Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i6.27648

A RESPONSABILIDADE DOS BANCOS E A PROTEÇÃO DO CONSUMIDOR DIANTE DE FRAUDES DIGITAIS E ACESSOS NÃO AUTORIZADOS A DADOS SENSÍVEIS

Camila Mota Lima[1]
Rosana Reis de Melo Silva[2]

RESUMO: A presente pesquisa tem como objeto a análise da responsabilidade civil dos bancos no Brasil, no período de 2020 a 2025, frente ao expressivo aumento de fraudes digitais e acessos não autorizados a dados sensíveis de consumidores. O estudo concentra-se na aplicação do Código de Defesa do Consumidor, (Lei n 8.078/1990) em casos de fraudes bancárias ocorridas por meio eletrônico, especialmente através do internet Banking e de aplicativos móveis, e em como as instituições financeiras vêm sendo responsabilizadas, ou não, pelo Judiciário brasileiro. O recorte espacial abrange a jurisprudência de Tribunais Brasileiros, com ênfase nas decisões dos Tribunais de Justiça estaduais e do Superior Tribunal de Justiça (STJ), cuja atuação é fundamental na uniformização da interpretação do direito consumerista. A escolha do tema justifica-se por sua elevada relevância social e jurídica diante da crescente digitalização dos serviços bancários e do aumento das fraudes eletrônicas, em razão da crescente digitalização dos serviços bancários e do expressivo aumento dos crimes cibernéticos que afetam diretamente os direitos dos consumidores. Portanto, esta pesquisa é de grande importância não apenas para o campo jurídico, mas também para a sociedade em geral, ao buscar soluções que garantam maior segurança nas relações bancárias digitais e para a efetiva proteção dos consumidores diante das novas formas de criminalidade tecnológica.

Palavras-chave: Proteção. Consumidor. Fraudes Digitais. Responsabilidade Juridica.

ABSTRACT: The purpose of this research is to analyze the civil liability of banks in Brazil, in the period from 2020 to 2025, in view of the significant increase in digital fraud and unauthorized access to sensitive consumer data. The study focuses on the application of the Consumer Protection Code, (governed by Law No. 8.078/1990) in cases of bank fraud that occurred by electronic means, especially through internet banking and mobile applications, and on how financial institutions have been held responsible, or not, by the Brazilian Judiciary. The spatial cut covers the jurisprudence of Brazilian Courts, with emphasis on the decisions of the state Courts of Justice and the Superior Court of Justice (STJ), whose performance is fundamental in the standardization of the interpretation of consumer law. The choice of the theme "The responsibility of banks and the protection of consumers in the face of digital fraud and unauthorized access to sensitive data" is justified by its social relevance and topicality, due to the growing digitalization of banking services and the significant increase in cybercrimes that directly affect consumer rights. Therefore, this research is of great importance not only for the legal field, but also for society in general, as it seeks solutions that ensure greater security in digital banking relationships and for the effective protection of consumers in the face of new forms of technological crime.

Keywords: Protection. Consumer. Digital Fraud. Legal Liability.

[1]Graduanda do curso de Bacharelado em Direito, no Centro Universitário FAMETRO, Brasil.
[2]Prof.ª Orientadora e Coordenadora do TCC II, no Centro Universitário FAMETRO: Prof.ª Esp. Rosana Reis de Melo Silva. Manaus, Amazonas, Brasil.

1 INTRODUÇÃO

A digitalização das relações sociais e comerciais, que foi acelerada pela internet e pelas novas tecnologias, fez com que o consumidor se tornasse mais vulnerável. Desde 1990, o Código de Defesa do Consumidor (CDC) já reconhecia essa vulnerabilidade como um aspecto fundamental nas relações de consumo (BRASIL, 1990). No ambiente digital, essa fragilidade fica ainda mais evidente, principalmente por causa da desigualdade de informações entre consumidores e fornecedores, da complexidade dos serviços digitais e do uso de técnicas avançadas de marketing.

A vulnerabilidade do consumidor é composta por várias razões, incluindo aspectos técnicos, informações disponíveis, fatores psicológicos e questões jurídicas. No ambiente digital, esses problemas ficam ainda maiores devido às dificuldades que as pessoas têm para entender contratos eletrônicos, à falta de transparência na coleta e uso dos dados pessoais e à personalização exagerada de ofertas por meio de algoritmos. Isso pode levar os consumidores a tomarem decisões de compra sem perceber exatamente como estão sendo influenciados (Doneda, 2006).

O avanço da tecnologia, especialmente da Inteligência Artificial (IA), tem provocado transformações profundas na forma como as pessoas interagem com produtos, serviços e plataformas digitais. Ferramentas como chatbots, algoritmos de recomendação e sistemas de análise de sentimentos tornaram-se parte integrante do cotidiano, modificando significativamente o comportamento do consumidor e a dinâmica das relações de consumo. Se por um lado essas inovações promovem comodidade, personalização e agilidade, por outro, levantam questionamentos importantes sobre privacidade, transparência, responsabilidade e equilíbrio contratual (Velloso, 2025).

O Código de Defesa do Consumidor precisa ser interpretado levando em conta essa nova realidade, o que exige uma atualização na forma como aplicamos princípios como boa-fé, equilíbrio nos contratos e transparência. Proteger o consumidor não deve se limitar a punir abusos, mas também envolver ações preventivas, como promover a educação digital e estabelecer regras mais claras para as práticas das empresas de tecnologia (TARTUCE, 2019).

No Brasil, a criação da Lei Geral de Proteção de Dados Pessoais (LGPD), em 2018, foi um passo importante. A norma garante direitos aos titulares de dados e impõe obrigações aos agentes que tratam essas informações (BRASIL, 2018). A integração entre LGPD e CDC fortalece a proteção do consumidor no meio digital, especialmente em plataformas online.

Assim, fica evidente que a vulnerabilidade do consumidor no ambiente digital exige uma atuação jurídica mais técnica e atualizada. O desafio está em equilibrar inovação tecnológica e liberdade econômica com os direitos fundamentais do consumidor, como informação, privacidade e dignidade.

2 MUDANÇA DE PARADIGMA DO SISTEMA PROCESSUAL

A evolução do sistema processual brasileiro revela que os modelos clássicos inquisitório e dispositivo já não dão conta dos desafios contemporâneos, especialmente nas demandas que envolvem fraudes bancárias e acessos não autorizados a dados sensíveis. O novo paradigma cooperativo, positivado no art. 6º do CPC/2015, exige a atuação conjunta entre partes, advogados e juiz, com respaldo nos princípios constitucionais da dignidade, isonomia, ampla defesa e devido processo legal (Moraes, 2016; Marinoni, Arenhart & Mitidiero, 2016).

No estudo "A responsabilidade civil nas fraudes bancárias eletrônicas", Ghani (2023) aponta que, nesses litígios, há um claro desequilíbrio informacional: os bancos detêm logs, registros de segurança e informações técnicas necessárias à comprovação do ilícito.

É nesse cenário que se impõe a necessidade de um modelo processual mais ativo e colaborativo, capaz de abrir caminho para o consumidor vulnerável acessar prova técnica essencial e participar efetivamente do contraditório (Nader, 2018; Theodoro Júnior, 2019).

2.1 Modelos de sistema processual

Fala-se que, no modelo adversarial, prepondera o princípio dispositivo, e, no modelo inquisitorial, o princípio inquisitivo. Princípio, aqui, é termo utilizado não no sentido de "espécie normativa", mas, sim, de "fundamento", "orientação preponderante" etc. Assim, quando o legislador atribui às partes as principais tarefas relacionadas à condução e instrução do processo, diz-se que se está respeitando o denominado princípio dispositivo; tanto mais poderes forem atribuídos ao magistrado, mais condizente com o princípio inquisitivo o processo será. A dicotomia princípio inquisitivo-princípio dispositivo está intimamente relacionada à atribuição de poderes ao juiz: sempre que o legislador atribuir um poder ao magistrado, independentemente da vontade das partes, vê-se manifestação de "inquisitividade"; sempre que se deixe ao alvedrio dos litigantes a opção, aparece a "dispositividade". (Didier, 2013).

Em “Fraudes em contratos eletrônicos de empréstimos bancários: vulnerabilidade do consumidor, inteligência artificial e prova pericial em sistemas de biometria”, Soares e Pereira de Carvalho (2023) descrevem casos em que a perícia técnica sobre sistemas biométricos ou algoritmos bancários é determinante para a solução da controvérsia, evidenciando que o Judiciário não pode esperar que o consumidor sozinho conduza essa produção (Soares & Pereira de Carvalho, 2023).

A análise apresentada pelo autor demonstra que a falta de educação sobre segurança digital é um fator que contribui para essa vulnerabilidade. Muitos usuários não têm consciência dos riscos associados ao compartilhamento de informações pessoais ou à utilização de redes Wi-Fi públicas para realizar transações financeiras. Essa falta de conhecimento pode ser explorada pelos golpistas, que se aproveitam da inexperiência dos clientes para aplicar seus golpes. Assim, a conscientização sobre segurança digital se torna uma necessidade urgente, não apenas para proteger os clientes, mas também para restaurar a confiança nas instituições financeiras (Rocha, 2025, p. 31).

2.2 Cooperação e sistema processual constitucional

O art. 6.° do CPC/2015 prevê que "Todos os sujeitos do processo devem cooperar entre si para que se obtenha, em tempo razoável, decisão de mérito justa e efetiva", inserindo, assim, o princípio da cooperação como uma das normas fundamentais do processo civil.

Este dispositivo exerce duas funções importantes no ordenamento jurídico-processual brasileiro: (i) estruturar o processo civil sob o modelo cooperativo; e (ii) firmar o funcionamento do sistema processual a partir do princípio da cooperação? Dentre os fins almejados pelo princípio da cooperação se encontram o combate ao desperdício, a primazia das decisões de mérito em desfavor das processuais, a busca da verdade e o emprego de técnicas executivas adequadas à efetivação dos direitos (Mitidieri, 2015, p. 48-49).

Em trabalhos sobre responsabilidade civil em fraudes digitais, autores apontam que a aplicação real desse princípio depende da abertura institucional para que dados técnicos imprescindíveis sejam compartilhados judicialmente (Ghani, 2023).

Além disso, os recentes números de fraudes digitais reforçam com urgência essa necessidade: segundo o Relatório de Identidade e Fraude 2025 da Serasa Experian, 51 % dos brasileiros declararam já ter sido vítimas de fraude, e muitas dessas fraudes envolvem perda financeira (Rocha, 2025). Também, só no primeiro trimestre de 2025 o setor de bancos e cartões

registrou 1.871.979 tentativas de fraude, evidenciando o ambiente de risco constante em que se opera (Rocha, 2025). Esse cenário exige que o modelo cooperativo transcenda o mero discurso e se materialize em decisões concretas.

2.3 Conteúdo da cooperação processual

Didier Jr. (2018) destaca: Os deveres de cooperação podem ser divididos em deveres de esclarecimento, lealdade e de proteção. Vejamos algumas manifestações desses deveres em relação às partes: (a) dever de esclarecimento: os demandantes devem redigir a sua demanda com clareza e coerência, sob pena de inépcia (art. 295, I, parágrafo único, do CPC); (b) dever de lealdade: as partes não podem litigar de má-fé (art. 17 do CPC), além de ter de observar o princípio da boa-fé processual (art. 14, II, do CPC); (c) dever de proteção: a parte não pode causar danos à parte adversária (punição ao atentado, arts. 879 a 881 do CPC; há a responsabilidade objetiva do exequente nos casos de execução injusta, arts. 475-O, I, e 574, do CPC).

O artigo 6.º do Código de Processo Civil "todos os sujeitos do processo devem cooperar entre si para que se obtenha, em tempo razoável, decisão de mérito justa e efetiva" exige-se uma postura colaborativa de todos os sujeitos processuais, inclusive do juiz, ao qual compete adotar as medidas necessárias na busca da tutela jurisdicional específica, adequada, célere, justa e efetiva. (Tribunal de Justiça do Distrito Federal e dos Territórios, tema "Princípio da cooperação").

Segundo Marinoni (apud Rezende, 2015): "Encara o processo civil como uma comunidade de trabalho regida pela ideia de colaboração, portanto, é reconhecer que o juiz tem o dever de cooperar com as partes, a fim de que o processo civil seja capaz de chegar efetivamente a uma decisão justa, fruto de efético 'dever de engajamento' do juiz no processo. Longe de aniquilar a autonomia individual e auto-responsabilidade das partes, a colaboração apenas viabiliza que o juiz atue para a obtenção de uma decisão justa com a incrementação de seus poderes de condução no processo, responsabilizando-o igualmente pelos seus resultados. A colaboração não apaga obviamente o princípio da demanda e as suas consequências básicas: o juízo de conveniência a respeito da propositura ou não da ação e a delimitação do mérito da causa continuar tarefas ligadas exclusivamente à conveniência das partes. O processo não é encarado nem como coisa exclusivamente das partes, nem como coisa exclusivamente do juiz é uma coisa comum ao juiz e às partes".

3 RESPONSABILIDADE DOS BANCOS E PROTEÇÃO DO CONSUMIDOR: FRAUDES E ACESSOS NÃO AUTORIZADOS A DADOS SENSÍVEIS

Com a expansão dos serviços bancários digitais, os consumidores passaram a enfrentar novos riscos relacionados a fraudes financeiras e ao vazamento de dados sensíveis. O Código de Defesa do Consumidor (CDC), em seu artigo 14, estabelece que o fornecedor de serviços responde objetivamente por danos causados ao consumidor, independentemente da existência de culpa, quando houver falha na prestação do serviço, o que inclui a segurança das operações (Brasil, 1990).

A Lei Geral de Proteção de Dados (LGPD) é um exemplo claro dessa regulamentação, estabelecendo diretrizes sobre como as informações pessoais devem ser coletadas, armazenadas e utilizadas. Essa legislação não apenas impõe obrigações, mas também oferece aos clientes direitos que garantem maior controle sobre suas informações. É essencial que os bancos compreendam e implementem essas diretrizes, não apenas para evitar penalidades, mas para construir uma relação de confiança com seus clientes (Rocha, 2025).

Nesse sentido, bancos devem garantir a proteção adequada de seus sistemas contra fraudes, considerando que essas práticas são riscos inerentes à atividade bancária. Como mostra o artigo "As fraudes bancárias e a Responsabilidade Civil das Instituições Financeiras" (Pereira & Silva), a jurisprudência brasileira tem admitido a responsabilização objetiva dos bancos em casos de falha nos mecanismos de segurança digital.

No contexto da responsabilidade civil de instituições financeiras, o Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT, 2023) firmou entendimento de que "as instituições financeiras respondem objetivamente por falha na prestação de serviços que não oferece a segurança legitimamente esperada ao consumidor, por não prevenir total ou parcialmente que golpistas possam ilegitimamente contratar serviços bancários em nome do consumidor". Essa decisão reforça a obrigação das instituições de adotar medidas eficazes de prevenção a fraudes, evidenciando a responsabilização objetiva prevista no Código de Defesa do Consumidor.

No contexto da educação financeira, é fundamental que os bancos não se limitem apenas a alertar sobre riscos, mas que promovam ações educativas que capacitem seus clientes a identificarem possíveis problemas. Nesse sentido, autores apontam que "os bancos devem investir em campanhas educativas que não apenas informem sobre os riscos, mas também

ensinem os clientes a reconhecerem sinais de alerta" (Rocha, 2025, p. 23), evidenciando a importância de uma abordagem preventiva e proativa na gestão financeira pessoal.

Os bancos têm a responsabilidade de garantir que suas tecnologias não apenas protejam, mas também respeitem a privacidade dos clientes. Dados estatísticos mostram que cerca de 70% das fraudes digitais são resultado da falta de conscientização dos usuários sobre as táticas utilizadas pelo golpista (Rocha, 2025, p. 39).

Com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, intensificou-se a obrigação das instituições financeiras quanto ao tratamento e à proteção de dados pessoais. A LGPD determina que os agentes de tratamento de dados devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Brasil, 2018).

A responsabilidade civil bancária também deve considerar a hipervulnerabilidade do consumidor digital. Consumidores idosos, pessoas com baixa escolaridade ou pouca familiaridade com tecnologia estão mais expostos a fraudes, o que demanda maior cuidado por parte das instituições financeiras. Nesse sentido, a digitalização dos serviços bancários representa uma mudança de paradigma que transformou radicalmente a forma como os bancos operam e como os clientes interagem com suas finanças (Rocha, 2025).

Embora existam hipóteses de excludente de responsabilidade como a culpa exclusiva da vítima, a jurisprudência é cautelosa em aceitá-las. Em geral, entende-se que o risco de fraudes é previsível e que os bancos, como detentores de tecnologia e recursos, têm o dever de mitigar esses riscos. No estudo de Pereira & Silva (2025), afirma-se que as instituições não podem se eximir da responsabilidade alegando simplesmente que a fraude foi praticada por terceiro, especialmente se não demonstraram medidas adequadas de segurança. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias." (SUPERIOR TRIBUNAL DE JUSTIÇA, 2012, Súmula 479).

3.1 Responsabilidade civil das instituições bancárias nas relações de consumo

A responsabilidade civil das instituições bancárias nas relações de consumo encontra fundamento no Código de Defesa do Consumidor, especialmente em razão da vulnerabilidade do consumidor diante das atividades financeiras e tecnológicas desempenhadas pelos bancos.

Nesse contexto, as instituições financeiras são consideradas fornecedoras de serviços, submetendo-se às normas consumeristas previstas na Código de Defesa do Consumidor. Conforme dispõe o art. 14 do CDC, o fornecedor responde objetivamente pelos danos causados ao consumidor em decorrência de defeitos relativos à prestação dos serviços, independentemente da comprovação de culpa. Dessa forma, basta a existência do dano e do nexo causal para surgir o dever de indenizar. Segundo Flávio Tartuce (2023), "a responsabilidade objetiva representa mecanismo de proteção da parte vulnerável da relação de consumo, dispensando a comprovação da culpa do fornecedor". Tal entendimento reforça a necessidade de proteção efetiva ao consumidor diante das falhas bancárias.

As instituições bancárias possuem o dever jurídico de garantir segurança, sigilo e proteção aos dados pessoais e financeiros de seus clientes, sobretudo diante do aumento das operações digitais. A utilização de aplicativos, internet banking e demais plataformas eletrônicas ampliou significativamente os riscos de fraudes, vazamentos e acessos indevidos a dados sensíveis. Nesse sentido, a Lei Geral de Proteção de Dados Pessoais estabelece que os agentes de tratamento devem adotar medidas aptas a proteger os dados pessoais contra acessos não autorizados e situações ilícitas de destruição, perda ou divulgação. Para Patrícia Peck (2022), a proteção de dados pessoais "passou a integrar o núcleo essencial dos direitos fundamentais relacionados à privacidade e à dignidade da pessoa humana". Assim, os bancos devem investir constantemente em mecanismos de segurança digital, sob pena de responsabilização pelos prejuízos ocasionados aos consumidores.

Além disso, o entendimento jurisprudencial consolidado no ordenamento jurídico brasileiro reconhece a responsabilidade objetiva das instituições financeiras em casos de fraudes praticadas por terceiros no âmbito das operações bancárias. O Superior Tribunal de Justiça consolidou esse entendimento por meio da Súmula 479, segundo a qual: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias". A partir desse posicionamento, compreende-se que golpes, clonagens, transferências indevidas e invasões de contas configuram riscos inerentes à atividade bancária, não podendo o consumidor suportar sozinho os prejuízos decorrentes dessas falhas. Desse modo, o risco da atividade econômica deve ser assumido pela instituição financeira, conforme preceitua a teoria do risco do empreendimento.

A responsabilidade civil dos bancos também decorre do dever de boa-fé objetiva e da confiança legítima existente nas relações contratuais bancárias. O consumidor deposita confiança na segurança prometida pelas instituições financeiras ao disponibilizarem serviços digitais e sistemas eletrônicos de movimentação financeira. Assim, quando ocorre falha na prestação do serviço, especialmente em razão de acessos indevidos ou fraudes eletrônicas, verifica-se violação aos deveres anexos de proteção, informação e segurança. Conforme leciona Cláudia Lima Marques (2021), "a boa-fé objetiva impõe aos fornecedores deveres de cooperação, transparência e lealdade durante toda a relação de consumo". Portanto, cabe às instituições financeiras atuar preventivamente, garantindo meios eficazes de autenticação e monitoramento de operações suspeitas.

Por fim, destaca-se que a proteção do consumidor no setor bancário possui relevante função social, especialmente diante da crescente digitalização dos serviços financeiros e do aumento dos crimes cibernéticos. A responsabilização objetiva das instituições financeiras contribui para o fortalecimento da segurança jurídica e para a efetivação dos direitos fundamentais do consumidor, sobretudo os direitos à privacidade, à informação e à reparação integral dos danos sofridos. Nesse sentido, a doutrina e a jurisprudência vêm consolidando o entendimento de que os bancos devem responder pelos danos causados por falhas de segurança em seus sistemas, inclusive quando houver vazamento ou acesso não autorizado a dados sensíveis dos consumidores. Dessa forma, a aplicação conjunta do CDC e da LGPD revela-se essencial para assegurar maior proteção aos usuários dos serviços bancários digitais.

3.2 A proteção dos dados sensíveis do consumidor no ambiente bancário

A proteção dos dados sensíveis do consumidor tornou-se uma das principais preocupações do ordenamento jurídico brasileiro diante da crescente digitalização dos serviços bancários. Informações como biometria, senhas, dados financeiros, histórico de transações e documentos pessoais passaram a integrar extensos bancos de dados administrados pelas instituições financeiras, exigindo elevado nível de segurança e controle. Nesse cenário, a Lei Geral de Proteção de Dados Pessoais estabelece diretrizes para o tratamento adequado das informações pessoais, impondo aos agentes de tratamento o dever de proteger os dados contra acessos não autorizados e situações ilícitas. De acordo com o art. 46 da LGPD, os controladores devem adotar "medidas de segurança, técnicas e administrativas aptas a proteger os dados

pessoais". Assim, os bancos possuem obrigação legal de implementar mecanismos eficazes de prevenção contra fraudes, vazamentos e invasões cibernéticas.

No âmbito das relações de consumo, a proteção dos dados pessoais relaciona-se diretamente aos direitos fundamentais da privacidade, intimidade e dignidade da pessoa humana. O consumidor, ao contratar serviços bancários, deposita confiança na instituição financeira quanto à guarda e sigilo de suas informações, motivo pelo qual qualquer falha de segurança pode gerar relevantes danos patrimoniais e morais. Conforme ensina Bruno Miragem (2022), a proteção de dados pessoais "constitui extensão dos direitos da personalidade no ambiente digital". Dessa forma, verifica-se que o tratamento inadequado de informações sensíveis ultrapassa a esfera meramente contratual, atingindo direitos fundamentais assegurados pela Constituição Federal e pela legislação consumerista. Nesse sentido, o Código de Defesa do Consumidor também garante ao consumidor o direito à segurança e à reparação integral pelos danos decorrentes da falha na prestação dos serviços.

Além disso, as instituições bancárias respondem objetivamente pelos danos ocasionados em razão da exposição indevida de dados sensíveis de seus clientes, especialmente quando demonstrada falha nos sistemas de segurança. O entendimento jurisprudencial brasileiro tem reconhecido que fraudes eletrônicas, golpes bancários e acessos não autorizados configuram fortuito interno, inerente à atividade desempenhada pelos bancos. O Superior Tribunal de Justiça consolidou esse entendimento ao editar a Súmula 479, estabelecendo que as instituições financeiras respondem objetivamente pelos danos decorrentes de fraudes praticadas no âmbito das operações bancárias. Segundo Rizzatto Nunes (2021), "*o fornecedor assume os riscos do empreendimento, devendo responder pelos prejuízos causados ao consumidor em decorrência da atividade exercida*". Portanto, a responsabilidade bancária decorre não apenas da falha operacional, mas também do dever permanente de vigilância e proteção das informações confiadas pelos consumidores.

Por fim, observa-se que a proteção dos dados sensíveis no ambiente bancário exige atuação preventiva, transparente e eficiente das instituições financeiras, sobretudo diante do avanço dos crimes cibernéticos e da sofisticação das fraudes digitais. A adoção de autenticação multifatorial, criptografia, monitoramento de transações suspeitas e educação digital dos consumidores representa importante instrumento de redução de riscos. Ademais, a observância dos princípios previstos na LGPD, como finalidade, necessidade, segurança e transparência, fortalece a confiança nas relações bancárias e contribui para a efetivação dos direitos do

consumidor. Conforme destaca Danilo Doneda (2021), "a proteção de dados pessoais constitui elemento indispensável para a preservação da liberdade e da autonomia dos indivíduos na sociedade da informação". Dessa maneira, a responsabilização das instituições financeiras revela-se fundamental para assegurar maior proteção jurídica aos consumidores diante das constantes ameaças digitais.

3.3 Fraudes bancárias digitais e o vazamento de informações pessoais

O avanço tecnológico e a ampliação dos serviços financeiros digitais proporcionaram maior praticidade aos consumidores, mas também contribuíram significativamente para o crescimento das fraudes bancárias eletrônicas e dos vazamentos de informações pessoais. A utilização de aplicativos bancários, internet banking, transferências instantâneas e pagamentos eletrônicos intensificou a circulação de dados sensíveis dos consumidores em ambientes virtuais, tornando-os alvos frequentes de ataques cibernéticos. Nesse contexto, as instituições financeiras assumem papel fundamental na proteção das informações de seus clientes, devendo garantir mecanismos eficazes de segurança digital. Conforme dispõe a Lei Geral de Proteção de Dados Pessoais, o tratamento de dados pessoais deve observar medidas técnicas e administrativas aptas a proteger as informações contra acessos não autorizados, vazamentos e situações ilícitas. Assim, a ausência de segurança adequada pode caracterizar falha na prestação do serviço bancário.

As fraudes bancárias digitais manifestam-se de diversas formas, como phishing, clonagem de cartões, engenharia social, invasão de contas bancárias, falsificação de boletos e transferências indevidas realizadas por terceiros. Em muitos casos, os criminosos utilizam dados pessoais previamente vazados para aplicar golpes cada vez mais sofisticados, aumentando os prejuízos suportados pelos consumidores. Segundo Patrícia Peck (2022), "o vazamento de dados pessoais potencializa a prática de crimes digitais e amplia os riscos de fraudes financeiras". Dessa maneira, percebe-se que a exposição indevida de informações sensíveis não gera apenas violação da privacidade, mas também consequências patrimoniais e emocionais ao consumidor, que frequentemente enfrenta dificuldades para reverter operações fraudulentas.

No âmbito das relações de consumo, a responsabilidade das instituições financeiras decorre da teoria do risco do empreendimento, segundo a qual aquele que exerce atividade lucrativa deve assumir os riscos inerentes ao serviço prestado. O Código de Defesa do

Consumidor prevê, em seu art. 14, a responsabilidade objetiva do fornecedor pelos danos causados em decorrência de defeitos relativos à prestação dos serviços. Assim, não há necessidade de comprovação de culpa da instituição financeira, bastando a demonstração do dano e do nexo causal. Conforme leciona Flávio Tartuce (2023), "a responsabilidade objetiva busca equilibrar a relação entre consumidor e fornecedor, atribuindo ao fornecedor os riscos da atividade econômica". Portanto, os bancos possuem dever de reparar os prejuízos decorrentes de falhas de segurança que possibilitem fraudes e acessos indevidos aos dados de seus clientes.

A jurisprudência brasileira também consolidou entendimento favorável à responsabilização das instituições financeiras em casos de fraudes eletrônicas praticadas por terceiros. O Superior Tribunal de Justiça, por meio da Súmula 479, estabeleceu que "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias". Dessa forma, os golpes virtuais são considerados riscos inerentes à atividade bancária, não podendo ser transferidos integralmente ao consumidor. Além disso, os tribunais brasileiros vêm reconhecendo o dever de indenização por danos morais e materiais quando demonstrada falha na segurança dos sistemas bancários ou ausência de mecanismos adequados de prevenção a fraudes.

Outro aspecto relevante refere-se à violação dos direitos fundamentais do consumidor em decorrência do vazamento de informações pessoais. Os dados bancários e financeiros integram a esfera da privacidade do indivíduo, sendo protegidos constitucionalmente pelos direitos à intimidade, honra e vida privada. Segundo Danilo Doneda (2021), "a proteção de dados pessoais representa instrumento essencial para a tutela da liberdade e da dignidade humana na sociedade digital". Nesse cenário, a observância dos princípios da segurança, transparência e prevenção previstos na LGPD mostra-se indispensável para garantir maior proteção aos usuários dos serviços bancários.

Por fim, destaca-se que o combate às fraudes bancárias digitais exige atuação conjunta das instituições financeiras, do Poder Público e dos próprios consumidores. Os bancos devem investir continuamente em tecnologias de autenticação, inteligência artificial, monitoramento de operações suspeitas e sistemas de criptografia, além de promover campanhas educativas voltadas à conscientização dos clientes sobre práticas de segurança digital. Da mesma forma, a atuação fiscalizatória da Autoridade Nacional de Proteção de Dados contribui para o fortalecimento da proteção dos dados pessoais no país. Nesse contexto, a responsabilização civil

das instituições financeiras revela-se mecanismo essencial para incentivar a adoção de medidas preventivas e assegurar maior efetividade aos direitos do consumidor diante do crescente cenário de criminalidade cibernética.

4 A EFETIVIDADE DA TUTELA JURÍDICA DO CONSUMIDOR DIANTE DAS FRAUDES BANCÁRIAS DIGITAIS

A crescente digitalização dos serviços bancários trouxe inúmeros benefícios aos consumidores, como praticidade, rapidez e facilidade no acesso às operações financeiras. Contudo, esse avanço tecnológico também ampliou significativamente os riscos relacionados às fraudes eletrônicas, vazamentos de dados e acessos não autorizados às informações sensíveis dos usuários. Nesse contexto, torna-se indispensável discutir a efetividade da tutela jurídica do consumidor diante das novas modalidades de criminalidade digital, especialmente no âmbito das relações bancárias.

O Código de Defesa do Consumidor estabelece mecanismos de proteção voltados à parte vulnerável da relação de consumo, impondo responsabilidade objetiva aos fornecedores de serviços pelos danos causados aos consumidores. Conforme dispõe o art. 14 do CDC, o fornecedor responde independentemente da comprovação de culpa pelos defeitos relativos à prestação dos serviços. Dessa forma, as instituições financeiras possuem o dever jurídico de garantir segurança adequada aos sistemas digitais utilizados pelos clientes.

Além disso, a Lei Geral de Proteção de Dados Pessoais (LGPD) fortaleceu a proteção jurídica dos consumidores ao estabelecer regras específicas para o tratamento de dados pessoais e sensíveis. A legislação determina que os agentes de tratamento adotem medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados, vazamentos e demais situações ilícitas. Assim, a responsabilidade bancária passou a abranger não apenas a prestação do serviço financeiro, mas também a adequada proteção das informações pessoais dos consumidores.

A jurisprudência brasileira também consolidou importante entendimento acerca da responsabilidade das instituições financeiras. O Superior Tribunal de Justiça, por meio da Súmula 479, estabeleceu que “as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias”. Tal posicionamento demonstra que os riscos inerentes à atividade bancária devem ser suportados pelas próprias instituições financeiras, e não exclusivamente

pelos consumidores.

Segundo Flávio Tartuce, a responsabilidade objetiva "representa mecanismo de proteção da parte vulnerável da relação de consumo". Nesse sentido, percebe-se que a tutela jurídica do consumidor busca equilibrar a desigualdade existente entre os usuários dos serviços bancários e as instituições financeiras, especialmente diante da complexidade tecnológica envolvida nas operações digitais.

Outro aspecto relevante refere-se ao crescimento expressivo das fraudes bancárias eletrônicas nos últimos anos. Os golpes digitais tornaram-se cada vez mais sofisticados, utilizando engenharia social, clonagem de dispositivos, phishing e vazamento de dados pessoais para obtenção ilícita de informações financeiras. Diante dessa realidade, a proteção jurídica do consumidor exige constante atualização legislativa, doutrinária e jurisprudencial, de modo a acompanhar a evolução das práticas criminosas no ambiente virtual.

Portanto, a efetividade da tutela jurídica do consumidor diante das fraudes bancárias digitais depende da atuação conjunta da legislação consumerista, da LGPD, do Poder Judiciário e das próprias instituições financeiras. A responsabilização civil dos bancos revela-se importante instrumento de prevenção e reparação dos danos sofridos pelos consumidores, além de incentivar investimentos em segurança digital e proteção de dados pessoais.

4.1 O papel da lei geral de proteção de dados na segurança das operações bancárias

A Lei Geral de Proteção de Dados Pessoais representou importante avanço na proteção jurídica das informações dos consumidores no ambiente digital. A partir de sua entrada em vigor, as instituições financeiras passaram a possuir obrigações mais rigorosas relacionadas ao tratamento, armazenamento e compartilhamento de dados pessoais e sensíveis dos clientes. Em razão disso, a LGPD tornou-se instrumento fundamental para garantir maior segurança nas operações bancárias eletrônicas.

O artigo 46 da LGPD estabelece que os agentes de tratamento devem adotar "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados". Assim, os bancos possuem obrigação legal de implementar sistemas de proteção capazes de prevenir fraudes, vazamentos de informações e invasões cibernéticas, especialmente diante do elevado fluxo de dados financeiros existentes nas plataformas digitais.

Segundo Patrícia Peck, a proteção de dados pessoais passou a integrar os direitos fundamentais relacionados à privacidade e à dignidade da pessoa humana. Dessa maneira, a

segurança das operações bancárias não se limita apenas à proteção patrimonial do consumidor, mas também envolve a preservação de sua intimidade, identidade digital e liberdade individual.

Além disso, a LGPD reforçou os deveres de transparência e informação das instituições financeiras perante os consumidores. Os bancos devem informar de maneira clara como os dados pessoais serão coletados, utilizados e compartilhados, permitindo que o titular exerça controle sobre suas próprias informações. Essa exigência fortalece o princípio da boa-fé objetiva nas relações de consumo e amplia a confiança dos usuários nos serviços bancários digitais.

A atuação da Autoridade Nacional de Proteção de Dados também desempenha papel relevante na fiscalização das práticas adotadas pelas instituições financeiras. A ANPD possui competência para aplicar sanções administrativas em casos de descumprimento da legislação, incluindo advertências, multas e publicização das infrações cometidas pelas empresas responsáveis pelo tratamento inadequado dos dados pessoais.

Outro ponto importante refere-se à necessidade de constante atualização tecnológica dos mecanismos de segurança utilizados pelos bancos. A rápida evolução dos crimes cibernéticos exige investimentos contínuos em autenticação multifatorial, inteligência artificial, criptografia e monitoramento de transações suspeitas. Conforme entendimento consolidado pelo Superior Tribunal de Justiça, os riscos decorrentes das fraudes eletrônicas integram a própria atividade econômica das instituições financeiras.

Dessa forma, verifica-se que a LGPD exerce papel essencial na segurança das operações bancárias digitais, funcionando como instrumento de proteção dos direitos fundamentais do consumidor e de responsabilização das instituições financeiras em casos de falhas relacionadas ao tratamento de dados pessoais.

4.2 A hipervulnerabilidade do consumidor nos serviços financeiros digitais

A vulnerabilidade do consumidor constitui princípio reconhecido expressamente pelo Código de Defesa do Consumidor. Entretanto, no ambiente digital, essa vulnerabilidade torna-se ainda mais intensa, dando origem ao fenômeno denominado hipervulnerabilidade. Nos serviços financeiros digitais, muitos consumidores enfrentam dificuldades relacionadas à compreensão dos sistemas tecnológicos, dos mecanismos de autenticação e dos riscos presentes nas operações bancárias eletrônicas.

A hipervulnerabilidade mostra-se ainda mais evidente em relação aos consumidores idosos, pessoas com baixa escolaridade ou usuários com pouca familiaridade tecnológica. Esses

grupos frequentemente tornam-se alvos preferenciais de criminosos especializados em golpes virtuais, engenharia social e fraudes bancárias. Em muitos casos, os consumidores realizam operações induzidos por terceiros sem compreender plenamente os riscos envolvidos.

Segundo Cláudia Lima Marques, a boa-fé objetiva impõe aos fornecedores deveres de proteção, cooperação e transparência durante toda a relação de consumo. Dessa forma, os bancos não podem limitar sua atuação apenas à disponibilização dos serviços digitais, devendo também promover mecanismos preventivos voltados à proteção dos consumidores mais vulneráveis.

Além disso, a desigualdade técnica existente entre consumidores e instituições financeiras amplia significativamente a dificuldade de produção de provas em processos judiciais envolvendo fraudes bancárias. Os bancos detêm registros internos, logs de acesso, sistemas de monitoramento e informações técnicas essenciais à apuração dos fatos, enquanto o consumidor geralmente possui acesso limitado às informações necessárias para comprovar a falha na prestação do serviço.

A jurisprudência do Superior Tribunal de Justiça reconhece que as instituições financeiras respondem objetivamente pelos danos decorrentes de fraudes praticadas por terceiros no âmbito das operações bancárias. Assim, o entendimento predominante busca evitar que a hipervulnerabilidade do consumidor resulte em transferência indevida dos riscos da atividade econômica para a vítima da fraude.

Outro aspecto relevante refere-se à necessidade de educação digital dos consumidores. Muitos golpes eletrônicos exploram justamente a falta de conhecimento dos usuários acerca das práticas de segurança digital, como reconhecimento de links falsos, clonagem de aplicativos e compartilhamento indevido de senhas. Nesse cenário, as instituições financeiras devem investir em campanhas educativas permanentes voltadas à conscientização dos clientes.

Portanto, a hipervulnerabilidade do consumidor nos serviços financeiros digitais exige atuação preventiva das instituições financeiras, aplicação efetiva das normas consumeristas e fortalecimento das políticas públicas de proteção de dados e educação digital, garantindo maior equilíbrio nas relações bancárias contemporâneas.

4.3 Medidas preventivas e mecanismos de segurança adotados pelas instituições financeiras

O crescimento das fraudes bancárias digitais intensificou a necessidade de adoção de mecanismos preventivos de segurança pelas instituições financeiras. Atualmente, os bancos

operam em ambiente altamente tecnológico e constantemente ameaçado por ataques cibernéticos, vazamentos de dados e práticas fraudulentas sofisticadas. Nesse contexto, a prevenção tornou-se elemento indispensável para a proteção dos consumidores e para a própria estabilidade do sistema financeiro.

As instituições financeiras possuem dever jurídico de garantir segurança adequada aos serviços disponibilizados aos consumidores. O Código de Defesa do Consumidor estabelece que o fornecedor responde pelos danos decorrentes de falhas na prestação do serviço, incluindo falhas relacionadas aos mecanismos de segurança digital. Dessa maneira, os bancos devem adotar medidas eficazes capazes de reduzir os riscos inerentes às operações eletrônicas.

Entre os principais mecanismos atualmente utilizados destacam-se a autenticação multifatorial, biometria facial, tokens de segurança, criptografia de dados, inteligência artificial e monitoramento em tempo real das transações financeiras. Essas tecnologias permitem identificar operações suspeitas e dificultam acessos indevidos às contas bancárias dos consumidores. Além disso, os sistemas de inteligência artificial vêm sendo utilizados para detectar padrões anormais de comportamento financeiro e prevenir possíveis fraudes.

Segundo Danilo Doneda, a proteção de dados pessoais constitui elemento indispensável para a preservação da liberdade e da autonomia dos indivíduos na sociedade da informação. Assim, os mecanismos de segurança bancária não possuem apenas finalidade patrimonial, mas também representam instrumento de proteção dos direitos fundamentais dos consumidores.

A responsabilidade preventiva das instituições financeiras também envolve o dever de informação e educação digital dos usuários. Muitas fraudes bancárias decorrem da utilização de técnicas de engenharia social, nas quais criminosos manipulam emocionalmente as vítimas para obtenção de dados pessoais e senhas bancárias. Por essa razão, os bancos devem promover campanhas educativas contínuas voltadas à conscientização dos consumidores acerca das práticas de segurança digital.

O Superior Tribunal de Justiça consolidou entendimento no sentido de que as instituições financeiras respondem objetivamente pelos danos decorrentes de fraudes e delitos praticados por terceiros no âmbito das operações bancárias. Tal entendimento reforça a necessidade de investimentos permanentes em segurança tecnológica e prevenção de riscos, considerando que os prejuízos decorrentes das falhas de segurança integram o risco da atividade econômica desempenhada pelos bancos.

Por fim, observa-se que a adoção de medidas preventivas eficazes representa importante instrumento de fortalecimento da confiança nas relações bancárias digitais. A combinação entre tecnologia, proteção de dados, educação digital e responsabilização civil das instituições financeiras contribui para maior segurança jurídica e para a efetiva proteção dos consumidores diante do crescente cenário de criminalidade cibernética.

5 CONSIDERAÇÕES FINAIS

O presente estudo analisou a responsabilidade civil das instituições financeiras diante do crescimento das fraudes bancárias digitais e dos acessos não autorizados a dados sensíveis dos consumidores, especialmente no contexto da expansão dos serviços financeiros eletrônicos no Brasil. A pesquisa demonstrou que a digitalização das relações bancárias trouxe inúmeros benefícios aos usuários, como praticidade e rapidez nas operações financeiras, porém também ampliou significativamente os riscos relacionados à criminalidade cibernética, ao vazamento de informações pessoais e às fraudes eletrônicas.

Ao longo do trabalho, verificou-se que o consumidor ocupa posição de vulnerabilidade nas relações de consumo, condição que se intensifica no ambiente digital em razão da desigualdade técnica e informacional existente entre os usuários e as instituições financeiras. A hipervulnerabilidade do consumidor nos serviços bancários digitais evidencia a necessidade de aplicação efetiva dos princípios previstos no Código de Defesa do Consumidor, especialmente os princípios da boa-fé objetiva, transparência, segurança e proteção da parte vulnerável da relação jurídica. Além disso, mostra-se necessário fortalecer medidas preventivas contra práticas abusivas, assegurando maior equilíbrio nas relações estabelecidas no ambiente digital.

Constatou-se ainda que a responsabilidade civil das instituições financeiras possui natureza objetiva, nos termos do artigo 14 do Código de Defesa do Consumidor, sendo desnecessária a comprovação de culpa para o surgimento do dever de indenizar. Nesse sentido, a jurisprudência consolidada do Superior Tribunal de Justiça, por meio da Súmula 479, reconhece que as instituições financeiras respondem pelos danos decorrentes de fraudes e delitos praticados por terceiros no âmbito das operações bancárias, considerando tais situações como fortuito interno inerente à atividade econômica desenvolvida pelos bancos.

A pesquisa também evidenciou a relevância da Lei Geral de Proteção de Dados Pessoais como instrumento de proteção dos consumidores no ambiente digital. A LGPD fortaleceu os

deveres das instituições financeiras quanto ao tratamento das informações pessoais dos clientes, exigindo medidas para prevenir acessos indevidos, vazamentos e violações de dados. Dessa forma, a proteção de dados passou a integrar os direitos fundamentais relacionados à privacidade, à dignidade e à segurança do consumidor.

Além disso, observou-se que a efetividade da tutela jurídica do consumidor depende não apenas da responsabilização posterior das instituições financeiras, mas também da adoção de medidas preventivas eficazes. A utilização de autenticação multifatorial, inteligência artificial, criptografia, monitoramento de operações suspeitas e campanhas de educação digital mostra-se essencial para reduzir os riscos das fraudes bancárias eletrônicas e fortalecer a confiança dos consumidores nos serviços financeiros digitais.

Outro ponto relevante identificado no estudo refere-se à necessidade de atuação conjunta entre instituições financeiras, Poder Judiciário, órgãos de proteção de dados e consumidores. O enfrentamento das fraudes digitais exige constante atualização tecnológica, aperfeiçoamento legislativo e fortalecimento das políticas públicas voltadas à segurança da informação e à educação digital da população. Nesse contexto, a cooperação entre os diversos agentes envolvidos torna-se indispensável para garantir maior efetividade à proteção jurídica dos consumidores.

Por fim, conclui-se que a responsabilização civil das instituições financeiras constitui importante mecanismo de proteção dos consumidores diante do crescente cenário de criminalidade cibernética. A aplicação conjunta do Código de Defesa do Consumidor e da Lei Geral de Proteção de Dados revela-se fundamental para assegurar equilíbrio nas relações bancárias digitais, impor maior dever de vigilância aos bancos e desestimular falhas de segurança. Essa integração normativa contribui para promover segurança jurídica e garantir a reparação dos danos suportados pelos consumidores vítimas de fraudes e acessos não autorizados a dados sensíveis.

REFERÊNCIAS

AGÊNCIA BRASIL. Metade dos brasileiros sofreu fraude em 2024, diz Serasa Experian. UOL Notícias, 25 mar.2025.Disponível em: https://noticias.uol.com.br/ultimas-noticias/agencia-brasil/2025/03/25/metade-dos-brasileiros-sofreu-fraude-em-2024-diz-serasa-experian.htm. Acesso em: 20 de abril de 2026.

AUTORIDADE Nacional de Proteção de Dados. Guia Orientativo: Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Brasília, 2022. Disponível em: ANPD – Guia de Segurança da Informação Acesso em: 20 de abril de 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: Planalto – Código de Defesa do Consumidor Acesso em: 15 de março de 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: Planalto – Lei Geral de Proteção de Dados Pessoais Acesso em: 01 de maio de 2026.

BRASIL. Superior Tribunal de Justiça (STJ). Recurso Especial n.º 1.197.929/PR. Rel. Min. Nancy Andrighi. Brasília, DF, julgado em 12 set. 2011. DJe 12 set. 2011. Disponível em: https://www.stj.jus.br/. Acesso em: 15 de março de 2026.

BRASIL. Superior Tribunal de Justiça (STJ). Recurso Especial n.º 2.037.088-SP. Rel. Min. Marco Aurélio Bellizze. Brasília, DF, julgamento em 7 mar. 2023. DJe 13 mar. 2023. Disponível em:https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/10082023-Contraditorio-nao-pode-ser-totalmente-vedado-na-hipotese-de-producao-antecipada-de-prova.aspx. Acesso em: 15 de março de 2026.

BRASIL. Superior Tribunal de Justiça (STJ). Súmula n.º 479. Brasília, DF, 27 jun. 2012. DJe 1 ago. 2012. Disponível em: https://arquivocidadao.stj.jus.br/index.php/sumula-479-2. Acesso em: 15 de março de 2026.

CHAVES, Rodrigo Almeida. A responsabilidade das instituições financeiras em face de golpes de engenharia social: análise à luz do Código de Defesa do Consumidor e da jurisprudência do STJ. Jus.com.br, 24 ago. 2024. Disponível em: https://jus.com.br/artigos/109740/a-responsabilidade-das-instituicoes-financeiras-em-face-de-golpes-de-engenharia-social-analise-a-luz-do-codigo-de-defesa-do-consumidor-e-da-jurisprudencia-do-stj. Acesso em: 01 de maio de 2026.

DIDIER JÚNIOR, Fredie. Curso de Direito Processual Civil: introdução ao direito processual civil – parte geral e processo de conhecimento. 23. ed. Salvador: JusPodivm, 2021. Acesso em: 01 de maio de 2026.

GONÇALVES, Carlos Roberto. Responsabilidade civil. 21. ed. São Paulo: Saraiva, 2021. Acesso em: 29 de abril de 2026.

GUARAGNI, Giovanni Vidal; KOZIKOSKI, Sandro Marcelo. Produção antecipada de prova ou ação autônoma de exibição de documento: a controvérsia sobre a prova documental no CPC/2015. Revista Eletrônica de Direito Processual, 2019. Disponível em: https://www.e-publicacoes.uerj.br/index.php/redp/article/view/40385. Acesso em: 29 de abril de 2026.

HIDD, Caroline de Carvalho Leitão; MAGALHÃES, Joseli Lima. A produção antecipada de prova sem o requisito da urgência como um meio para a resolução pacífica de conflitos. Revista de Processo, Jurisdição e Efetividade da Justiça, v. 9, n. 1, 2023. DOI: 10.26668/IndexLawJournals/2023.v9i1.9563. Disponível em: https://indexlaw.org/index.php/revistaprocessojurisdicao/article/view/9563. Acesso em: 29 de abril de 2026.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz; MITIDIERO, Daniel. Novo curso de processo civil: teoria do processo civil. 2. ed. São Paulo: Revista dos Tribunais, 2016. Acesso em: 29 de abril de 2026.

MITIDIERO, Daniel. A colaboração como norma fundamental do novo processo civil brasileiro. Revista do Advogado, São Paulo, n. 126, p. 47-52, maio 2015. Acesso em: 29 de abril de 2026.

MITIDIERO, Daniel Francisco. Colaboração no processo civil: pressupostos sociais, lógicos e éticos. 3. ed. rev. e ampl. São Paulo: Revista dos Tribunais, 2015. Acesso em: 29 de abril de 2026.

NADER, Paulo. Curso de direito civil: parte geral. 18. ed. Rio de Janeiro: Forense, 2018. Acesso em: 29 de abril de 2026.

NERY, Frank Gonçalves. A produção antecipada de provas no novo Código de Processo Civil. Revista da Escola da AGU (EAGU). Disponível em: https://revistaagu.agu.gov.br/index.php/EAGU/article/view/1950. Acesso em: 29 de abril de 2026.

OLIVEIRA DE REZENDE, Frederico Antonio. Responsabilidade civil dos bancos em relação às fraudes eletrônicas. Revista FMU Direito, São Paulo, ano 24, n. 32, p. 75-81, 2010. Disponível em:https://revistaseletronicas.fmu.br/index.php/FMUD/article/download/78/77/225. Acesso em: 29 de abril de 2026.