das atividades que desenvolve, inclusive por danos decorrentes de falhas de segurança no ambiente digital.

Embora a Súmula 479 do STJ (Brasil, 2025f) disponha que “as instituições financeiras respondem objetivamente pelos danos gerados por fortuito relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias”, é fundamental ressaltar que estão ressalvadas as hipóteses de caso fortuito, força maior ou culpa exclusiva da vítima, com base nas excludentes de responsabilidade civil objetiva, observando o § 3º do artigo 14 do CDC (Brasil, 2025a).

Conforme Gagliano; Pamplona Filho (2024), a responsabilidade civil configura-se como uma obrigação sucessiva que decorre da prática de um ato lesivo, sendo o dever de indenizar consequência jurídica imposta ao agente pela violação da ordem jurídica. Tal instituto pode apresentar-se de forma simples, quando o agente responde por ato próprio, ou complexa, quando há responsabilização por fato de terceiro, em virtude de previsão legal, como nos casos de fraudes.

Nesse contexto, a distinção entre responsabilidade contratual e extracontratual assume papel relevante para a adequada compreensão dos deveres atribuídos às Instituições financeiras diante de fraudes praticadas por terceiros. Em regra, a relação entre Banco e cliente é de natureza contratual, regida pelos princípios da boa-fé, confiança legítima e segurança na prestação do serviço, princípios esses expressos no Artigo 422 do Código Civil (Brasil, 2025b) e amplamente reforçados pela principiologia do Código de Defesa do Consumidor.

Contudo, as fraudes praticadas por terceiro podem configurar uma violação a direitos extrapatrimoniais, impondo ao Banco um dever de vigilância indireta, derivada de sua posição privilegiada na cadeia de consumo. É nesse ponto que se insere a crítica acerca da necessidade de o sistema jurídico responsabilizar os agentes mais bem posicionados técnica e financeiramente para prevenir o dano.

Mesmo em hipóteses nas quais o Banco não seja o causador direto do dano, sua obrigação contratual pressupõe a assunção de um dever de resultado, cuja inexecução acarreta, por si só, a presunção de culpa, uma vez que a responsabilidade contratual exige vínculo jurídico prévio entre as partes e decorre do inadimplemento de uma prestação que constitui o objeto do contrato, qual seja a segurança, eficácia e confiabilidade na prestação de serviço, sendo portanto, a culpa contratual a violação direta de um dever assumido (Gagliano; Pamplona Filho, 2024).

Assim, nos termos do Artigo 14 do CDC (Brasil, 2025a), os prestadores de serviços, categoria na qual se enquadram os Bancos, respondem objetivamente pelos danos causados aos consumidores em

razão dos defeitos relativos à prestação do serviço. De modo igual, o Código Civil, em seu Artigo 927 (Brasil, 2025b), impõe o dever de reparar o dano àquele que, por ato ilícito, violar direito e causar prejuízo a outrem, sendo essa responsabilidade subjetiva na regra geral, mas podendo ser objetiva quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Portanto, diante da relação contratual e da natureza arriscada da atividade bancária, é possível fundamentar a responsabilização objetiva das instituições financeiras tanto pelo CDC quanto pelo Código Civil, em razão do risco da atividade, aplicando-se o diálogo de fontes, sobretudo quando não demonstrada culpa exclusiva da vítima ou inexistência do defeito na segurança do serviço.

A fraudes de *Phishing*, que demandam uma ação da vítima ao clicar em links ou fornecer seus dados, têm sido analisadas com mais cautela pelos tribunais, especialmente quando há indícios de negligência do consumidor. Em julgamento recente, o STJ afirmou que “a instituição não pode ser responsabilizada automaticamente por fraudes eletrônicas se comprovado que o consumidor agiu com culpa exclusiva ao fornecer seus dados pessoais e sensíveis a terceiro” (Brasil, 2024d)

O Tribunal de Justiça de São Paulo, no processo nº 1001692-87.2024.8.26.0030, ainda acerca do *Phishing,* negou provimento à apelação do autor ao entender que houve contribuição decisiva do autor para a consumação do golpe. Tratando-se de fortuito externo, reconheceu a excludente de responsabilidade prevista no Artigo 14, § 3º, II do CDC, afastando o nexo causal entre o serviço bancário e o dano experimentado. Assim, não se evidenciando falha na prestação do serviço. (São Paulo, 2025a).

De forma semelhante, nos autos nº 1006343-34.2024.8.26.0008, o mesmo Tribunal destacou que as operações realizadas não destoavam do perfil do correntista, e ressaltou que golpes dessa natureza são públicos e notórios, sendo objeto de campanhas de prevenção, inclusive no site do Banco réu. Assim, exigiu-se maior cautela do “homem médio” e reconheceu-se novamente o fortuito externo, afastando a responsabilidade da instituição financeira e declarando inaplicáveis tanto o Enunciado n. 14 do TJSP quanto a Súmula n. 479 do STJ (São Paulo, 2025b).

Por outro lado, nos casos de *Pharming* – a fraude ocorre independentemente da ação do usuário, mediante redirecionamento invisível a sites falsos por meio de malware, sem que o consumidor perceba – nota-se uma preocupante equivocidade ao equiparar, sem a devida distinção técnico-jurídica à fraude supracitada. Essa equiparação simplista desconsidera elementos essenciais à análise da responsabilidade civil, em especial no que tange a sofisticação tecnológica, imperceptibilidade do ataque e a ausência de contribuição da vítima do ataque.

A conduta da vítima no *Pharming* é, em certa medida, neutra. O ataque é caracterizado pela alteração técnica de elementos do sistema de navegação do usuário,de modo que, mesmo digitando corretamente o endereço oficial do Banco, a vítima é redirecionada a uma página falsa, visualmente idêntica ao site legitimo, assim, trata-se de um ataque invisível aos olhos do consumidor. Dessa forma,a invisibilidade do ataque leva à discussão do afastamento, em tese, da aplicação do Artigo 14, § 3º, II, do Código de Defesa do Consumidor, que exige culpa exclusiva da vítima para que se configure excludente de responsabilidade.

Nesse sentido, na Apelação Cível nº 1105851-36.2022.8.26.0100, o Tribunal de Justiça de São Paulo reconheceu a responsabilidade objetiva da instituição financeira diante de movimentações indevidas realizadas por meio de site clonado (São Paulo, 2023c). Embora a decisão tenha corretamente identificado a falha na prestação de serviço bancário, fundamentado no Artigo 14 do CDC, ao classificar o caso como fraude decorrente de *Phishing,* incorreu um erro conceitual.

A fraude em questão resultou na vinculação de novo dispositivo e na realização de treze transferências via PIX em curto intervalo de tempo, sem que o Banco demonstrasse culpa exclusiva da vítima ou apresentasse mecanismos eficazes para impedir a movimentação atípica. Assim, ainda que a responsabilidade tenha sido corretamente atribuída à instituição financeira, o acórdão revela uma certa deficiência conceitual relevante, pois a não distinção entre *Phishing e Pharming* compromete a coerência da fundamentação jurídica e a adequada compreensão do risco tecnológico envolvido.

A jurisprudência tem consolidado o entendimento de que as instituições financeiras devem implementar sistemas robustos de segurança, sendo responsáveis caso se verifique vulnerabilidade no sistema de autenticação, ausência de avisos de movimentação ou demora no bloqueio da conta após a detectação da fraude, como visto no caso supracitado, corroborando então para a imputação da responsabilização às instituições.

Importa ressaltar que o dever de informação, previsto tanto no Código de Defesa do Consumidor quanto na Lei Geral de Proteção de Dados Pessoais, e nos princípios fundamentais da relação contratual, com fulcro no Artigo 422 do Código Civil, é de observância obrigatória e não se satisfaz com meros alertas genéricos em sites institucionais, visto que se trata de um dever anexo à prestação principal, impondo obrigações que vão além do que está expresso no contrato, exigindo das partes transparência e lealdade na comunicação.

A falta de informação devida pode ser considerada como uma conduta ilícita, seja no âmbito contratual ou fora dele, dando ao consumidor o direito de indenização, uma vez que ficou impossibilitado de tomar decisões informadas quanto aos riscos existentes. (Tartuce, 2021)

No campo normativo, a aplicação da Lei Geral de Proteção de Dados Pessoais alcança diretamente as instituições financeiras, que devem observar com rigor os dispositivos legais, considerando que detêm acesso não apenas a dados pessoais, mas também a dados sensíveis de seus clientes. Nesse contexto, qualquer descuido no tratamento dessas informações pode não apenas viabilizar fraudes, uma vez que a fragilização dos danos permite a atuação de fraudadores, como também gerar penalidades administrativas.

De acordo com o Artigo 46 do mesmo diploma (Brasil, 2025c), o controlador de dados, como é o caso das Instituições financeiras, deve adotar medidas eficazes de prevenção contra acessos não autorizados, bem como contra situações acidentais ou ilícitas. O descumprimento desses deveres, por sua vez, pode acarretar não apenas sanções administrativas, mas também responsabilização civil pelos danos eventualmente causados.

Em suma, a discussão em torno da responsabilidade civil das instituições financeiras diante de fraudes como *Phishing* e *Pharming* exige a harmonização entre proteção do consumidor, preservação da segurança jurídica e delimitação precisa das obrigações contratuais. O reconhecimento da responsabilidade não deve ser automático, mas deve fundamentar-se análise concreta da conduta de ambas as partes, dos mecanismos preventivos adotados e do nexo causal entre o serviço prestado e o dano sofrido.

Conclusão

Este artigo analisou a responsabilidade civil das instituições financeiras frente as fraudes eletrônicas, com destaque para as práticas de *Phishing* e *Pharming*, que têm desafiado os mecanismos tradicionais de proteção nas relações de consumo bancárias. À luz da doutrina, da legislação brasileira e da jurisprudência recente, foi possível constatar que, embora tais fraudes sejam perpetradas por terceiros, a posição estratégica dos Bancos no ciclo contratual e informacional impõe-lhes deveres reforçados de diligência, segurança e informação.

Verificou-se que, nas situações em que há falhas nos sistemas de autenticação, ausência de alertas ou demora injustificada na contenção de danos, as instituições financeiras devem ser responsabilizadas com base na responsabilidade objetiva prevista no Código de Defesa do Consumidor, bem como nos princípios da boa-fé e da confiança legítima que regem os contratos. A aplicação da Lei Geral de Proteção de Dados reforça a proteção de dados pessoais, cujo descumprimento pode acarretar a responsabilização civil.

Ainda que o consumidor tenha o dever de cuidado com suas informações, esse ônus não é suficiente para exonerar a instituição financeira de sua responsabilidade, especialmente quando se verifica a assimetria técnica entre as partes e a expectativa legitima de que o Banco ofereça um serviço seguro. Nos casos de *Pharming*, em que não há participação ativa do consumidor, a responsabilização do Banco se apresenta ainda mais evidente, diante da impossibilidade de o cliente perceber a fraude ou de evitá-la por seus próprios meios, sobretudo quando há falhas no dever de informação prestadas pela instituição.

Conclui-se, portanto, que a responsabilização das instituições financeiras por fraudes digitais não pode ser afastada de forma genérica, tampouco presumida automaticamente. Deve ser resultado de análise criteriosa do caso concreto, observando os deveres assumidos, as medidas de segurança implementadas, a conduta do consumidor e o nexo de causalidade e, principalmente o equilíbrio entre a proteção do consumidor e a limitação da responsabilidade bancária é essencial para assegurar a segurança jurídica e o adequado funcionamento do sistema financeiro digital no Brasil.

Referências

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 6 abr. 2025a.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 6 abr. 2025b.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera as Leis nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), e nº 13.853, de 8 de julho de 2019. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 6 abr. 2025c.

BRASIL. Superior Tribunal de Justiça. AgInt no AREsp n. 2.653.859/SC. Relator: Ministro Raul Araújo. Quarta Turma. Julgado em: 21 out. 2024. Publicado em: Diário da Justiça Eletrônico, 4 nov. 2024d.

BRASIL. Superior Tribunal de Justiça. Súmula nº 297, de 13 de outubro de 2004. O Código de Defesa do Consumidor é aplicável às instituições financeiras. Diário da Justiça Eletrônico, Brasília, DF, 14 out. 2004. Disponível em: https://www.stj.jus.br/sites/portalp/Inicio/sumulas/sumulas-do-stj/sumula-297. Acesso em: 6 abr. 2025e.

BRASIL. Superior Tribunal De Justiça. Súmula nº 479, de 24 de junho de 2011. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Diário da Justiça Eletrônico, Brasília, DF, 27 jun. 2011. Disponível em: https://www.stj.jus.br/sites/portalp/Inicio/sumulas/sumulas-do-stj/sumula-479. Acesso em: 6 abr. 2025f.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo Mário Veiga. Novo curso de direito civil: responsabilidade civil. 22. ed. São Paulo: Saraiva Jur., 2024. 1 recurso online. ISBN 978-65-536-2974-5.

REINALDO FILHO, Demócrito. A responsabilidade dos Bancos pelos prejuízos resultantes do *Phishing*. Revista Magister de Direito Empresarial, Concorrencial e do Consumidor, 2006.

SILVA, Maria Teresa Resende Neiva Martins da. A responsabilidade dos Bancos em casos de *Phishing* e *Pharming*. 2021. 88 f. Dissertação (Mestrado em Direito) – Universidade de Coimbra, Coimbra, 2021.

SÃO PAULO. Tribunal de Justiça. Apelação Cível n. 1001692-87.2024.8.26.0030. Relator: Fernão Borba Franco. 24ª Câmara de Direito Privado. Foro de Apiaí – Vara Única. Julgado em: 8 jul. 2025. Registrado em: 8 jul. 2025a.

SÃO PAULO. Tribunal de Justiça. Apelação Cível n. 1006343-34.2024.8.26.0008. Relator: Carlos Eduardo Borges Fantacini. 16ª Câmara de Direito Privado. Foro Regional VIII – Tatuapé – 3ª Vara Cível. Julgado em: 8 abr. 2025. Registrado em: 9 abr. 2025b.

SÃO PAULO. Tribunal de Justiça. Apelação Cível n. 1105851-36.2022.8.26.0100. Relator: Salles Vieira. 24ª Câmara de Direito Privado. Foro Regional XI – Pinheiros – 4ª Vara Cível. Julgado em: 28 set. 2023. Registrado em: 3 out. 2023c.

TARTUCE, Flávio. et al. Código Civil comentado CD - doutrina e jurisprudência. 3ª edição. ed. Rio de Janeiro: Editora Forense, 2021. 1 recurso online: ISBN 978-65-5964-071-3.