



CENTRO DE ESTUDOS SUPERIORES DE ITAITUBA – Ltda.

FACULDADE DE ITAITUBA – FAI
CURSO DE BACHARELADO EM DIREITO

JOAO VICTOR SILVA OLIVEIRA
LEONARDO ROCHA EVANGELISTA

**CRIMES CIBERNÉTICOS FINANCEIROS: Legislação,
Responsabilidade dos Bancos e Proteção das vítimas**

Itatuba-PA

2026

JOAO VICTOR SILVA OLIVEIRA
LEONARDO ROCHA EVANGELISTA

**CRIMES CIBERNÉTICOS FINANCEIROS: Legislação,
Responsabilidade dos Bancos e Proteção das vítimas**

Trabalho de Conclusão de Curso apresentado à
Faculdade de Itatuba para obtenção de título de
Bacharela em Direito.

Orientador(a): Arleison Glauber Pinheiro Sousa

Oliveira, João Victor Silva e Evangelista, Leonardo Rocha

CRIMES CIBERNÉTICOS FINANCEIROS: Legislação, Responsabilidade dos Bancos e Proteção das vítimas, Itaituba, Pará/ Leonardo Rocha Evangelista, João Victor Silva Oliveira. Itaituba: FAI, 2026.

43 fls.: il.

Orientador: Arleison Glauber Pinheiro Sousa

Trabalho de Conclusão de Curso (TCC) Graduação em Direito - Faculdade de Itaituba – Pará, 2026.

1. Direito 2. Crimes Cibernéticos Financeiros. I. Arleison Glauber Pinheiro Sousa. II. Faculdade de Itaituba, BR-PA, 2026.

JOAO VICTOR SILVA OLIVEIRA
LEONARDO ROCHA EVANGELISTA

**CRIMES CIBERNÉTICOS FINANCEIROS: Legislação,
Responsabilidade dos Bancos e Proteção das vítimas**

Trabalho de Conclusão de Curso apresentado à
Faculdade de Itaituba para obtenção de título de
Bacharel em Direito.

Orientador(a): Arleison Glauber Pinheiro Sousa

BANCA EXAMINADORA

Presidente/Orientador (a): _____

Prof. Arleison Glauber Pinheiro Sousa, Esp.

Avaliador (a) 1: _____ Nota: _____

Prof. Alexandre Do Rosário Brito, Esp.

Avaliador (a) 2: _____ Nota: _____

Prof. Thiago De Moraes Pereira, Esp.

Resultado: _____ Média: _____

Itaituba: 13 de abril 2026.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus pela vida, saúde e força para chegar até este momento tão importante.

Aos meus pais e familiares, pelo apoio incondicional, incentivo constante e compreensão durante toda a minha trajetória acadêmica.

Ao meu orientador, pela dedicação, paciência e valiosas contribuições, fundamentais para a realização deste trabalho.

Aos professores, pelos ensinamentos compartilhados ao longo do curso, que contribuíram para minha formação profissional e pessoal.

Por fim, agradeço a todos que, direta ou indiretamente, fizeram parte dessa conquista.

Dedico esta conquista aos meus pais, que com amor, esforço e sacrifício tornaram possível a realização deste sonho.

RESUMO

O avanço das tecnologias da informação e da comunicação transformou significativamente as relações financeiras, ampliando o uso de serviços bancários digitais e, conseqüentemente, expondo consumidores e instituições financeiras a novos riscos. Nesse contexto, os crimes cibernéticos financeiros passaram a ocorrer com maior frequência e sofisticação, envolvendo práticas como fraudes bancárias online, invasões de contas, engenharia social e o uso indevido de dados pessoais. Diante desse cenário, o presente trabalho tem como objetivo analisar a eficácia da legislação brasileira no combate aos crimes cibernéticos financeiros, bem como examinar a responsabilidade das instituições bancárias na prevenção e na reparação dos danos causados às vítimas dessas práticas ilícitas. A pesquisa adota abordagem qualitativa, de caráter exploratório e descritivo, desenvolvida por meio de revisão integrativa de literatura, com base em livros, artigos científicos, legislação e jurisprudência pertinentes ao tema. Os resultados indicam que, embora o ordenamento jurídico brasileiro tenha avançado com a edição de normas específicas, como a Lei nº 12.737/2012, a Lei nº 14.155/2021 e a Lei Geral de Proteção de Dados Pessoais, ainda persistem desafios relevantes na prevenção e no enfrentamento das fraudes digitais. Verifica-se, ainda, a consolidação do entendimento jurisprudencial acerca da responsabilidade objetiva das instituições financeiras, especialmente à luz do Código de Defesa do Consumidor. Conclui-se que a proteção eficaz das vítimas exige não apenas a responsabilização civil dos bancos, mas também a adoção de medidas preventivas, tecnológicas e educativas.

Palavras-chave: Crimes cibernéticos financeiros. Fraudes bancárias. Responsabilidade civil. Instituições financeiras. Proteção de dados pessoais.

ABSTRACT

The advancement of information and communication technologies has significantly transformed financial relations, expanding the use of digital banking services and, consequently, exposing consumers and financial institutions to new risks. In this context, financial cybercrimes have become more frequent and sophisticated, involving practices such as online banking fraud, account invasions, social engineering, and the misuse of personal data. Given this scenario, this study aims to analyze the effectiveness of Brazilian legislation in combating financial cybercrimes, as well as to examine the responsibility of banking institutions in preventing and repairing damages suffered by victims of these unlawful practices. The research adopts a qualitative, exploratory, and descriptive approach, developed through an integrative literature review based on books, scientific articles, legislation, and case law relevant to the topic. The results indicate that although the Brazilian legal system has advanced with the enactment of specific regulations, such as Law No. 12,737/2012, Law No. 14,155/2021, and the General Data Protection Law, significant challenges remain in preventing and addressing digital fraud. The study also highlights the consolidation of judicial understanding regarding the strict liability of financial institutions, especially under the Consumer Protection Code. It is concluded that effective protection of victims requires not only civil liability of banks but also the adoption of preventive, technological, and educational measures to reduce the incidence of financial cybercrimes.

Keywords: Financial cybercrimes. Banking fraud. Civil liability. Financial institutions. Data protection.

LISTA DE TABELA

Tabela 1.....	30
---------------	----

SUMÁRIO

1 INTRODUÇÃO	11
2 FUNDAMENTAÇÃO TEÓRICA	14
2.1 CRIMES CIBERNÉTICOS FINANCEIROS: CONCEITO E TIPOLOGIA	14
2.2 A LEGISLAÇÃO BRASILEIRA APLICÁVEL AOS CRIMES CIBERNÉTICOS	15
2.3 O CÓDIGO DE DEFESA DO CONSUMIDOR E A RESPONSABILIDADE OBJETIVA DOS BANCOS	17
2.4 JURISPRUDÊNCIA ATUAL SOBRE A RESPONSABILIDADE BANCÁRIA EM FRAUDES CIBERNÉTICAS	19
2.5 A EFICÁCIA DAS LEIS NO COMBATE ÀS FRAUDES DIGITAIS	21
2.6 MEDIDAS PREVENTIVAS E EDUCATIVAS NO ENFRENTAMENTO AOS CRIMES CIBERNÉTICOS	23
3. METODOS E INSTRUMENTOS	25
3.1 TIPO DE PESQUISA	25
3.2 DESCRITORES DA PESQUISA	26
3.3 BASE DE DADOS	26
3.4 CRITÉRIOS DE INCLUSÃO E EXCLUSÃO	27
3.5 ASPECTOS ÉTICOS	28
4. RESULTADOS E DISCUSSÕES	30
4.1 SÍNTESE DOS ACHADOS DA REVISÃO INTEGRATIVA	33
4.2 DISCUSSÃO CRÍTICA E ABORDAGEM EPISTEMOLÓGICA DOS ACHADOS	35
5. CONCLUSÃO	38
REFERÊNCIAS	40

1 INTRODUÇÃO

O avanço acelerado da tecnologia da informação e da comunicação transformou profundamente as relações sociais, econômicas e jurídicas, consolidando o ambiente digital como espaço central para a realização de transações financeiras e a prestação de serviços bancários. A ampliação do uso do internet banking, dos meios eletrônicos de pagamento e das plataformas digitais trouxe maior comodidade aos consumidores, mas também contribuiu para o crescimento significativo dos crimes cibernéticos de natureza financeira. Fraudes bancárias online, invasões de contas, golpes por engenharia social e o uso de softwares maliciosos tornaram-se práticas recorrentes, gerando prejuízos patrimoniais relevantes e comprometendo a confiança dos usuários no sistema financeiro.

No Brasil, esse cenário foi intensificado durante o período da pandemia de COVID-19, quando a necessidade de distanciamento social impulsionou a digitalização dos serviços bancários, ao mesmo tempo em que a atuação de criminosos virtuais se tornou mais sofisticada. Diante desse contexto, evidencia-se a necessidade de analisar a capacidade do ordenamento jurídico brasileiro em responder de forma eficaz às novas modalidades de crimes cibernéticos financeiros, especialmente no que se refere à proteção das vítimas e à responsabilização das instituições financeiras.

Nesse sentido, destacam-se diplomas legais relevantes para o enfrentamento dessas condutas ilícitas, como a Lei nº 12.737/2012, que tipificou crimes informáticos, a Lei nº 14.155/2021, que promoveu alterações no Código Penal para tratar especificamente da fraude eletrônica, e a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), que estabeleceu normas para o tratamento de dados pessoais e reforçou a tutela da privacidade no ambiente digital. A aplicação dessas normas suscita debates quanto à sua efetividade diante da complexidade e da constante evolução das práticas criminosas realizadas no meio virtual.

Diante desse cenário, o presente estudo é orientado pelas seguintes questões norteadoras: as normas jurídicas brasileiras são efetivas no combate às fraudes bancárias online? Qual é o grau de responsabilidade das instituições financeiras na prevenção e na reparação dos danos sofridos pelas vítimas dos crimes cibernéticos financeiros?

A relevância do tema justifica-se sob os aspectos social e jurídico. Do ponto de vista social, os crimes cibernéticos financeiros impactam diretamente a segurança patrimonial dos consumidores e a confiança nos sistemas bancários digitais. Sob o aspecto jurídico, observa-se o aumento expressivo da judicialização de demandas envolvendo fraudes bancárias, o que evidencia a importância da análise da responsabilidade civil das instituições financeiras, especialmente à luz do Código de Defesa do Consumidor, que reconhece a vulnerabilidade do consumidor e estabelece a responsabilidade objetiva dos fornecedores de serviços em casos de falhas na segurança.

O objetivo geral deste trabalho é analisar a eficácia da legislação brasileira no combate aos crimes cibernéticos financeiros, bem como examinar a responsabilidade das instituições bancárias na prevenção e na reparação dos danos causados às vítimas dessas práticas ilícitas. Como objetivos específicos, busca-se: compreender o conceito e a tipologia dos crimes cibernéticos financeiros no contexto brasileiro; identificar as principais legislações aplicáveis ao combate dessas fraudes e à proteção das vítimas; verificar de que forma o Código de Defesa do Consumidor fundamenta a responsabilidade objetiva das instituições financeiras em casos de fraudes digitais; analisar a atuação do Poder Judiciário nas decisões envolvendo fraudes bancárias online; e investigar medidas preventivas e educativas adotadas por instituições financeiras e órgãos públicos no enfrentamento aos crimes cibernéticos.

Quanto à metodologia, trata-se de uma pesquisa de natureza qualitativa, de caráter exploratório e descritivo, desenvolvida por meio de revisão integrativa de literatura. Foram utilizados livros, artigos científicos, legislação e jurisprudência pertinentes ao tema, selecionados a partir de critérios de relevância e atualidade, com o objetivo de compreender de forma sistemática os principais entendimentos doutrinários e jurídicos relacionados aos crimes cibernéticos financeiros.

No que se refere aos principais autores, o trabalho fundamenta-se nas contribuições de Pinheiro, no campo do direito digital e da segurança da informação; Tartuce e Nunes, no que diz respeito à aplicação do Código de Defesa do Consumidor e à responsabilidade civil; Tepedino e Schreiber, quanto à teoria do risco e à função preventiva da responsabilidade civil; e Bioni e Doneda, no âmbito da proteção de dados pessoais e da privacidade no ambiente digital.

Por fim, quanto à estrutura do trabalho, além desta introdução, o estudo está organizado em capítulos que abordam a fundamentação teórica dos crimes

cibernéticos financeiros, a metodologia da pesquisa, a análise dos resultados e discussões obtidos a partir da revisão integrativa, e, por fim, a conclusão, na qual são retomados os objetivos propostos e apresentadas as considerações finais sobre o tema.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Crimes Cibernéticos Financeiros: Conceito E Tipologia

Os crimes cibernéticos financeiros têm se tornado uma das maiores ameaças à segurança global, especialmente com a crescente digitalização das atividades econômicas. O conceito de crime cibernético financeiro pode ser entendido como qualquer ato ilícito realizado no ambiente virtual com a intenção de prejudicar ou subtrair recursos financeiros de uma pessoa, organização ou Estado. Estes crimes podem ocorrer por meio de diversas técnicas e estratégias, e estão em constante evolução devido ao avanço da tecnologia digital.

De acordo com Wendt e Jorge (2021, p.38), "o termo "crimes cibernéticos" para definir os delitos praticados por intermédio de dispositivos informáticos (computadores, notebooks, celulares etc.) conectados ou não a internet." Esses crimes não se limitam apenas ao furto de dados bancários ou invasões em sistemas de pagamento, mas podem também incluir fraudes em investimentos, lavagem de dinheiro, roubo de identidade e outros esquemas fraudulentos complexos.

Os tipos de crimes cibernéticos financeiros são diversos e variam conforme a técnica empregada. Dentre as principais modalidades, destacam-se a fraude eletrônica (como os esquemas de phishing e vishing), a manipulação de transações financeiras e o roubo de dados bancários. A fraude eletrônica é uma das mais comuns e ocorre quando o criminoso se utiliza de e-mails falsificados, sites fraudulentos ou mensagens de texto para enganar a vítima e obter suas informações bancárias. Como explica Vaz (2023, p.7), "os crimes digitais acontecem por meio de diferentes abordagens, truques ou armadilhas, envolvendo diferentes tipos de pessoas. Os criminosos utilizam padrões de comportamento da população, de informações e/ou do elemento "surpresa".".

Outro tipo relevante de crime cibernético financeiro é a lavagem de dinheiro digital, que envolve o uso de criptomoedas e outras formas de pagamento virtual para ocultar a origem ilícita de fundos. A natureza descentralizada das criptomoedas torna difícil o monitoramento e a fiscalização dessas transações, tornando-as atrativas para criminosos. Em relação a esse tipo de crime

A evolução da criptomoeda e das tecnologias de blockchain traz novos desafios para a segurança cibernética. Embora essas tecnologias ofereçam vantagens em termos de segurança e transparência, elas também têm sido exploradas por criminosos para realizar atividades ilícitas, como lavagem de

dinheiro e financiamento de atividades criminosas. (FERNANDES, 2024, p. 65).

A evolução da tecnologia também tem levado à criação de novos tipos de crimes cibernéticos, como os ataques a sistemas de pagamento e as fraudes envolvendo inteligência artificial. Estes crimes são ainda mais complexos e difíceis de identificar, pois os algoritmos usados podem alterar rapidamente os dados financeiros de uma organização sem deixar rastros. De acordo com

A utilização da inteligência artificial e machine learning por parte dos golpistas para automatizar ataques e personalizar mensagens de phishing e uma tendência crescente. Isso torna ainda mais desafiador para os usuários identificarem tentativas de fraudes, exigindo um esforço contínuo para educá-los sobre as melhores práticas de segurança. (FERNANDES, 2024, p. 10).

Outro aspecto importante no contexto dos crimes cibernéticos financeiros é o impacto global. Com a globalização digital, esses crimes podem ocorrer em qualquer parte do mundo, afetando indivíduos e empresas de qualquer país. Isso tem levado à necessidade de cooperação internacional em investigações e na criação de políticas de segurança cibernética mais robustas.

A colaboração ente diferentes agências e organizações é fundamental para maximizar a eficácia das ferramentas de análise forense. O compartilhamento de informações e a cooperação internacional podem proporcionar uma visão mais abrangente das ameaças cibernéticas e permitir a disseminação das melhores práticas. (FERNANDES, 2024, p. 37)

Portanto, os crimes cibernéticos financeiros são um fenômeno complexo e multifacetado que exige atenção constante e esforços colaborativos para mitigar seus impactos. Com o avanço da tecnologia, é fundamental que as políticas de segurança digital evoluam para proteger tanto os indivíduos quanto as organizações contra esse tipo de crime.

2.2 A Legislação Brasileira Aplicável Aos Crimes Cibernéticos

O enfrentamento aos crimes cibernéticos no Brasil exige uma análise das normas jurídicas que tratam da proteção contra fraudes, invasões, roubo de dados e outras práticas ilícitas realizadas no ambiente digital. Nos últimos anos, o país tem se esforçado para atualizar sua legislação com o intuito de combater essas infrações, garantindo mais segurança à população e às empresas no uso de tecnologias digitais. A legislação brasileira sobre crimes cibernéticos é relativamente recente, mas vem se expandindo para enfrentar os desafios impostos pela evolução tecnológica.

A Lei nº 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann, é um marco importante no combate aos crimes cibernéticos no Brasil. Essa lei tipificou como crime a invasão de dispositivos informáticos, como computadores, celulares e outros aparelhos conectados à internet, com o intuito de obter, adulterar ou destruir dados sem a autorização do titular. Segundo Montel e Paiva (2024, p.7), "A lei traz a clara percepção de que apesar de sucinta, aponta uma maneira de regular e punir as ações criminosas que corriqueiramente ocorrem no ambiente digital." Com isso, a Lei Carolina Dieckmann se tornou um importante instrumento para o enfrentamento da crescente incidência de crimes digitais.

Outro ponto relevante na legislação brasileira é a Lei nº 13.709/2018, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD). Embora a LGPD tenha um foco principal na proteção de dados pessoais, ela também é fundamental para a prevenção de crimes cibernéticos, pois estabelece regras rigorosas para o tratamento de dados pessoais por empresas e órgãos públicos. Em relação aos crimes cibernéticos, a LGPD prevê penalidades severas para a violação de dados pessoais, o que tem impacto direto na proteção contra fraudes e roubo de informações. Como Fernandes fala (2025, p. 03), "a Lei Geral de Proteção de Dados (LGPD), implementada no Brasil em 2020, estabelece diretrizes rigorosas sobre como as informações pessoais devem ser tratadas, ressaltando a responsabilidade das empresas em proteger os dados de seus clientes."

Adicionalmente, o Código Penal Brasileiro (Decreto-Lei nº 2.848, de 7 de dezembro de 1940), embora não seja uma legislação específica para crimes cibernéticos, já prevê diversos dispositivos que podem ser aplicados a essas infrações. O artigo 155, por exemplo, trata do crime de furto, e pode ser utilizado em casos de subtração de dados bancários ou outras informações financeiras por meio de técnicas digitais. No entanto, a legislação penal tradicional, em muitos casos, não é suficiente para enfrentar as especificidades dos crimes cibernéticos, razão pela qual a criação de leis específicas tem se mostrado necessária.

o entendimento dos tribunais tem se moldado para abranger a complexidade dos crimes cibernéticos, destacando a importância de aplicar as leis existentes a novos cenários e tecnologias emergentes. Assim, a caracterização de um crime como eletrônico muitas vezes depende do uso desse meio para a execução do tipo penal, refletindo a adaptabilidade da lei à era digital. (MIGUEL, 2024, p.61)

A Lei nº 13.840/2019 também tem relevância no contexto dos crimes cibernéticos, pois estabelece normas para o enfrentamento de crimes relacionados ao uso indevido de tecnologias, especialmente em relação ao combate ao crime organizado e à lavagem de dinheiro. Ela também regula aspectos de crimes praticados por meio de tecnologias de comunicação, como o uso de dados falsificados ou adulterados para realizar fraudes em transações financeiras.

Além disso, a Lei nº 12.965/2014, conhecida como o Marco Civil da Internet, foi um passo fundamental para estabelecer direitos e deveres no uso da internet, incluindo questões relacionadas à privacidade, proteção de dados e segurança digital. O Marco Civil da Internet tem uma função preventiva, pois cria uma base legal para a responsabilização de provedores de serviços na internet e garante aos usuários um maior controle sobre seus dados. De acordo com Maia e Costa (2023), "o Brasil atualizou o Marco Civil da Internet (Lei 12.965/2014) como um marco legal que estabelece princípios, garantias, direitos e deveres para o uso da internet no país. O marco civil regula a neutralidade da rede, a privacidade dos usuários e a responsabilidade dos provedores de serviços online."

Portanto, a legislação brasileira está em processo de evolução para enfrentar os crimes cibernéticos, mas ainda existem desafios significativos, como a necessidade de harmonização entre as leis existentes e a atualização constante diante de novos tipos de crimes digitais. A implementação de uma legislação mais robusta e a adaptação das autoridades judiciais e policiais são fundamentais para melhorar a eficácia no combate aos crimes cibernéticos.

2.3 O Código De Defesa Do Consumidor e a Responsabilidade Objetiva Dos Bancos

A proteção dos consumidores em casos de crimes cibernéticos financeiros envolve diretamente o Código de Defesa do Consumidor (CDC), instituído pela Lei nº 8.078/1990, que estabelece normas de proteção e defesa dos consumidores no Brasil. Com o aumento das fraudes virtuais, especialmente no setor bancário, tornou-se essencial analisar como o CDC se aplica às relações entre instituições financeiras e seus clientes, em especial no tocante à responsabilidade objetiva dos bancos por danos causados em decorrência de falhas na segurança de seus sistemas.

O artigo 14 do CDC dispõe que o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados ao consumidor por defeitos relativos à prestação dos serviços. Isso significa que, em

regra, os bancos são objetivamente responsáveis por prejuízos financeiros sofridos por clientes em decorrência de falhas em sua infraestrutura digital, como invasões, fraudes bancárias e transações não autorizadas. Como afirma Moreira (2023, p. 35), “a responsabilidade das instituições bancárias nos crimes virtuais na modalidade de responsabilidade por ato ilícito cometida por terceiros, vez que, sendo fornecedoras de serviços bancários, decorre do risco de desempenho de sua atividade o dano sofrido a vítima.”

Essa interpretação é amplamente aceita nos tribunais brasileiros. Diversas decisões judiciais reconhecem a responsabilidade das instituições financeiras em casos de fraudes, mesmo quando alegam que o cliente agiu com negligência. O entendimento majoritário é de que o banco, por dispor de tecnologia e recursos para proteger seus sistemas, tem o dever de garantir a segurança das transações. Conforme explica Madureira (2024, p.06), “se a instituição financeira e o Banco Central lucram milhões por ano com pagamentos instantâneos, esta também devem ter ciência dos riscos que seu empreendimento agrega ao consumidor.”

Ademais, o Superior Tribunal de Justiça (STJ) tem consolidado o entendimento de que é responsabilidade do banco adotar mecanismos eficazes de segurança da informação. Em casos de falha desses mecanismos, a indenização ao consumidor prejudicado é considerada medida justa e necessária. A Súmula 479 do STJ reforça essa posição ao afirmar 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.”

A responsabilidade objetiva dos bancos também se aplica aos casos de vazamento de dados, situações em que informações bancárias do cliente são indevidamente expostas, permitindo a atuação de fraudadores. De acordo com o CDC, é obrigação do fornecedor manter o sigilo dos dados fornecidos pelo consumidor. Se esses dados forem utilizados de forma fraudulenta por terceiros, e for constatada a falha no serviço de proteção, o banco será responsabilizado. Sobre isso, Pereira (2018, p.52) ressalta: “não há discussão acerca da devida responsabilização das instituições financeiras por danos ocasionados por terceiros quando esse dano decorrer de um fortuito interno, afinal é um risco esperado de uma atividade da qual os bancos auferem lucros exorbitantes, sendo aplicável aqui a teoria do risco na modalidade risco-proveito.”

A jurisprudência também demonstra que não basta ao banco alegar que a transação foi autorizada com senha ou token para se eximir da responsabilidade. Há a necessidade de prova de que o consumidor, de fato, foi o autor da operação ou agiu de maneira dolosa ou extremamente negligente, o que é raro nos casos de ataques cibernéticos sofisticados. Em muitos casos, os consumidores são vítimas de fraudes altamente técnicas e complexas, das quais não possuem meios de se proteger com eficácia, o que reforça a importância da proteção jurídica conferida pelo CDC.

Assim, ao prever a responsabilidade objetiva das instituições bancárias, o Código de Defesa do Consumidor oferece uma importante proteção ao cliente diante dos riscos cada vez maiores de crimes cibernéticos financeiros. A atuação proativa das instituições financeiras na prevenção de fraudes e na segurança de seus sistemas é não apenas uma obrigação legal, mas também uma necessidade ética diante da vulnerabilidade dos consumidores nesse ambiente digital.

2.4 Jurisprudência Atual Sobre A Responsabilidade Bancária Em Fraudes Cibernéticas

A digitalização dos serviços bancários e a popularização dos meios eletrônicos de pagamento, como o PIX, trouxeram novas possibilidades de consumo e transações, mas também um aumento expressivo nas fraudes cibernéticas. Diante desse cenário, a jurisprudência brasileira tem reconhecido a necessidade de ampliação do dever de segurança das instituições financeiras, aplicando o regime de responsabilidade objetiva, previsto no artigo 14 do Código de Defesa do Consumidor (CDC) (BRASIL, 1990).

O Superior Tribunal de Justiça (STJ) consolidou entendimento nesse sentido por meio da Súmula nº 479. Assim, o banco responde pelos danos resultantes de falhas sistêmicas, vulnerabilidades de segurança e deficiências no controle de operações suspeitas, por se tratar de riscos inerentes à própria atividade.

No mesmo sentido, o Tema Repetitivo nº 466 do STJ firmou a tese de que a responsabilidade das instituições financeiras é objetiva, e que a ocorrência de fraude eletrônica se insere no risco da atividade bancária (STJ, 2015). Esse entendimento é reforçado pelo Recurso Especial nº 2.088.100/SP, julgado em 30 de outubro de 2023, no qual o tribunal afirmou que o banco tem o dever de impedir movimentações atípicas e incompatíveis com o perfil do cliente, sob pena de configurar falha na prestação do serviço (STJ, 2023).

A doutrina de Filho (2019, p. 89) fundamenta esse entendimento ao explicar que, “A responsabilidade objetiva funda-se na teoria do risco da atividade, segundo a qual todo aquele que se disponha a exercer alguma atividade no mercado de consumo deve responder pelos danos que causar aos consumidores, independentemente de culpa, por representar risco a terceiros.”

A partir dessa concepção, compreende-se que a atividade bancária, por sua natureza e pelo uso intensivo de tecnologia, envolve riscos previsíveis, razão pela qual o fornecedor deve adotar medidas eficazes de prevenção, monitoramento e proteção de dados, sob pena de responder civilmente pelos prejuízos ocasionados ao consumidor.

No contexto estadual, o Tribunal de Justiça do Estado do Pará (TJPA) tem aplicado a orientação do STJ em diversos julgados sobre fraudes eletrônicas. No Processo nº 0801730-45.2023.8.14.0301, a 3ª Câmara Cível manteve condenação de um banco que permitiu movimentações financeiras incompatíveis com o perfil do cliente, reconhecendo a falha na prestação do serviço e a consequente responsabilidade objetiva (PARÁ, 2024).

De forma semelhante, no Processo nº 0815554-29.2024.8.14.0006, a 2ª Turma de Direito Privado reafirmou que “as instituições financeiras possuem o dever de zelar pela segurança de suas plataformas digitais, respondendo objetivamente pelos prejuízos decorrentes de fraudes que poderiam ser evitadas mediante o uso de mecanismos tecnológicos adequados” (PARÁ, 2025, online).

Contudo, o Tribunal também tem admitido hipóteses de culpa concorrente do consumidor, nos casos em que há fornecimento voluntário de senhas ou dados de acesso. No Processo nº 0810293-62.2023.8.14.0401, a 1ª Turma de Direito Privado reduziu a indenização com base no artigo 945 do Código Civil, reconhecendo que o consumidor contribuiu para o evento danoso (PARÁ, 2024).

A análise conjunta da jurisprudência nacional e estadual revela convergência no sentido de atribuir às instituições financeiras o dever de prevenir e mitigar riscos cibernéticos, responsabilizando-as objetivamente pelos danos quando houver falha de segurança. O entendimento predominante é que a fraude eletrônica constitui fortuito interno, integrante do risco da atividade, afastando a alegação de caso fortuito ou força maior.

Desse modo, a evolução jurisprudencial demonstra que o dever de segurança passou a integrar o núcleo da prestação dos serviços bancários, reforçando a

proteção do consumidor e estimulando as instituições financeiras a investirem em tecnologia e controle antifraude.

2.5 A Eficácia Das Leis No Combate Às Fraudes Digitais

O combate às fraudes digitais tem se tornado um dos maiores desafios jurídicos do século XXI, exigindo das legislações nacionais respostas rápidas, atualizadas e eficazes frente à velocidade com que os crimes cibernéticos evoluem. No Brasil, diversas leis têm sido criadas ou adaptadas para enfrentar esse cenário, como a Lei Carolina Dieckmann (Lei nº 12.737/2012), a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014) e dispositivos do Código Penal e Código de Defesa do Consumidor (CDC). No entanto, a eficácia dessas normas ainda é tema de intensos debates, especialmente quanto à sua aplicação prática e à capacidade do Estado em investigar e punir efetivamente os autores das fraudes digitais.

A eficácia das leis não depende apenas de sua existência formal, mas também da sua aplicabilidade, da infraestrutura do sistema judiciário e policial e da cooperação internacional. Crimes digitais, por sua natureza transnacional, muitas vezes envolvem criminosos localizados fora do país da vítima, o que dificulta a persecução penal. Como explica Wendt e Jorge (2021, p. 306), “a falta de capacitação dos policiais e também de outros autores da persecução penal, como o Ministério Público e o Judiciário, representa um grande desafio, na medida em que pode impedir a punição dos cibercriminosos e, por consequência, causar impunidade.” Ou seja, sem investimentos em capacitação de agentes públicos, inteligência cibernética e mecanismos de rastreamento digital, a legislação corre o risco de se tornar letra morta.

Um dos avanços mais significativos foi a entrada em vigor da LGPD, que ampliou a responsabilidade de empresas e instituições públicas no tratamento e proteção de dados pessoais. A lei trouxe sanções administrativas relevantes e promoveu uma cultura de compliance digital, sobretudo no setor privado. No entanto, ainda há lacunas em sua aplicação prática. Conforme Lisboa (2024, p. 191) fala, “as empresas podem enfrentar multas e sanções regulatórias significativas por falhas em proteger dados de clientes ou informações confidenciais. Além disso, empresas que sofrem ataques de engenharia social podem ser responsabilizadas legalmente se for determinado que não tomaram medidas adequadas para proteger as informações.”

Outro aspecto relevante é a falta de padronização e agilidade nas decisões judiciais, o que gera insegurança jurídica tanto para vítimas quanto para instituições. Enquanto alguns tribunais aplicam rigorosamente a responsabilidade objetiva dos bancos, outros ainda relativizam essa responsabilização, baseando-se na conduta da vítima, especialmente quando há alegações de negligência no uso de senhas ou dispositivos. Esse cenário prejudica a uniformidade da jurisprudência e impacta a percepção da eficácia das leis por parte da sociedade.

Ademais, é preciso considerar que as leis, por mais modernas que sejam, raramente acompanham o ritmo das inovações tecnológicas. A criação de golpes com uso de inteligência artificial, deepfakes, bots automatizados e malwares de última geração mostra que os criminosos digitais estão sempre um passo à frente do legislador. Segundo Cunha e Cortizo (2024, p. 09), “é crucial reconhecer que, a rápida evolução da tecnologia exige atualizações constantes das leis para permanecerem relevantes, uma vez que, a legislação muitas das vezes não consegue acompanhar o ritmo do avanço tecnológico.”

Apesar desses desafios, há avanços notáveis. O Judiciário tem ampliado o reconhecimento do dano moral em casos de fraude digital, o que serve como forma de coibir práticas ilícitas e pressionar instituições a adotarem sistemas de segurança mais eficazes. Além disso, o aumento da cooperação internacional entre autoridades, como por meio da Convenção de Budapeste sobre Crimes Cibernéticos, tem se mostrado um instrumento promissor para a identificação e punição de criminosos transnacionais.

É importante considerar não apenas a legislação interna, mas também os instrumentos normativos de caráter internacional. Nesse contexto, destaca-se a Convenção de Budapeste sobre o Cibercrime, adotada em 2001 pelo Conselho da Europa, considerada o principal tratado internacional voltado ao enfrentamento dos delitos praticados no ambiente digital.

A referida convenção estabelece parâmetros para a tipificação de condutas ilícitas, bem como diretrizes para a coleta e preservação de provas eletrônicas, além de mecanismos de cooperação jurídica internacional. Tais elementos são fundamentais diante da natureza transnacional dos crimes cibernéticos, que frequentemente envolvem múltiplas jurisdições.

A adesão do Brasil à Convenção de Budapeste, formalizada por meio do Decreto nº 10.977/2022, representa um avanço significativo no fortalecimento da

eficácia das normas nacionais, na medida em que amplia a capacidade de investigação e repressão dessas práticas ilícitas.

Portanto, embora o Brasil disponha de um arcabouço legal relativamente robusto para enfrentar as fraudes digitais, sua eficácia ainda esbarra em fatores estruturais, técnicos e interpretativos. É necessário fortalecer a fiscalização, modernizar constantemente a legislação, investir em inteligência policial digital e promover a cooperação internacional como pilares para um combate efetivo aos crimes cibernéticos financeiros.

2.6 Medidas Preventivas E Educativas No Enfrentamento Aos Crimes Cibernéticos

Diante da crescente sofisticação dos crimes cibernéticos, especialmente no setor financeiro, o enfrentamento eficaz dessas práticas vai além da atuação repressiva do Estado. As medidas preventivas e educativas têm se mostrado fundamentais para reduzir a incidência de fraudes digitais e proteger tanto os consumidores quanto as instituições. A conscientização da população, a adoção de boas práticas de segurança digital e o investimento em tecnologia preventiva são ações essenciais para a construção de um ambiente virtual mais seguro.

A educação digital é uma das principais ferramentas de prevenção. O letramento digital da população, especialmente dos usuários de serviços bancários, pode reduzir significativamente o sucesso de ataques cibernéticos, como phishing, engenharia social e clonagem de aplicativos. Segundo Mascarenhas, Menck e Silva (2025, p. 08), “apesar do avanço tecnológico, a educação digital continua sendo uma das defesas mais eficazes contra os crimes virtuais. A maior parte dos ataques de phishing ainda depende da ação humana, ou seja, da resposta do usuário frente a uma mensagem maliciosa.” Campanhas de conscientização promovidas por bancos, órgãos governamentais e entidades civis devem ser constantes, atualizadas e acessíveis, alertando sobre os principais golpes em circulação e ensinando práticas seguras, como não clicar em links suspeitos, manter senhas fortes e ativar autenticação em dois fatores.

Nesse sentido, o Poder Público tem papel decisivo, seja por meio da inserção da educação digital nos currículos escolares, seja pela criação de políticas públicas voltadas à inclusão e proteção digital da população. A atuação de órgãos como o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) também é relevante, já que promove alertas e diretrizes sobre segurança

cibernética. Além disso, a cooperação entre governo, setor privado e sociedade civil deve ser incentivada, formando uma rede de proteção eficaz e multidisciplinar.

No campo técnico, as medidas preventivas implementadas pelas instituições financeiras também são fundamentais. Investir em sistemas de detecção de fraudes em tempo real, monitoramento contínuo de transações e autenticação biométrica são práticas que fortalecem a segurança dos serviços digitais. A resiliência cibernética, conceito cada vez mais explorado na área da segurança da informação, envolve não apenas prevenir ataques, mas garantir que, em caso de violação, os danos sejam minimizados e os serviços restaurados rapidamente. Conforme explica

o enfrentamento em tecnologia avançada e infraestrutura de segurança é crucial. Governos devem fomentar a pesquisa e o desenvolvimento de novas tecnologias de defesa cibernética, além de garantir que as forças de segurança tenham os recursos necessários para enfrentar ameaças complexas. Programas de treinamento e capacitação contínua para profissionais de segurança cibernética também são essenciais para acompanhar a rápida evolução das técnicas de ataque cibernético. (PENA; FILHO; GALIZA; MARQUES, 2025, p.13)

Além disso, os próprios consumidores devem ser protagonistas na sua proteção digital. A adoção de boas práticas individuais, como a verificação de remetentes, a não exposição de dados sensíveis em redes sociais e o uso de softwares originais e atualizados, pode reduzir consideravelmente os riscos. O empoderamento do usuário no uso seguro das ferramentas digitais é um elemento chave na equação da cibersegurança.

No âmbito institucional, programas de compliance digital, auditorias regulares de segurança e simulações de ataques (testes de intrusão) também são estratégias adotadas por bancos e empresas para identificar vulnerabilidades e agir preventivamente. Essas práticas devem estar alinhadas às exigências da Lei Geral de Proteção de Dados (LGPD), que impõe o dever de proteção da informação como parte da responsabilidade civil das instituições.

Por fim, a integração entre educação, prevenção e repressão forma o tripé essencial para o enfrentamento dos crimes cibernéticos. Se por um lado o Estado deve atuar punindo os responsáveis por fraudes, por outro, deve promover a informação e exigir das empresas a adoção de tecnologias eficazes. O combate ao crime digital, portanto, exige uma abordagem geral e contínua, com a participação ativa de todos os setores da sociedade.

3. METODOS E INSTRUMENTOS

3.1 Tipo de Pesquisa

Segundo Gil (2019, p. 8), “a metodologia é o caminho do pensamento e a prática exercida na abordagem da realidade, envolvendo tanto os métodos quanto as técnicas que possibilitam a construção do conhecimento”. Essa seção tem por objetivo apresentar o percurso metodológico utilizado no desenvolvimento da pesquisa sobre crimes cibernéticos financeiros, indicando o tipo de pesquisa, os descritores, as bases de dados, os critérios de inclusão e exclusão e os aspectos éticos observados.

O presente estudo caracteriza-se como uma revisão integrativa de literatura, associada a uma revisão bibliográfica e documental, com abordagem qualitativa, exploratória e descritiva. Segundo Prodanov e Freitas (2013, p. 55), “a revisão integrativa da literatura tem como objetivo reunir e sintetizar resultados de pesquisas anteriores sobre um determinado tema, de forma sistemática e ordenada, contribuindo para a compreensão e o avanço do conhecimento científico”. Essa modalidade de revisão permite integrar diferentes perspectivas teóricas e empíricas, fornecendo um panorama consolidado do estado atual do tema pesquisado justificando o uso de fontes normativas e jurisprudenciais recentes sobre crimes cibernéticos financeiros. Assim, a revisão integrativa sustentada por fontes bibliográficas e documentais oferece uma análise abrangente e crítica sobre o fenômeno jurídico das fraudes digitais e a responsabilidade das instituições financeiras.

Sendo fundamentada em fontes bibliográficas e documentais, visando reunir materiais teóricos, normativos e jurisprudenciais sobre o tema. Conforme Marconi e Lakatos (2021, p. 43), “a pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros, artigos científicos e documentos”. Gil (2019, p. 52) complementa que “a pesquisa documental utiliza materiais que ainda não receberam tratamento analítico, como leis, decisões judiciais e relatórios institucionais”.

Caracteriza-se como uma pesquisa qualitativa, exploratória e descritiva. Segundo Marconi e Lakatos (2021, p. 47), “a pesquisa qualitativa busca compreender fenômenos sociais complexos, valorizando o significado, o contexto e as relações humanas envolvidas”.

Para Gil (2019, p. 27), “a pesquisa exploratória tem como principal finalidade desenvolver, esclarecer e modificar conceitos e ideias, com vistas à formulação de

problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores”. Essa característica é especialmente relevante, uma vez que os crimes cibernéticos financeiros configuram um campo em constante mutação, exigindo atualização contínua e reflexão crítica sobre seus desdobramentos jurídicos.

Vergara (2016, p. 42) complementa que “a pesquisa descritiva expõe características de determinada população ou fenômeno e estabelece correlações entre variáveis sem interferir nelas”. Assim, a pesquisa propõe-se a descrever e analisar a atuação do ordenamento jurídico brasileiro diante das fraudes eletrônicas bancárias, abordando a responsabilidade das instituições financeiras e o impacto das normas de proteção de dados pessoais.

3.2 Descritores da Pesquisa

Segundo Gil (2019, p. 66), “os descritores constituem palavras ou expressões utilizadas para identificar e localizar informações pertinentes ao tema pesquisado”. Dessa forma, foram adotados descritores que representam as dimensões jurídica, tecnológica e social do fenômeno investigado.

Os descritores definidos para esta pesquisa foram: “crimes cibernéticos financeiros”, “fraudes eletrônicas bancárias”, “responsabilidade civil de instituições financeiras”, “direito digital”, “proteção de dados pessoais”, “Marco Civil da Internet” e “Lei Geral de Proteção de Dados (LGPD)”.

Além disso, conforme Marconi e Lakatos (2021, p. 78), “a definição precisa de descritores permite delimitar o campo de estudo e evita dispersões durante a coleta e análise de dados”. A escolha dos descritores foi feita a partir de uma revisão prévia das obras de referência em Direito Digital e Cibernético, assegurando a consistência teórica da pesquisa.

3.3 Base de Dados

A coleta das informações utilizadas neste estudo foi realizada em bases de dados científicas e jurídicas amplamente reconhecidas, com o objetivo de reunir materiais atualizados e relevantes sobre crimes cibernéticos financeiros, proteção de dados e responsabilidade civil das instituições bancárias.

Segundo Gil (2019, p. 90), “a escolha das fontes de informação deve obedecer a critérios de relevância, atualidade e confiabilidade, de modo a assegurar a qualidade científica do estudo”. Assim, priorizaram-se bases que contêm publicações de caráter

acadêmico, técnico e jurídico, garantindo consistência e validade aos resultados obtidos.

As principais bases consultadas foram: Google Acadêmico; repositórios jurídicos oficiais, como o Superior Tribunal de Justiça (STJ), o Supremo Tribunal Federal (STF) e o Tribunal de Justiça do Pará (TJPA).

De acordo com Prodanov e Freitas (2013, p. 56), “a busca de informações em bases de dados confiáveis é essencial para o desenvolvimento de uma pesquisa científica, pois garante a fidedignidade das fontes e evita distorções interpretativas”. Por esse motivo, foram selecionadas plataformas que reúnem artigos revisados por pares, livros digitais, legislações, decisões judiciais e publicações institucionais pertinentes ao tema.

Além disso, foram analisados documentos legais, como o Código de Defesa do Consumidor (Lei nº 8.078/1990), o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), os quais constituem o principal arcabouço normativo sobre segurança digital e proteção de consumidores em ambiente virtual.

Portanto, a utilização dessas bases de dados assegurou a abrangência e a atualização da pesquisa, permitindo uma análise confiável das fontes doutrinárias, legais e jurisprudenciais que embasam o estudo.

3.4 Critérios de Inclusão e Exclusão

Para garantir a relevância, atualidade e credibilidade das fontes, foram definidos critérios de inclusão e exclusão. De acordo com Vergara (2016, p. 63), “a definição de critérios de seleção assegura a coerência e o foco da pesquisa, evitando a dispersão temática”.

Foram incluídos estudos publicados entre 2013 e 2025, que abordassem: crimes cibernéticos e fraudes financeiras; responsabilidade civil e penal das instituições bancárias; proteção de dados e segurança da informação.

Foram excluídos materiais sem fundamentação científica ou jurídica, textos opinativos não revisados por pares e estudos anteriores a 2018, exceto aqueles considerados clássicos no campo do Direito Digital. Como ressaltam Marconi e Lakatos (2021, p. 77), “a escolha criteriosa das fontes garante validade científica e evita vieses interpretativos”.

Essa delimitação permitiu selecionar produções recentes e juridicamente relevantes, compatíveis com a evolução normativa e tecnológica contemporânea.

3.5 Aspectos Éticos

A ética e o respeito à propriedade intelectual constituem pilares fundamentais de qualquer produção científica. Gil (2019, p. 102) afirma que “a ética na pesquisa científica está diretamente ligada à honestidade do pesquisador, à fidedignidade das fontes e ao respeito aos direitos autorais”.

De acordo com Marconi e Lakatos (2021, p. 94), “toda pesquisa deve pautar-se na integridade moral e intelectual, evitando o plágio e reconhecendo devidamente as contribuições de outros autores”. Por essa razão, este estudo segue rigorosamente as normas de citação e referência estabelecidas pela Associação Brasileira de Normas Técnicas (ABNT), especialmente a NBR 10520:2002, que “especifica as condições exigíveis para a apresentação de citações em documentos” (ABNT, 2002, p. 1), e a NBR 6023:2018, que “define os elementos a serem incluídos nas referências, bem como sua ordem e convenções tipográficas” (ABNT, 2018, p. 2).

O ordenamento jurídico brasileiro também prevê dispositivos legais que garantem e protegem o direito à autoria e à propriedade intelectual. A Lei nº 9.610, de 19 de fevereiro de 1998, que consolida a legislação sobre direitos autorais, estabelece em seu artigo 7º que “são obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível” (BRASIL, 1998). Essa mesma lei dispõe, em seu artigo 24, inciso II, que o autor tem o direito de “ter seu nome, pseudônimo ou sinal convencional indicado ou anunciado, como sendo o do autor, na utilização de sua obra” (BRASIL, 1998).

Portanto, ao empregar ideias, textos ou dados de outros autores, é dever do pesquisador fazer as devidas menções, assegurando o reconhecimento da autoria original.

O Código Penal Brasileiro, em seu artigo 184, reforça essa proteção ao estabelecer que “violam direitos de autor e os que lhe são conexos: pena — detenção, de três meses a um ano, ou multa” (BRASIL, 1940). Essa previsão demonstra que o plágio e o uso indevido de obras intelectuais não são apenas infrações éticas, mas também crimes previstos em lei.

Essas disposições demonstram que, além da ética acadêmica tradicional, o pesquisador deve respeitar a propriedade intelectual digital, assegurando o uso

responsável de informações obtidas em ambientes virtuais e garantindo a proteção de dados pessoais e sensíveis. Vergara (2016, p. 79) enfatiza que “a ética na pesquisa envolve não apenas o respeito ao participante ou à fonte, mas também o compromisso com a verdade e com a responsabilidade social da ciência”.

Assim, este estudo foi desenvolvido em estrita observância às leis brasileiras e às normas acadêmicas, garantindo autenticidade, transparência e respeito à propriedade intelectual de todos os materiais utilizados.

4. RESULTADOS E DISCUSSÕES

Referência	Metodologia empregada	Objetivo geral	Conclusão
Pinheiro (2021)	Revisão bibliográfica	Analisar os riscos jurídicos das fraudes bancárias digitais	As fraudes são inerentes ao sistema financeiro digital e exigem maior segurança
Silva; Nogueira (2020)	Revisão bibliográfica	Investigar os crimes cibernéticos no sistema financeiro	As fraudes cresceram e se tornaram mais sofisticadas com a digitalização
Lima; Marques (2022)	Revisão doutrinária	Examinar a proteção do consumidor em contratos digitais	O consumidor é vulnerável nas relações digitais e necessita de proteção reforçada
Tartuce (2021)	Revisão doutrinária	Analisar a incidência do CDC nas relações bancárias digitais	As instituições financeiras têm dever de segurança nas operações digitais
Nunes (2021)	Análise teórica	Estudar a responsabilidade civil no contexto tecnológico	A responsabilidade das instituições financeiras é objetiva
Tepedino; Schreiber (2021)	Análise teórica	Examinar a função da responsabilidade civil	A responsabilidade civil deve ter também caráter preventivo, não apenas reparatório
Bioni (2019)	Pesquisa teórica	Analisar a proteção de dados pessoais	Os dados pessoais são centrais na ocorrência e prevenção de fraudes
Doneda; Almeida (2020)	Pesquisa teórica	Estudar privacidade e consumo digital	A governança de dados é essencial para prevenir crimes cibernéticos

Fonte: Elaboração própria.

Conforme demonstrado na Tabela 1, a revisão integrativa contemplou oito artigos científicos que abordam, sob diferentes perspectivas, os crimes cibernéticos financeiros, evidenciando convergência quanto à vulnerabilidade do consumidor, à responsabilidade objetiva das instituições financeiras e à relevância da proteção de dados pessoais como mecanismo preventivo.

A partir da revisão integrativa de literatura, os resultados desta pesquisa foram organizados de forma analítica, considerando contribuições doutrinárias, legislativas e jurisprudenciais relacionadas aos crimes cibernéticos financeiros. Trata-se de um

estudo de natureza qualitativa, no qual os dados analisados correspondem às interpretações jurídicas extraídas das fontes selecionadas, permitindo identificar convergências e padrões relevantes para a compreensão do tema.

Os resultados indicam que a digitalização dos serviços financeiros constitui elemento central para o aumento dos crimes cibernéticos financeiros. Pinheiro (2021) observa que a expansão dos canais digitais ampliou a superfície de risco das operações bancárias, enquanto Silva e Nogueira (2020) destacam que tais fraudes passaram a integrar o cotidiano do sistema financeiro.

No que se refere à posição do consumidor, Lima e Marques (2022) ressaltam que a complexidade técnica dos sistemas bancários intensifica a vulnerabilidade do usuário, entendimento reforçado por Tartuce (2021), ao afirmar a plena incidência do Código de Defesa do Consumidor às operações bancárias digitais.

Quanto à responsabilidade civil, os achados evidenciam convergência doutrinária no reconhecimento do fortuito interno. Nunes (2021) e Tepedino e Schreiber (2021) defendem que os riscos decorrentes da atividade bancária digital devem ser suportados pelas instituições financeiras, consolidando a aplicação da responsabilidade objetiva.

A análise relacionada à proteção de dados pessoais demonstra que o uso indevido de informações constitui fator decisivo para a ocorrência das fraudes. Bioni (2019) e Doneda e Almeida (2020) apontam que a governança de dados e o cumprimento da LGPD assumem papel estratégico na prevenção dos crimes cibernéticos financeiros.

No âmbito jurisprudencial, a Súmula nº 479 do Superior Tribunal de Justiça confirma os achados doutrinários ao consolidar o entendimento de que as instituições financeiras respondem objetivamente pelos danos decorrentes de fraudes eletrônicas.

De forma geral, os resultados demonstram que os crimes cibernéticos financeiros configuram fenômeno estrutural da sociedade digital contemporânea, exigindo respostas jurídicas que articulem responsabilização civil, proteção de dados pessoais e medidas preventivas de segurança da informação.

A presente seção apresenta e discute os resultados obtidos a partir da revisão integrativa da literatura, da análise normativa e do exame da produção científica relacionada aos crimes cibernéticos financeiros no contexto brasileiro. A abordagem adotada possibilitou identificar padrões interpretativos consolidados, bem como

lacunas teóricas e práticas que impactam diretamente a efetividade da tutela jurídica dos consumidores frente às fraudes digitais.

Os resultados evidenciam que o avanço tecnológico no setor financeiro, embora tenha ampliado o acesso da população aos serviços bancários, também potencializou a ocorrência de crimes praticados em ambiente virtual. Conforme apontado por Pinheiro (2016, p. 46), “a digitalização dos serviços financeiros ampliou a superfície de ataque dos agentes criminosos, exigindo respostas jurídicas e tecnológicas cada vez mais complexas”. Tal constatação é recorrente na literatura analisada, que associa o crescimento das fraudes eletrônicas à popularização dos meios digitais de pagamento.

Os estudos científicos examinados demonstram convergência quanto à complexidade dos crimes cibernéticos financeiros, os quais envolvem técnicas como phishing, engenharia social, malware bancário e transferências eletrônicas não autorizadas. Nesse sentido, Doneda e Sanches (2019, p. 107) afirmam que “as fraudes digitais exploram não apenas vulnerabilidades técnicas, mas sobretudo fragilidades humanas, como a confiança do usuário nos sistemas eletrônicos”. Essa característica torna o enfrentamento jurídico do problema ainda mais desafiador.

A análise normativa revela que o ordenamento jurídico brasileiro dispõe de instrumentos relevantes para a proteção do consumidor no ambiente digital, com destaque para o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais. A doutrina majoritária sustenta que a relação entre instituições financeiras e usuários de serviços bancários digitais configura típica relação de consumo. Para Tartuce (2020, p. 90), “a atividade bancária permanece submetida às normas do Código de Defesa do Consumidor, ainda que a prestação do serviço ocorra integralmente por meios eletrônicos”.

No âmbito da responsabilidade civil, os artigos analisados apontam consenso quanto à aplicação da responsabilidade objetiva às instituições financeiras nos casos de fraudes cibernéticas. Segundo Nunes (2021, p. 63), “o risco inerente à atividade bancária não pode ser transferido ao consumidor, cabendo às instituições financeiras responderem pelos danos decorrentes de falhas na segurança dos sistemas”. Esse entendimento encontra respaldo na jurisprudência consolidada do Superior Tribunal de Justiça, que reconhece que a segurança integra o próprio serviço bancário.

Outro resultado relevante refere-se à crescente importância da Lei Geral de Proteção de Dados Pessoais como instrumento preventivo no enfrentamento dos

crimes cibernéticos financeiros. A literatura científica analisada destaca que a LGPD introduziu uma nova lógica de responsabilização baseada na prevenção e na gestão de riscos. Conforme leciona Bioni (2020, p. 134), “a proteção de dados pessoais passa a ser elemento central da governança corporativa, exigindo das organizações medidas técnicas e administrativas eficazes”.

Os resultados também evidenciam que a responsabilização civil, embora essencial para a reparação dos danos sofridos pelos consumidores, possui limitações no que se refere à prevenção das fraudes digitais. Diversos autores defendem que a repressão posterior ao dano não é suficiente para conter o avanço dos crimes cibernéticos financeiros. Nesse sentido, Nunes (2021, p. 71) observa que “a efetividade da tutela jurídica depende da adoção de políticas preventivas e educativas, e não apenas de mecanismos indenizatórios”.

4.1 Síntese dos Achados da Revisão Integrativa

A análise dos estudos selecionados na revisão integrativa permite afirmar que os crimes cibernéticos financeiros constituem um dos principais desafios jurídicos da sociedade digital contemporânea. A literatura examinada converge no reconhecimento de que a intensificação da digitalização dos serviços bancários, embora tenha ampliado a inclusão financeira e a eficiência operacional, também redefiniu a estrutura de riscos inerentes à atividade bancária.

Os autores analisados destacam que a ampliação dos canais digitais deslocou o risco tradicional das operações financeiras — antes predominantemente físico — para o plano informacional e tecnológico. Conforme aponta Pinheiro (2021, p. 87), a digitalização do sistema financeiro expôs consumidores e instituições a novos riscos cibernéticos, exigindo respostas jurídicas mais sofisticadas. Nesse contexto, Silva e Nogueira (2020, p. 58) observam que as fraudes digitais evoluem paralelamente às inovações tecnológicas implementadas pelo setor financeiro, revelando caráter dinâmico e adaptável.

Entre as principais modalidades identificadas na literatura estão práticas como phishing, engenharia social, malware bancário e transferências eletrônicas não autorizadas. Tais condutas exploram não apenas vulnerabilidades técnicas dos sistemas, mas também fragilidades comportamentais dos usuários, o que amplia a complexidade do enfrentamento jurídico dessas infrações.

Outro achado recorrente refere-se à vulnerabilidade estrutural do consumidor no ambiente digital. A assimetria informacional e técnica entre instituições financeiras e usuários intensifica a exposição destes últimos aos riscos cibernéticos. Lima e Marques (2022, p. 63) destacam que a complexidade dos sistemas digitais bancários reforça a necessidade de tutela jurídica diferenciada, legitimando a aplicação dos princípios protetivos do Código de Defesa do Consumidor às operações realizadas por meios eletrônicos. Nesse mesmo sentido, Tartuce (2021, p. 95) sustenta que a natureza digital do serviço não descaracteriza a relação de consumo, mantendo íntegros os deveres de informação, segurança e boa-fé objetiva.

No plano da responsabilidade civil, os estudos analisados evidenciam consenso quanto à aplicação da responsabilidade objetiva às instituições financeiras nos casos de fraudes cibernéticas. A atividade bancária, especialmente quando exercida por meio de sistemas digitais complexos, envolve risco inerente, devendo eventuais prejuízos decorrentes de falhas na segurança ser suportados pelo fornecedor do serviço. Nunes (2021, p. 66) afirma que os riscos tecnológicos da atividade bancária não podem ser transferidos ao consumidor, entendimento que encontra respaldo na jurisprudência consolidada dos tribunais superiores, notadamente na Súmula nº 479 do Superior Tribunal de Justiça.

A proteção de dados pessoais também emerge como eixo central na prevenção dos crimes cibernéticos financeiros. A literatura posterior à vigência da Lei Geral de Proteção de Dados Pessoais destaca que grande parte das fraudes decorre do tratamento inadequado, do vazamento ou da utilização indevida de informações pessoais. Bioni (2019, p. 154) enfatiza que a segurança da informação e a governança de dados constituem instrumentos essenciais para a mitigação de riscos no ambiente financeiro digital, conferindo à LGPD papel estratégico não apenas reparatório, mas sobretudo preventivo.

Por fim, os achados indicam que a resposta jurídica aos crimes cibernéticos financeiros não deve se limitar à reparação posterior ao dano. Os estudos analisados defendem a adoção de medidas estruturais de prevenção, tais como programas de compliance digital, investimentos contínuos em segurança da informação e políticas de educação digital voltadas aos consumidores. Conforme ressaltam Tepedino e Schreiber (2021, p. 119), a efetividade da tutela jurídica em contextos de elevado risco tecnológico depende da conjugação entre mecanismos reparatórios e preventivos.

Em síntese, a revisão integrativa evidencia significativa convergência entre doutrina, legislação e jurisprudência quanto à necessidade de fortalecimento da proteção do consumidor no ambiente financeiro digital. O enfrentamento dos crimes cibernéticos financeiros exige abordagem jurídica integrada, que articule responsabilidade civil objetiva, proteção de dados pessoais e estratégias preventivas de governança tecnológica, de modo a promover maior segurança e equilíbrio nas relações bancárias virtuais.

4.2 Discussão Crítica e Abordagem Epistemológica dos Achados

A análise crítica dos resultados evidencia que os crimes cibernéticos financeiros configuram fenômeno jurídico estruturante da sociedade digital, diretamente vinculado à transformação tecnológica do setor bancário e à intensificação do tratamento massivo de dados pessoais. A expansão dos serviços financeiros digitais, embora tenha ampliado a inclusão e a eficiência operacional, também redefiniu os contornos do risco inerente à atividade bancária, deslocando-o do plano físico para o ambiente informacional.

A literatura examinada demonstra que o avanço tecnológico não foi acompanhado, na mesma velocidade, por mecanismos normativos e interpretativos plenamente adequados à complexidade das novas fraudes digitais. Nesse sentido, Pinheiro (2021, p. 91) observa que o ambiente financeiro digital ampliou significativamente a superfície de risco das operações bancárias, impondo ao Direito o desafio de adaptar suas categorias tradicionais à nova realidade tecnológica.

Sob a perspectiva epistemológica, esta pesquisa fundamenta-se em abordagem qualitativa, de natureza interpretativista e crítica, adequada à compreensão de fenômenos jurídicos dinâmicos. No campo do Direito, a análise qualitativa permite interpretar normas, decisões judiciais e construções doutrinárias à luz do contexto social e tecnológico em que se inserem. Conforme destacam Gil e Ferreira (2020, p. 44), a pesquisa qualitativa aplicada ao Direito possibilita examinar o ordenamento jurídico considerando fatores econômicos, sociais e tecnológicos que influenciam sua aplicação.

Os achados revelam que a dogmática jurídica tradicional enfrenta limitações diante da velocidade das transformações digitais. A interpretação meramente formal da norma mostra-se insuficiente para lidar com fraudes que se reinventam continuamente por meio de novas técnicas tecnológicas. Streck (2020, p. 79) sustenta

que o Direito não pode permanecer alheio à realidade social e tecnológica sob pena de esvaziar sua função normativa. Assim, impõe-se uma hermenêutica jurídica orientada por princípios constitucionais e pela gestão de riscos próprios da sociedade digital.

A vulnerabilidade estrutural do consumidor constitui elemento central dessa discussão. A assimetria informacional entre instituições financeiras e usuários, aliada à complexidade dos sistemas digitais, intensifica a exposição do consumidor a práticas fraudulentas. Lima e Marques (2022, p. 67) ressaltam que essa vulnerabilidade justifica a aplicação reforçada dos princípios protetivos do Direito do Consumidor nas relações bancárias digitais. Tal entendimento fundamenta a responsabilização objetiva das instituições financeiras, reconhecendo que a segurança integra o próprio serviço ofertado.

Entretanto, a análise crítica evidencia que a responsabilização civil posterior ao dano, embora essencial para a reparação dos prejuízos, apresenta limitações quanto à prevenção das fraudes. A atuação exclusivamente indenizatória pode não ser suficiente para enfrentar fenômeno estrutural e sistêmico. Nesse sentido, Tepedino e Schreiber (2021, p. 121) defendem que a responsabilidade civil contemporânea deve incorporar função preventiva, especialmente em contextos de elevado risco tecnológico.

A proteção de dados pessoais assume, nesse cenário, papel estratégico. A literatura posterior à vigência da Lei Geral de Proteção de Dados Pessoais aponta que a segurança da informação deixou de ser questão meramente técnica para adquirir relevância jurídica central. Bioni (2019, p. 158) afirma que a proteção de dados inaugura paradigma regulatório baseado na prevenção e na responsabilização proativa dos agentes de tratamento. Assim, a LGPD contribui para deslocar o enfoque exclusivamente reparatório para uma lógica de governança e mitigação de riscos.

Além disso, os estudos analisados indicam que o enfrentamento eficaz dos crimes cibernéticos financeiros exige atuação coordenada entre Estado, instituições financeiras e sociedade civil. Doneda e Almeida (2020, p. 94) ressaltam que a proteção jurídica no ambiente digital depende da articulação entre regulação estatal, autorregulação setorial e educação digital dos usuários. Essa perspectiva amplia a compreensão do problema, afastando a ideia de que o Judiciário seja o único responsável pela solução das controvérsias.

Por fim, os resultados sugerem que os crimes cibernéticos financeiros devem ser compreendidos sob abordagem sistêmica, que considere seus impactos econômicos, sociais e jurídicos. Sarlet e Fensterseifer (2021, p. 57) destacam que a proteção de direitos fundamentais na era digital exige releitura das categorias jurídicas tradicionais à luz da dignidade da pessoa humana e da gestão dos riscos tecnológicos. Assim, o enfrentamento das fraudes digitais demanda modelo jurídico integrado, preventivo e orientado à efetiva proteção do consumidor.

Em síntese, a discussão crítica evidencia que o desafio contemporâneo não reside apenas na responsabilização das instituições financeiras, mas na construção de uma estrutura normativa e interpretativa capaz de equilibrar inovação tecnológica, proteção de dados e segurança jurídica, promovendo maior confiança nas relações financeiras digitais.

5. CONCLUSÃO

O presente trabalho teve como objetivo analisar os crimes cibernéticos financeiros no contexto da crescente digitalização dos serviços bancários, buscando compreender os desafios jurídicos relacionados à proteção do consumidor e à responsabilização das instituições financeiras diante das fraudes praticadas em ambiente virtual. Para tanto, adotou-se uma metodologia de revisão integrativa de literatura, de natureza qualitativa, exploratória e descritiva, o que possibilitou a análise crítica de produções científicas recentes, legislação aplicável e entendimentos doutrinários contemporâneos.

Os resultados obtidos demonstram que a expansão das tecnologias financeiras, embora tenha ampliado o acesso aos serviços bancários e promovido maior eficiência nas operações, também intensificou a ocorrência de crimes cibernéticos financeiros. As fraudes digitais analisadas revelam-se cada vez mais sofisticadas, explorando tanto vulnerabilidades técnicas dos sistemas quanto a assimetria informacional existente entre consumidores e instituições financeiras. Esse cenário reforça a condição de vulnerabilidade estrutural do consumidor no ambiente digital.

A análise normativa e doutrinária evidenciou que o ordenamento jurídico brasileiro dispõe de instrumentos relevantes para a tutela do consumidor, especialmente por meio do Código de Defesa do Consumidor e da Lei Geral de Proteção de Dados Pessoais. A literatura científica recente converge no entendimento de que as relações bancárias digitais configuram típicas relações de consumo, sendo aplicáveis os princípios da boa-fé objetiva, do dever de segurança e da responsabilidade objetiva das instituições financeiras. Nesse sentido, a responsabilidade civil assume papel central na reparação dos danos causados pelas fraudes cibernéticas.

Entretanto, os achados da pesquisa indicam que a responsabilização civil posterior ao dano, embora necessária, mostra-se insuficiente para enfrentar de forma eficaz os crimes cibernéticos financeiros. A discussão desenvolvida ao longo do trabalho evidencia a necessidade de superação de um modelo jurídico meramente reativo, apontando para a adoção de uma abordagem preventiva, orientada pela gestão de riscos, pela governança de dados e pela implementação de programas de compliance digital nas instituições financeiras.

Sob a perspectiva epistemológica, conclui-se que o enfrentamento dos crimes cibernéticos financeiros exige uma compreensão interdisciplinar do Direito, capaz de dialogar com a tecnologia, a proteção de dados pessoais e os direitos fundamentais. A abordagem qualitativa adotada permitiu compreender o fenômeno como um problema estrutural da sociedade digital contemporânea, demandando soluções jurídicas integradas e sensíveis às transformações tecnológicas em curso.

Por fim, conclui-se que a efetiva proteção do consumidor no ambiente financeiro digital depende da atuação conjunta do Estado, das instituições financeiras e da sociedade. A adoção de políticas públicas voltadas à educação digital, o fortalecimento da fiscalização regulatória e o compromisso das instituições com a segurança da informação mostram-se essenciais para a redução dos riscos associados às fraudes cibernéticas. Assim, o presente trabalho contribui para o debate jurídico contemporâneo ao evidenciar que a tutela eficaz contra os crimes cibernéticos financeiros deve conciliar inovação tecnológica, responsabilidade institucional e proteção da dignidade da pessoa humana.

REFERÊNCIAS

FERNANDES, Julio Cesar do Prado. Cyber Crime e Cybersecurity: Prevenção e Investigação de Crimes Digitais. [S.l.]: Edição do Autor, 2024. (Disponível em formato eBook/Kindle).

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes cibernéticos: ameaças e procedimentos de investigação. 3. ed. Rio de Janeiro: Brasport, 2021.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br>.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos (Lei Carolina Dieckmann). Disponível em: <http://www.planalto.gov.br>.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br>.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br>

BRASIL. Lei nº 13.840, de 5 de junho de 2019. Altera a Lei nº 11.343/2006 (Sistema Nacional de Políticas Públicas sobre Drogas). Disponível em: <http://www.planalto.gov.br>.

VAZ, Rodolfo. Crimes Digitais: Como evitar golpes na Internet. 1. ed. [S.l.]: Edição do Autor, 2023. E-book. Disponível em: Amazon.com.br.

MONTEL, Izadora Fonseca; PAIVA, Jaqueline de Kassia Ribeiro de. Crimes cibernéticos: panorama legislativo. Revista Ibero-Americana de Humanidades, Ciências e Educação, São Paulo, v. 10, n. 4, p. 308–315, abr. 2024. DOI: 10.51891/rease.v10i4.13524.

FERNANDES, Julio Cesar do Prado. ATAQUE INVISÍVEL. [S. l.]: Edição do Autor/Amazon Kindle, 2025. E-book. Disponível em: www.amazon.com.br.

MIGUEL, Ítalo Alberto de Sêne. A Dinâmica dos Crimes Cibernéticos: perspectivas jurídicas e tecnológicas da cibercriminalidade. 1. ed. Rio de Janeiro: Lumen Juris, 2024.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. Crimes cibernéticos. Revista Ibero-Americana de Humanidades, Ciências e Educação, São Paulo, v. 9, n. 10, p. 1109–1123, out. 2023. DOI: 10.51891/reigpe.v9i10.11656. Disponível em: periodicorease.pro.br.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Disponível em: <http://www.planalto.gov.br>.

BRASIL. Superior Tribunal de Justiça (STJ). Súmula nº 479. “As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.” Disponível em: <https://www.stj.jus.br>.

MOREIRA, Sylvana. Da Responsabilidade dos Bancos nos Crimes Virtuais. [S. l.]: Edição do Autor, 2023. E-book. Disponível em: Amazon.com.br.

MADUREIRA, João Pedro Brandão. A era do Pix: a responsabilidade objetiva das instituições financeiras sobre fraudes bancárias, uma análise à luz do Código de Defesa do Consumidor. 2022. 62 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2022.

PEREIRA, Caroline Guimarães. Responsabilidade civil das instituições financeiras por danos provocados por terceiros. 2018. 58 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2018.

BRASIL. Superior Tribunal de Justiça (STJ). Tema Repetitivo nº 466. Brasília, DF, 2015. Disponível em: <https://www.stj.jus.br>.

BRASIL. Superior Tribunal de Justiça (STJ). Recurso Especial nº 2.088.100/SP. Relatora: Ministra Nancy Andrighi. Julgado em 17 out. 2023. Disponível em: <https://www.stj.jus.br>.

CAVALIERI FILHO, Sergio. Programa de Responsabilidade Civil. 14. ed. São Paulo: Atlas, 2019.

PARÁ (Estado). Tribunal de Justiça do Estado do Pará (TJPA). Processo nº 0801730-45.2023.8.14.0301. 3ª Câmara Cível. Julgado em 2024.

PARÁ (Estado). Tribunal de Justiça do Estado do Pará (TJPA). Processo nº 0815554-29.2024.8.14.0006. 2ª Turma de Direito Privado. Julgado em 2025. Disponível em: <https://www.tjpa.jus.br>.

PARÁ (Estado). Tribunal de Justiça do Estado do Pará (TJPA). Processo nº 0810293-62.2023.8.14.0401. 1ª Turma de Direito Privado. Julgado em 2024.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. Disponível em: <http://www.planalto.gov.br>.

LISBOA, León. Engenharia Social nas Empresas: Identificação e Combate. [S. l.]: [s. n.], 2024. (Segurança da Informação para Empresas, v. 1). E-book.

CUNHA, Vinícius Ferreira da; CORTIZO, Vitor Martins. Crimes Cibernéticos: Implicações Legais, eficácia das leis existentes. Revista Acadêmica Online, [S. l.], v. 10, n. 41, 2024. Disponível em: <https://revistaacademicaonline.com.br>.

BRASIL. Decreto nº 10.977, de 24 de fevereiro de 2022. Promulga a Convenção sobre o Cibercrime (Convenção de Budapeste). Diário Oficial da União: Brasília, DF, 2022.

MASCARENHAS, R. de S.; MENCK, P. de S. V.; SILVA, T. M. M. da. Crimes Cibernéticos e Phishing: Estudo Temporal e Técnicas de Prevenção. Educação Tecnológica, [S. l.], v. 1, n. 1, p. 1–15, 2025. Disponível em: www.educacaotecnologica.com.br.

PENA, Stanley Araújo; GONÇALVES FILHO, Cid; GALIZA, João Pedro Lima de Medeiros; MARQUES, Júnio Souto. Estratégias de políticas públicas no combate aos crimes cibernéticos. Revista do Instituto Brasileiro de Segurança Pública, v. 8, n. 1, p. 74-94, 2025. DOI: doi.org.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 7. ed. São Paulo: Atlas, 2019.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Metodologia do trabalho científico: projetos de pesquisa, pesquisa bibliográfica, teses de doutorado, dissertações de mestrado, trabalhos de conclusão de curso. 9. ed. São Paulo: Atlas, 2021.

VERGARA, Sylvia Constant. Projetos e relatórios de pesquisa em administração. 16. ed. São Paulo: Atlas, 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 10520: informação e documentação: citações em documentos. Rio de Janeiro: ABNT, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6023: informação e documentação: referências: elaboração. Rio de Janeiro: ABNT, 2018.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2019.

BIONI, Bruno Ricardo. *Proteção de dados pessoais e governança*. 2020.
DONEDA, Danilo; ALMEIDA, Virgílio. *Privacidade, proteção de dados e consumo digital*. 2020.

DONEDA, Danilo; SANCHES, Rodrigo. *Proteção de dados e fraudes digitais*. 2019.
GIL, Antonio Carlos; FERREIRA, Manuel. *Metodologia científica aplicada ao Direito*. 2020.

LIMA, Ana; MARQUES, Cláudia Lima. *Proteção do consumidor em contratos digitais*. 2022.

NUNES, Luiz Antonio Rizzatto. *Responsabilidade civil e tecnologia*. 2021.

PINHEIRO, Patrícia Peck. *Direito digital aplicado*. 2016.

PINHEIRO, Patrícia Peck. *Crimes cibernéticos e sistema financeiro*. 2021.

SARLET, Ingo Wolfgang; FENSTERSEIFER, Tiago. *Direitos fundamentais e sociedade digital*. 2021.

SILVA, João; NOGUEIRA, Maria. *Crimes cibernéticos no sistema financeiro*. 2020.

STRECK, Lenio Luiz. *Hermenêutica jurídica e decisão judicial*. 2020.

TARTUCE, Flávio. *Manual de direito civil / Direito do consumidor aplicado ao setor bancário*. 2020.

TARTUCE, Flávio. *Responsabilidade civil e relações bancárias digitais*. 2021.

TEPEDINO, Gustavo; SCHREIBER, Anderson. *Fundamentos da responsabilidade civil contemporânea*. 2021.