UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL
CURSO DE DIREITO – CPTL

JHÔNATAS GABRIEL ATAÍDE DE SOUZA

CRIMES FINANCEIROS NA ERA DIGITAL: A EVOLUÇÃO DOS MÉTODOS DOS CIBERCRIMES

TRÊS LAGOAS-MS
2025

JHÔNATAS GABRIEL ATAÍDE DE SOUZA

CRIMES FINANCEIROS NA ERA DIGITAL: A EVOLUÇÃO DOS MÉTODOS DOS CIBERCRIMES

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Direito do Campus de Três Lagoas da Universidade Federal de Mato Grosso do Sul, como requisito parcial para obtenção do grau de Bacharel em Direito, sob orientação do Professor Dr. Carlos Eduardo Pereira Furlani.

TRÊS LAGOAS-MS
2025

JHÔNATAS GABRIEL ATAÍDE DE SOUZA

CRIMES FINANCEIROS NA ERA DIGITAL: A EVOLUÇÃO DOS MÉTODOS DOS CIBERCRIMES

Este Trabalho de Conclusão de Curso foi avaliado e julgado _____ em sua forma final, como requisito parcial para obtenção do grau de Bacharel em Direito, perante Banca Examinadora constituída pelo Colegiado do Curso de Graduação em Direito do Campus de Três Lagoas da Universidade Federal de Mato Grosso do Sul, composta pelos seguintes membros: Professor Doutor Carlos Eduardo Furlani UFMS/CPTL – Orientador, Professor Doutor Marçal Rogério Rizzo UFMS/CPTL – Membro e Professor Doutor Adailson da Silva Moreira UFMS/CPTL – Membro.

Dr. Carlos Eduardo Pereira Furlani
UFMS/CPTL – Orientador

Dr. Marçal Rogério Rizzo
UFMS/CPTL – Membro

Dr. Adailson da Silva Moreira
UFMS/CPTL - Membro

TRÊS LAGOAS-MS
2025

DEDICATÓRIA

A quem segura minha mão quando o caminho se torna incerto, sustenta meu coração quando o cansaço se aproxima e ilumina meus passos mesmo nas noites mais escuras — dedico a realização deste sonho. Dedico este trabalho à minha família, razão da minha existência, origem da minha fé e porto seguro.

Aos meus amados pais, Enio e Luzia, que me ensinaram que o verdadeiro valor de um homem está na honestidade, na humildade e na persistência diante da adversidade. Tudo o que sou nasceu da força e do exemplo de vocês. Obrigado por cada incentivo, por cada oração e por nunca permitirem que eu desistisse, mesmo quando o cansaço tentava me calar. Vocês me ensinaram que sonhar é preciso — mas lutar, mesmo cansado, é o que nos torna vitoriosos.

À minha esposa e grande amor, Ariane, que caminhou comigo lado a lado nessa longa jornada, você foi a calmaria no meio da tempestade e o sorriso que reacendia minha fé nos dias mais longos. Seu amor foi abrigo, sua paciência foi bálsamo, e sua presença foi luz. Obrigado por acreditar em mim quando eu mesmo duvidava. Esta vitória é nossa — conquistada entre lágrimas, muito café e esperança.

Aos meus filhos, Valentim e Nicolas, meus tesouros e razões de continuar. Cada passo que dei foi pensando em vocês. Que este marco em minha vida lhes mostre que nenhum sonho é inalcançável quando se tem propósito, disciplina e fé. Que aprendam com meu esforço que desistir nunca é opção para quem conhece o valor do que sonha. Vocês são, e sempre serão, um motivo de orgulho e felicidade para mim.

Aos meus amigos de jornada — Bruno, Felipe, Anderson, Ediego, Lauro, Jackson e Alexandre —, companheiros de luta e de risadas, de noites de estudo e dias de incerteza. Cada conversa, cada palavra de apoio, cada momento de descontração foi combustível nesta caminhada. Obrigado por me lembrarem que a amizade verdadeira é também uma forma de coragem, e que os sonhos se tornam mais leves quando compartilhados com pessoas que acreditam junto com você.

Aos professores e colaboradores da UFMS – Campus de Três Lagoas, minha eterna gratidão. Obrigado por conduzirem com sabedoria, paciência e paixão o processo que me transformou. Cada ensinamento transmitido foi uma semente de justiça e conhecimento plantada em mim, e dela brotará o compromisso de fazer a diferença no mundo.

Esta trajetória me ensinou que o sucesso não está apenas na conquista, mas na resiliência de permanecer em pé quando tudo parece desabar. Por isso, a cada obstáculo vencido, reafirmo: vale a pena lutar, vale a pena continuar, vale a pena acreditar.

A todos que, de alguma forma, me estenderam a mão, me ofereceram uma palavra, um olhar, uma prece — o meu mais sincero e eterno agradecimento.

Jhônatas Gabriel Ataíde de Souza

CRIMES FINANCEIROS NA ERA DIGITAL: A EVOLUÇÃO DOS MÉTODOS DOS CIBERCRIMES

Jhônatas Gabriel Ataíde de Souza[1]

RESUMO

Os crimes financeiros cometido por meios digitais tornaram-se uma preocupação global, refletindo o impacto da transformação tecnológica sobre o sistema financeiro. Esses delitos abrangem práticas como fraudes eletrônicas, lavagem de dinheiro, phishing, ransomware, clonagem de cartões e manipulação de ativos virtuais. Este artigo objetiva demonstrar a evolução desses delitos e as repostas legislativas que visam combater essas condutas danosas.

Palavras-chave: Cibercrime. Finanças. Tecnologia. Fraudes.

ABSTRACT

Financial crimes committed through digital means have become a global concern, reflecting the impact of technological transformation on the financial system. These crimes include practices such as electronic fraud, money laundering, phishing, ransomware, card cloning, and virtual asset manipulation. This article aims to demonstrate the evolution of these crimes and the legislative responses aimed at combating these harmful behaviors.

Keywords: Cybercrime. Finance. Technology. Fraud.

SUMÁRIO

1 INTRODUÇÃO

A relevância dos crimes financeiros nesta era digital é indiscutível diante do aumento significativo da utilização de tecnologias e meios eletrônicos para transacionar no mercado financeiro, e os criminosos têm se aproveitado deste fato para desenvolver métodos para cometer fraudes. Com o avanço da internet e a popularização das transações online, os criminosos encontraram novas formas de agir, explorando vulnerabilidades nos sistemas de segurança das instituições financeiras e dos usuários. Esse cenário evidencia a necessidade de estudos aprofundados sobre o tema, a fim de compreender as estratégias utilizadas pelos criminosos e desenvolver medidas eficazes de prevenção e combate. Tarcísio Teixeira traz um retrospecto valioso em seu livro “Direito Digital e Processo Eletrônico” sobre essa temática.

> O avanço e a popularização da internet, ao passo em que simultaneamente te ela fornece inúmeras facilidades aos usuários, torna-se a rede um grande atrativo aos criminosos. E, também, a partir da pulverização do comércio eletrônico, grandes quantias de dinheiro e informações circulam conjunta mente; criou-se assim um ambiente muito visado pelos delinquentes virtuais. Bem ponderou a professora Ivette Senise Ferreira que: “a informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo al cance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução”. Atualmente, algumas condutas praticadas pela internet são penalmente tidas por típicas, mas outras como atípicas. Ou seja, estas não seriam consideradas como crime, em face da rara legislação sobre condutas utilizando a informática, juntamente com o Princípio da Reserva Legal, que é um pilar do Direito Penal, em que não há crime nem pena se não houver prévia cominação legal. Esses crimes vêm sendo praticados de variadas formas, por exemplo, transações nos caixas de bancos, redes de telecomunicações, entre outras inúmeras peripécias realizadas por criminosos que atuam na rede, demonstrando assim a vulnerabilidade do sistema informático. O professor Ulrich Sieber, da Universidade de Wurzburg, afirma que essa espécie de criminalidade surgiu na década de 1960, quando se iniciaram na imprensa e na literatura científica os primeiros casos do uso do computador para a prática de delitos;

> constituída, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas. Mas somente na década seguinte iriam iniciar-se os estudos sistemáticos e científicos sobre o tema. A partir da década de 1980, com a evolução das técnicas e a expansão da informática, os crimes se diversificaram, passando a incidir em pirataria de programas, manipulações da rede bancária, entre outros. Isso demonstrou a fragilidade que os criadores desses processos não haviam previsto; e que seria necessária uma proteção com formas de controle de segurança eficientes, bem como de previsões criminais para as condutas delitivas. Um estudo da Norton divulgado no dia 20 de setembro de 2011 mostrou que 80% dos adultos no Brasil já foram vítimas de crimes na internet, sendo que 77.000 pessoas são vítimas de crimes cibernéticos por dia no país. No mundo, são 1 milhão de pessoas vitimadas por dia, em 24 países pesquisados, cujos prejuízos chegaram a US$ 388 bilhões em 2010. Com um prejuízo financeiro total para o país de US$ 10,3 bilhões, 42,4 milhões de brasileiros foram vítimas de crimes virtuais no ano de 2016. Um acréscimo de 10% em relação a 2015. Desse modo, em matéria de crimes cibernéticos, o Brasil é o 5º no ranking entre os países. Crimes como subtração de dados pessoais e fraudes de cartão de crédito são os principais delitos praticados por aqui. De acordo com Safernet Brasil, em 11 anos ela recebeu 3,6 milhões de denúncias anônimas envolvendo a prática delitiva no Brasil. (Teixeira, 2025, p. 592)

Os impactos econômicos e sociais causados pelos crimes financeiros na era digital são alarmantes, uma vez que as fraudes afetam não apenas empresas e governos, mas também indivíduos que têm suas informações pessoais e financeiras comprometidas. Os prejuízos decorrentes dessas práticas fraudulentas podem ser devastadores, resultando em perdas financeiras expressivas, danos à reputação das organizações e desconfiança por parte da sociedade em relação aos meios eletrônicos de pagamento. Veja a os dados do Banco Central noticiados pelo Jornal Poder360 em 25/04/2025:

> O BC (Banco Central) registrou 4,7 milhões de fraudes envolvendo Pix em 2024. O prejuízo total chegou a R$ 6,5 bilhões, segundo dados divulgados pela Folha de S.Paulo na 5ª feira (24.abr.2025). Em relação a 2023, quando foram registrados 2,6 milhões de casos, o número de fraudes aumentou cerca de 80%. Do valor total, apenas R$ 459 milhões retornaram às vítimas, o que corresponde a 7% do montante movimentado em golpes. (Poder360, 2025)

A complexidade das investigações e processos judiciais envolvendo crimes financeiros praticados por meios cibernéticos é um desafio constante para as autoridades responsáveis pela aplicação da lei. A rapidez e sofisticação dos métodos utilizados pelos criminosos dificultam a identificação dos responsáveis e a coleta de provas robustas para embasar as acusações. Além disso, a transnacionalidade desses crimes torna ainda mais complexa a cooperação entre os órgãos de segurança pública de diferentes países, haja vista que muitos desses criminosos usam VPNs para mascarar o local e as máquinas utilizadas para os delitos.

A importância da prevenção e combate aos cibercrimimes financeiros é crucial para garantir a segurança das transações online e proteger os dados sensíveis dos usuários. Nesse sentido, políticas públicas eficazes que promovam a colaboração entre os setores público e privado são essenciais para mitigar os riscos associados às fraudes cibernéticas. A cooperação internacional também se mostra imprescindível diante da natureza globalizada desses crimes.

As lacunas legais existentes no que tange aos delitos ligados aos meios virtuais representam um grande obstáculo para as autoridades responsáveis pela aplicação da lei. A constante evolução tecnológica exige uma legislação ágil e adaptável às novas modalidades de crime, o que nem sempre é possível dada a morosidade do processo legislativo. As lacunas legais abrem brechas para que os criminosos explorem falhas no sistema jurídico em benefício próprio.

As principais tendências e desafios futuros relacionados a esses crimes apontam para o uso crescente de criptomoedas e inteligência artificial pelos criminosos. A anonimidade proporcionada pelas criptomoedas dificulta a rastreabilidade das transações fraudulentas, enquanto o uso da inteligência artificial possibilita o desenvolvimento de ataques cada vez mais sofisticados. Diante desse cenário, é fundamental que as autoridades estejam preparadas para lidar com essas novas ameaças.

> A criptomoeda representa uma alternativa aos bancos, pois o controle está nas mãos das pessoas-parte da transação, o que significa que não necessita de um terceiro envolvido, ou seja, as transações ocorrem sem intermediadores. Por não ter a necessidade do envolvimento de terceiros, tem-se uma maior facilidade de transferência, que ocorre em tempo real, além da garantia da privacidade e liberdade pessoal. A primeira criptomoeda que

> se tem notícia foi a Bit Gold que surgiu nos anos 90 com os cypherpunks, um grupo de criptoanarquistas, que, usando a criptografia, desenvolveram as criptomoedas. Satoshi Nakamo-to foi o criador do Bitcoin, que ganhou força após a crise financeira de 2008, onde as pessoas estavam cansadas de um intermediador em suas transações financeiras, ou seja, dos bancos. (Cury, 2020, p. 109)

importância da conscientização da população sobre os riscos inerentes ao uso das transações online, uma vez que a proteção dos dados pessoais e financeiros dos indivíduos depende em grande parte do seu próprio conhecimento sobre as práticas seguras na internet. Educar os usuários sobre como identificar possíveis golpes online, proteger suas informações sensíveis e adotar medidas preventivas é essencial para reduzir a incidência de fraudes cibernéticas. A conscientização pública também contribui para criar uma cultura de segurança digital mais sólida e resiliente frente às ameaças virtuais.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Conceito de Crime Financeiro na Era Digital

Crimes financeiros cometidos por meios eletrônicos/digitais representam práticas ilícitas que utilizam-se da tecnologia e sistemas eletrônicos para fraudar, roubar ou manipular recursos financeiros de indivíduos e empresas. Esses crimes têm crescido significativamente com o avanço da digitalização dos serviços bancários e a dependência da internet para transações financeiras. Entre os métodos criminosos mais comuns, destacam-se o *phishing*, no qual os agentes enviam sistematicamente mensagens falsas para obter dados confidenciais, como senhas e informações bancárias, e o *ransomware*, que se caracteriza pelo sequestro de dados da vítima por meio de criptografia, exigindo resgate em moedas digitais como o Bitcoin.

A evolução dos tempos levou-nos à era cibernética, com todas as vantagens e desvantagens que essa evolução tecnológica pode proporcionar. Tem havido, em todo o mundo, a criação de novos crimes cibernéticos, decorrentes da necessidade de ordenar, disciplinar e limitar o uso indevido da moderna e avançada tecnologia cibernética. (BITENCOURT, 2025)

Outros delitos frequentes incluem a clonagem de cartões de crédito, a falsificação de boletos bancários e fraudes em transações instantâneas, como as

realizadas via PIX. Golpistas também criam sites falsos de e-commerce e leilões online para atrair vítimas com ofertas atraentes, desviando pagamentos para contas fraudulentas. Esses crimes exploram tanto vulnerabilidades tecnológicas quanto a ingenuidade ou falta de atenção dos usuários, utilizando técnicas de engenharia social para enganar as vítimas.

O crime de estelionato digital, previsto no § 2º-A do artigo 171 do Código Penal Brasileiro, destaca-se como uma das principais ameaças no ambiente digital contemporâneo. Esse delito, introduzido pela Lei nº 14.155/2021, ocorre quando a fraude é praticada por meio de dispositivos eletrônicos, como computadores ou smartphones, para obter vantagem ilícita em prejuízo de terceiros. Uma característica marcante desse crime é o uso de engenharia social, uma técnica que explora vulnerabilidades humanas, como confiança, descuido ou falta de conhecimento sobre segurança digital, para manipular vítimas e obter informações sensíveis, como senhas, dados bancários ou transferências financeiras. Para uma correta compreensão dessa tipificação, vejamos a excelente lição que o professor Bitencourt nos dá, a respeito da evolução histórica dessa prática denominada de estelionato:

> O antigo direito romano desconhecia o crime hoje denominado estelionato. Era integrado ao dolus malus que, juntamente com a fraus e o metus, constituía crime privado, produto de criação pretoriana. Na Grécia antiga a fraude era severamente reprimida.No tempo do império (século II d. C.) aparece uma figura genérica do stelionatus (de stellio, que significa camaleão), uma espécie de crime extraordinário, que abrangeria todos os casos em que coubesse a actio doli, e que não se adequassem a qualquer outro crime contra o patrimônio. O Código Penal francês de 1810 incriminava a obtenção ou tentativa de obtenção de vantagem patrimonial, por meio de manobras fraudulentas (art. 405). O estelionato recebeu nomes diversificados nos mais diversos países, embora em todos eles a manobra fraudulenta tenha sido a nota característica comum; na Itália recebeu as denominações frode (Código toscano) e truffa (Códigos Zanardelli e Rocco); na Espanha, estafa; em Portugal, burla; na Alemanha, Betrug (engano).Nas Ordenações Filipinas, o estelionato denominou-se “burla” ou “inliço” (Livro V, Título 665), e lhe era cominada a pena de morte quando o prejuízo fosse superior a vinte mil-réis.O Código Criminal do Império (1830) adotou o nomen juris “este-lionato”, prevendo várias figuras, além da seguinte descrição genérica: “todo e qualquer artifício fraudulento, pelo qual se obtenha de outrem toda a sua fortuna ou parte dela, ou quaisquer títulos”. O Código Penal republicano (1890) seguiu a mesma orientação casuística, tipificando onze figuras de

> estelionato, incluindo uma modalidade genérica, nos seguintes termos: “usar de artifício para surpreender a boa-fé de outrem, iludir a sua vigilância, ou ganhar-lhe a confiança; induzindo-o em erro ou engano por esses e outros meios astuciosos, procurar para si lucro ou proveito”. (Bitencourt, 2025, p. 284)

As autoridades enfrentam diversas dificuldades na investigação e combate aos crimes financeiros cometidos virtualmente, em parte devido à complexidade das transações online e à dificuldade de rastreamento. A natureza globalizada da internet torna mais difícil identificar os responsáveis por esses delitos, uma vez que muitos criminosos atuam em países diferentes do local onde são cometidos os crimes. Além disso, a utilização de criptomoedas e outras tecnologias que garantem o anonimato dificulta ainda mais o trabalho das autoridades (FARINHA, 2021).

2.2 Evolução dos Crimes Financeiros

A evolução dos delitos financeiros impetrados digitalmente reflete a constante adaptação dos criminosos às novas tecnologias e às mudanças nos hábitos das pessoas e empresas. Inicialmente, essas práticas limitavam-se a ações como a clonagem de cartões ou transferências bancárias não autorizadas. Contudo, com a ampliação do acesso à internet e o surgimento da IA e dos ativos digitais, os golpes se tornaram mais sofisticados e elaborados. Atualmente, práticas como *phishing*, *ransomware*, falsos leilões e fraudes em plataformas digitais estão entre as mais comuns, explorando lacunas na segurança tecnológica e na educação digital dos usuários. Podemos afirmar que o dinheiro no sentido de valor econômico está cada vez mais digitalizado, vejamos a lição de Rogério Cury expressada no seu livro de Direito Penal Econômico:

> O dinheiro, bem de expressão máxima da ideia de valor econômico, hodiernamente, como se sabe, circula em boa parte no chamado “mundo virtual” da informática. Esses valores recebidos e transferidos por meio da manipulação de dados digitais não são tangíveis, mas nem por isso deixaram de ser dinheiro. O bem, ainda que de forma virtual, circula como qualquer outra coisa, com valor econômico evidente. De fato, a informação digital e o bem material correspondente estão intrínseca e inseparavelmente ligados, se confundem. Esses registros contidos em banco de dados não possuem existência autônoma, desvinculada do bem que representam, por isso são passíveis de movimentação, com a troca de titularidade. (Cury, 2020, p. 108)

A pandemia de COVID-19 acelerou essa evolução. O isolamento social forçou a migração em massa para o ambiente digital, seja para trabalho remoto, transações financeiras ou consumo online. Nesse contexto pandêmico, o aumento drástico da dependência de tecnologias expôs indivíduos e empresas a novas vulnerabilidades. Criminosos passaram a aplicar golpes que exploravam a fragilidade emocional e a desinformação geradas pela crise.

Paralelamente, o lançamento de sistemas como o PIX criou novas oportunidades para os golpistas. Embora a ferramenta tenha modernizado e agilizado as transações financeiras, também facilitou a prática de crimes, como a clonagem de contas, transferências não autorizadas e golpes envolvendo falsas solicitações de pagamento. Uma técnica central nesse cenário é a engenharia social, que utiliza táticas de manipulação psicológica para enganar as vítimas.

Diante desse cenário, a resposta do poder público e das instituições financeiras evoluiu. No Brasil, a Lei nº 14.155/2021 passou a punir de forma mais severa os crimes de estelionato digital, aumentando as penas para fraudes realizadas por meios eletrônicos. Contudo, o fator humano permanece como a principal vulnerabilidade, uma vez que muitos usuários ainda desconhecem as práticas básicas de segurança digital. A pandemia evidenciou que a educação digital é tão importante quanto a tecnologia no combate aos crimes financeiros digitais.

2.3 Principais Tipos de Crimes Financeiros Digitais

Dentre os principais tipos de crimes financeiros que têm se destacado no ambiente digital, destacam-se o *phishing*, as fraudes em cartões de crédito e a lavagem de dinheiro virtual.

- **Phishing**: Consiste em enganar os usuários por meio de mensagens falsas ou sites fraudulentos para obter informações pessoais e financeiras. Os criminosos se passam por instituições legítimas para induzir as vítimas a fornecerem seus dados.
- **Malware Financeiro**: A utilização de *malware* é outra técnica comum. Cavalos de Troia (*Trojans*) e *ransomware* são frequentemente empregados para invadir sistemas, roubar informações ou extorquir dinheiro. *Ransomware* criptografa os arquivos da vítima e exige um resgate, geralmente em criptomoedas, para liberá-los.

- **Fraudes com Cartões (*Carding*)**: Esta prática envolve a compra e venda de informações de cartões de crédito roubados ou clonados no mercado ilegal. Os dados são obtidos por meio de ataques cibernéticos ou interceptação de transações e, em seguida, utilizados para realizar compras fraudulentas.
- **Lavagem de Dinheiro Virtual**: Refere-se à prática de ocultar a origem ilícita dos recursos por meio de transações eletrônicas, muitas vezes utilizando criptomoedas para dificultar o rastreamento (SILVA; AMARAL, 2024).

2.4 Legislação Brasileira e Impactos na Sociedade

A legislação brasileira tem evoluído para acompanhar a crescente prática de crimes financeiros no ambiente digital. O principal marco regulatório é o Código Penal, que, com a Lei nº 14.155/2021, passou a tratar diretamente do estelionato digital. Outros pilares da regulamentação são o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018) e a Lei Carolina Dieckmann (Lei nº 12.737/2012). Além disso, a Lei de Lavagem de Dinheiro (Lei nº 9.613/1998) é fundamental no combate à ocultação de bens de origem ilícita.

Os impactos desses crimes na sociedade são profundos. Eles minam a confiança da sociedade nas instituições financeiras, levando à desconfiança dos consumidores. A dificuldade de recuperação dos recursos perdidos gera prejuízos econômicos significativos para as vítimas e afeta a economia como um todo. Há também uma relação preocupante entre crimes financeiros e o aumento da desigualdade social, pois os mais vulneráveis são frequentemente as principais vítimas. Para mitigar esses efeitos, são essenciais o investimento em tecnologia de segurança cibernética e, crucialmente, a promoção da educação financeira e digital para a população (NETO, 2023).

2.5 Responsabilidade penal dos cibercrimes

A transposição das atividades criminosas para o ambiente digital impôs ao Direito Penal um de seus mais complexos desafios contemporâneos. A lógica territorial e os mecanismos probatórios tradicionais, pilares da persecução penal, mostram-se frequentemente inadequados para lidar com a fluidez, a

transnacionalidade e o pseudoanonimato que caracterizam a criminalidade informática. Como bem elucida Teixeira em sua obra dedicada ao tema:

> O combate à criminalidade informática encontra vários entraves relacionados às lacunas legislativas, mas não somente; também aos reflexos que podem causar restrição à liberdade de expressão e ao acelerado desenvolvimento tecnológico. Em boa medida, a internet permite o anonimato, o que dificulta a identificação do autor, haja vista a possibilidade de manipulação dos dados. O flagrante também é um problema, uma vez que é quase impossível de acontecer, pois, muitas vezes, o resultado do crime vem muito depois do início da execução, até porque a vítima muitas das vezes só conhece o prejuízo após um lapso temporal razoável, não imediatamente à sua execução. A popularização da internet cumulada com a falta de conscientização da importância de prevenção, com a adoção de medidas de segurança, reflete outra fragilidade da internet. Ou melhor, muitos se utilizam da internet sem a preocupação do perigo de invasão ao computador, por exemplo; sem utilizar antivírus; sem verificar a credibilidade de uma empresa que oferece serviços on-line por ocasião do pagamento de algo ou do fornecimento de dados pessoais, entre outras situações. Podem ser citadas também como problemas as leis obsoletas, em especial no Brasil, que regulamentam o sistema normativo penal, o que acarreta atipi cidade de vários atos, que não poderiam ser previstos no passado. Ainda, há uma barreira por parte de alguns grupos que acreditam que uma repressão muito forte inibiria a liberdade de expressão e a democracia, características da grande rede. Entramos em um dos pontos mais polêmicos da internet, já que não se pode determinar o limite que separa a liberdade de expressão e o dano social. A falta de limites estabelecidos na jurisdição pode gerar efeitos relaciona dos à soberania nacional, nos casos em que mais de um país estivesse envolvi do. Aparece aqui o problema relacionado ao princípio da territorialidade, ou seja, definir se a jurisdição é: a do país de onde partiram os dados: de onde estes dados estão armazenados; ou do país em que o dano foi causado. A de terminação dos lugares em que o crime foi executado e gerou resultados, assim como a definição da materialidade, da autoria e da culpabilidade, acaba por dificultar ainda mais os procedimentos de investigação. Normalmente, o criminoso da informática é um estudioso e está sem pre buscando novos horizontes para aplicar seus conhecimentos. Apesar de cada vez mais a tecnologia aumentar a segurança na rede, os criminosos ultrapassam essas barreiras de acordo com o desafio. Além disso, muitas vezes, o procedimento investigatório não se apresenta vestido de provas ir refutáveis e contundentes do crime cometido. Isto acaba por ser um sintoma decorrente da falta de preparo de alguns agentes de investigação e

> da estrutura disponível. Em solidariedade às dificuldades anteriores, os documentos eletrônicos ou arquivos de computador são provas facilmente modificáveis, permitindo adulterações comprometedoras a seu conteúdo probatório. Portanto, há grandes dificuldades na comprovação da veracidade desses documentos, que podem ser no caso concreto as únicas provas do crime. Vale salientar que não é complicado identificar a máquina utilizada para o crime, mas, sim, identificar a pessoa que a manuseou em determinado momento. Cada vez é mais fácil localizar o computador emitente das informações; o problema é saber quem estava no seu comando. Talvez para isso fosse o caso de regulamentar a responsabilidade do proprietário do equipamento emissor das informações, sendo que na impossibilidade de localizar o criminoso que utilizou o computador para a execução do crime, responsabilizar-se-ia o proprietário da máquina. (Teixeira, 2025, p. 108)

No campo dos crimes financeiros, essa inadequação é ainda mais acentuada, pois a velocidade das transações e a sofisticação dos métodos empregados pelos agentes criminosos demandam uma resposta legislativa e judicial igualmente ágil e especializada.

Inicialmente, o ordenamento jurídico brasileiro tentou enquadrar as fraudes digitais em tipos penais clássicos, como o estelionato (art. 171 do Código Penal) e o furto (art. 155 do Código Penal). Contudo, essa abordagem revelou-se insuficiente. A discussão sobre a natureza jurídica da subtração de valores de uma conta bancária por meio eletrônico – se seria furto mediante fraude ou estelionato – gerou intensos debates doutrinários e jurisprudenciais.

No estelionato, a vítima, induzida a erro, entrega voluntariamente o bem ao criminoso, enquanto no furto qualificado pela fraude, a fraude é um meio para diminuir a vigilância da vítima e permitir a subtração sem a sua anuência. Essa distinção, embora sutil, era crucial e demonstrava a dificuldade de adaptar figuras pensadas para o mundo físico a uma realidade onde a "entrega" e a "subtração" ganham novos contornos.

Percebendo essa lacuna, o legislador brasileiro promoveu alterações significativas no Código Penal. A Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, foi um marco inicial, embora seu foco não fosse primordialmente financeiro. A respeito desse delito do artigo 154-A leciona brilhante o professor Guilherme Nucci:

> Invadir significa violar, transgredir, entrar à força em algum lugar, carregando o verbo nuclear do tipo um forte conteúdo normativo. Logo, a

> conduta do agente não é simplesmente entrar no dispositivo informático alheio, o que se pode dar por mero acidente, mas ocupar um espaço não permitido. O objeto da conduta é o dispositivo informático (qualquer mecanismo apto a concentrar informação por meio de computador ou equipamento similar). São dispositivos informáticos: computador de mesa (desktop), notebook, tablet (ipad e outros), laptop, bem como os smartphones, que hoje constituem verdadeiros “minicomputadores”, dentre outros a surgir com idêntica finalidade. Tal dispositivo informático há de ser alheio (pertencente a terceira pessoa), elemento normativo do tipo, tal como figura no furto (art. 155, CP). Faz-se menção expressa ao estado do dispositivo no tocante à rede de computadores, incluindo, por óbvio, a internet (rede mundial de computadores): é indiferente haja conexão ou não. E está correta tal medida, pois o agente pode invadir computadores desconectados de redes, conseguindo obter dados, adulterar ou destruir informes ali constantes. Pode, ainda, instalar vulnerabilidades, que somente se manifestarão quando houver conexão futura à rede. Há finalidade específica para a conduta, como se verá em nota própria. Finalmente, a outra conduta é instalar (preparar algo para funcionar) vulnerabilidade (mecanismos aptos a gerar aberturas ou flancos em qualquer sistema). É de caráter alternativo (praticar a invasão ou a instalação constitui tipo misto alternativo, vale dizer, cometer uma ou as duas condutas implica crime único). Deve-se complementar o objeto dessa conduta, que é o dispositivo informático. Portanto, o propósito do agente é obter qualquer vantagem ilícita, tornando o dispositivo informático, como, por exemplo, o computador de alguém, acessível à violação. Nota-se que a mera instalação de vulnerabilidade (ex.: softwares mal-intencionados, que permitem o acesso ao conteúdo do dispositivo informático tão logo seja conectado à rede) não causa a violação, mas é nitidamente o seu preparo. (Nucci, 2025, p. 275)

Ao introduzir o art. 154-A no Código Penal, que tipifica a "invasão de dispositivo informático", a lei criminalizou uma conduta que frequentemente constitui um ato preparatório para crimes financeiros. A obtenção de senhas e dados bancários muitas vezes se dá por meio da invasão de computadores ou smartphones, de modo que a punição desse ato, por si só, já representou um avanço na proteção da segurança digital, ainda sobre a temática discorre Nucci:

> Optou o legislador por equiparar a preparação e a execução em igual quilate, para fins de criminalização. Assim, o autor pode apenas instalar vulnerabilidade no dispositivo informático para que, no futuro, outrem dele se valha, como também pode, ele mesmo, utilizar o mecanismo de espionagem

> para a violação de dados e informes. Se o mesmo agente instalar a vulnerabilidade e, depois, invadir o dispositivo informático cometerá um só crime. Caso ele instale, mas outro invada, cada qual cometerá o seu delito distinto, ambos tipificados no art. 154-A. Se duas pessoas, mancomunadas, dividem tarefas (um instala; outro invade), trata-se de crime único, em concurso de agentes (art. 29, CP). Na redação anterior à Lei 14.155/2021, havia a expressão "mediante violação indevida de mecanismo de segurança", agora retirada. Fez bem o legislador em assim proceder, pois era um empecilho inserido no tipo penal, mas desnecessário. Afinal, indicava haver proteção somente para dispositivos informáticos que tivessem um sistema de proteção instalado; em tese, os que não possuíssem esse mecanismo de segurança ficariam ao largo da tutela deste dispositivo. A prova do delito não é simples, mas se admitem todos os meios lícitos possíveis. Quando a invasão estiver em andamento, a vítima pode comprovar o fato imaterial por meio de testemunhas e da ata notarial (documento produzido por tabelião de notas com fé pública, atestando o fato), além de fotos, filmagens, impressão da tela do computador etc. (Nucci, 2025, p. 276)"

Contudo, a resposta mais contundente e específica veio com a Lei nº 14.155/2021, que alterou diretamente o crime de estelionato para abranger de forma inequívoca as fraudes cometidas no ambiente digital. A lei inseriu os parágrafos 2º-A e 2º-B ao artigo 171 do Código Penal, criando a figura da fraude eletrônica. O § 2º-A estabelece que a pena para o estelionato cometido com informações fornecidas pela vítima ou por terceiro induzido a erro, por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, será de reclusão de 4 a 8 anos e multa. Também sobre essa temática, mais uma vez de maneira brilhante nos ensina o professor Guilherme Nucci:

> Trata-se de tipo penal voltado a punir o estelionato digital ou o criptoestelionato, razão pela qual se exige o cenário dessa espécie de delito, envolvendo a obtenção de uma vantagem ilícita (qualquer benefício, ganho ou lucro auferido de modo indevido, ou seja, contrário às regras do ordenamento jurídico. Logicamente, trata-se de vantagem de natureza econômica, uma vez que se cuida de crime patrimonial), em detrimento do patrimônio da vítima. Não basta visualizar apenas o ganho ilícito, pois ele precisa originar-se de um cenário de erro (falsa percepção da realidade) provocado em que perde o seu bem jurídico, erro este causado pelo emprego de artifício (astúcia, esperteza, manobra que implica engenhosidade), ardil (também é um artifício, embora na forma de armadilha, cilada ou estratagema) ou outro meio fraudulento (trata-se de interpretação analógica,

> ou seja, após ter mencionado duas modalidades de meios enganosos, o tipo penal faz referência a qualquer outro semelhante ao artifício e ao ardil, que possa, igualmente, ludibriar a vítima). Em verdade, a fraude é o gênero, que abrange o artifício e o ardil, significando a trapaça, urdida de má-fé, envolvendo a desonestidade para iludir alguém. Nos termos da Lei 14.478/2022, "considera-se ativo virtual a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento, não incluídos: I – moeda nacional e moedas estrangeiras; II – moeda eletrônica, nos termos da Lei n.º 12.865, de 9 de outubro de 2013 [art. 6.º, VI: "moeda eletrônica – recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento"]; III – instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de pontos e recompensas de programas de fidelidade; e IV – representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de valores mobiliários e de ativos financeiros. Parágrafo único. Competirá a órgão ou entidade da Administração Pública federal definido em ato do Poder Executivo estabelecer quais serão os ativos financeiros regulados, para fins desta Lei". Destaque-se que o art. 1.º, parágrafo único, da Lei 14.478/2022 exclui deste âmbito os valores mobiliários, regidos, ainda, pela Lei 6.385/1976. Com origem na Medida Provisória 1.637, de 8 de janeiro de 1998, são valores mobiliários, "quando ofertados publicamente, quaisquer títulos ou contratos de investimento coletivo que gerem direito de participação, de parceria ou remuneração, inclusive resultante da prestação de serviços, cujos rendimentos advêm do esforço do empreendedor ou de terceiros" (disponível em: <https://www.gov.br/investidor/pt-br/investir/como-investir/conheca-o-mercado-de-capitais/o-que-sao-valores-mobiliarios>, acesso em: 26 dez. 2022). (Nucci, 2025, p. 276)

O autor demonstra como a criminalidade acompanha a evolução tecnológica, evidenciando que o *estelionato digital* surge como expressão moderna do antigo ardil humano de enganar, agora potencializado pela virtualização das relações econômicas.

Sob uma perspectiva jurídica e social, percebe-se que a digitalização do dinheiro — antes símbolo material da riqueza — transformou-se em mera representação criptográfica de valor, o que desafia o Estado e o Direito a repensarem seus instrumentos de tutela penal. O ambiente cibernético, ao mesmo tempo em que

democratiza o acesso financeiro, cria um novo espaço de vulnerabilidade, no qual o erro da vítima é explorado com sofisticação técnica e psicológica.

A Lei 14.478/2022, mencionada por Nucci, representa um esforço normativo relevante, mas ainda embrionário, para conter essa nova forma de delinquência patrimonial. A regulamentação dos prestadores de serviços de ativos virtuais não apenas reconhece a existência jurídica das criptomoedas, como também reforça a necessidade de um Direito Penal tecnológico, capaz de acompanhar as inovações financeiras sem perder de vista a proteção da boa-fé e da confiança — pilares históricos das relações econômicas.

O crime, antes praticado com artifícios manuais, agora é cometido por meio de códigos binários, mas continua fundamentado na mesma essência moral — a fraude como forma de violação da confiança social, Nucci segue:

> Conforme dispõe o art. 2.º da referida Lei 6.385/1976, são valores mobiliários: "I – as ações, debêntures e bônus de subscrição; II – os cupons, direitos, recibos de subscrição e certificados de desdobramento relativos aos valores mobiliários referidos no inciso II; III – os certificados de depósito de valores mobiliários; IV – as cédulas de debêntures; V – as cotas de fundos de investimento em valores mobiliários ou de clubes de investimento em quaisquer ativos; VI – as notas comerciais; VII – os contratos futuros, de opções e outros derivativos, cujos ativos subjacentes sejam valores mobiliários; VIII – outros contratos derivativos, independentemente dos ativos subjacentes; e IX – quando ofertados publicamente, quaisquer outros títulos ou contratos de investimento coletivo, que gerem direito de participação, de parceria ou de remuneração, inclusive resultante de prestação de serviços, cujos rendimentos advêm do esforço do empreendedor ou de terceiros". São excluídos da referida Lei: "I – os títulos da dívida pública federal, estadual ou municipal; II – os títulos cambiais de responsabilidade de instituição financeira, exceto as debêntures" (§ 1.º). Pode-se obter vasta quantidade de informações, navegando pela Internet, a respeito de moeda virtual ou digital, denominada criptomoeda, pois se trata de um dinheiro virtual, vale dizer, não existe fisicamente. Surge, então, um novo vocabulário a ser dominado com o passar do tempo não somente pelos investidores desse mercado, mas, igualmente, pelos operadores do Direito, visto que, onde há circulação de valores passíveis de gerar riqueza, encontra-se o criminoso valendo-se da novidade para, também, inaugurar uma fatia de delinquência inovadora. Os agentes estatais devem lidar com esses golpes, que representam formatos de delitos contra o patrimônio tecnologicamente mais avançados.Diante

> disso, a Lei 14.478/2022 foi editada para dispor sobre as diretrizes da prestação de serviços relativos a ativos virtuais, regulamentando as prestadoras desses serviços. Não é a primeira nem será a derradeira a abordar essa temática, cada vez mais presente no cotidiano de todos. Em verdade, a era do dinheiro fisicamente existente já passou há muito, pois a confiança no mercado digital cresce a cada dia não somente porque as pessoas apreciam essa inovação, mas pelo fato de haver a imposição das instituições financeiras de um modo geral. Lembre-se do fechamento gradual das agências bancárias, onde havia atendimento pessoal por diversos funcionários, surgindo, em seu lugar, postos de atendimento e, muito mais, pontos eletrônicos para transações ou retirada de papel-moeda. Não se guarda mais o dinheiro no cofre, esperando que ele valorize com o passar do tempo (considerando-se uma moeda forte, como o dólar ou o euro), desaparecendo, quase por completo, a era do dinheiro guardado no colchão (exceto para alguns corruptos que conseguem preencher um apartamento inteiro com papel-moeda espalhado pelos cômodos). Na atualidade, o cidadão comum é conduzido a promover transações por meio de aplicativos e, cada vez mais (por enquanto), por intermédio do celular, a ponto de se poder imaginar que a perda desse aparelho pode significar o desaparecimento de documentos digitais, contendo dados pessoais (CNH, RG, CPF, título de eleitor, entre outros, em formato digital), aplicativos de bancos, onde se encontram dados financeiros detalhados e a viabilidade de se fazer transferências de quantias para outras contas (vide o incremento do PIX, utilizado, hoje, até para pessoas carentes solicitarem ajuda nos semáforos de grandes cidades), aplicativos de estabelecimentos comerciais, que podem ser usados para fazer compras on-line, além de uma infinidade de outras situações similares. (Nucci, 2025, p. 415)

Essa inovação legislativa foi crucial por três motivos principais. Primeiro, estabeleceu uma pena significativamente mais alta do que a do estelionato comum, reconhecendo a maior gravidade e o maior potencial de dano das fraudes digitais. Segundo, descreveu o *modus operandi* típico dos crimes cibernéticos, como o *phishing* e a engenharia social, eliminando a dubiedade jurídica anterior. Terceiro, o § 2º-B previu um aumento de pena (de 1/3 a 2/3) se o crime for praticado mediante a utilização de servidor mantido fora do território nacional, um reconhecimento explícito do caráter transnacional desses delitos.

> Enfim, goste-se ou não, o cenário virtual já atinge a sociedade de modo definitivo e o papel-moeda perdeu seu status no meio econômico-financeiro, embora seja relevante para representar a riqueza de alguém, de

> uma empresa e até mesmo de um país. O dinheiro digital, criado por meio de software de criptografia, ocupa um espaço relevante nas aplicações e nos investimentos, de modo que se tornou um alvo dos criminosos, em particular, dos estelionatários. Torna-se impossível furtar um bitcoin, que não é uma coisa móvel, embora seja perfeitamente viável administrar uma carteira de investimentos de ativos virtuais fraudulenta, captando recursos, enganando várias pessoas e amealhando o patrimônio de terceiros. (Nucci, 2025, p. 416)

Apesar dos avanços na tipificação, a responsabilização penal ainda enfrenta enormes desafios probatórios e processuais. A primeira barreira é a identificação da autoria. Criminosos digitais utilizam uma série de ferramentas para mascarar sua identidade e localização, como o uso de redes privadas virtuais (VPNs), servidores proxy e redes de anonimização como a Tor. Para superar esse obstáculo, a cooperação de provedores de conexão e de aplicação torna-se indispensável. O Marco Civil da Internet (Lei nº 12.965/2014) estabelece, em seu artigo 10º, a obrigatoriedade de guarda dos registros de conexão pelo prazo de um ano, dados que só podem ser fornecidos mediante ordem judicial. Esses registros são vitais para rastrear o endereço de IP (Internet Protocol) utilizado na prática do crime, sendo o primeiro passo para chegar ao autor.

No entanto, quando os servidores ou os provedores estão localizados no exterior, a dificuldade aumenta exponencialmente, esbarrando na soberania de outros países. Nesses casos, a obtenção de dados depende da ativação de mecanismos de cooperação jurídica internacional, como os Tratados de Assistência Jurídica Mútua (MLATs - *Mutual Legal Assistance Treaties*). Este é um processo burocrático e lento, que muitas vezes se choca com a necessidade de celeridade na investigação de crimes cibernéticos, nos quais as provas digitais são extremamente voláteis. A adesão do Brasil à Convenção de Budapeste sobre o Cibercrime, embora tardia, representa uma esperança de agilizar essa cooperação, criando canais de comunicação mais diretos e eficientes entre os países signatários para a preservação e o compartilhamento de evidências digitais.

Outro desafio colossal reside na questão da competência jurisdicional. Onde julgar um crime em que o autor está em um país, utiliza um servidor em outro, para atacar uma vítima em uma terceira localidade no Brasil, cuja conta bancária está sediada em uma quarta cidade? A regra geral do Código de Processo Penal brasileiro fixa a competência pelo lugar da consumação da infração (*locus delicti commissi*). Nos

crimes financeiros digitais, o Superior Tribunal de Justiça (STJ) tem firmado o entendimento de que a consumação ocorre no local onde a vítima sofre o prejuízo financeiro, ou seja, onde está localizada a agência bancária da conta da qual os valores foram subtraídos. Essa interpretação visa proteger a vítima e facilitar a colheita de provas, evitando que a competência seja pulverizada ou transferida para jurisdições estrangeiras de difícil acesso. Conforme leciona Cury:

> O bem jurídico tutelado pela norma penal econômica toma a tonalidade de internacionalizado frente ao cenário atual globalizado de fluxo econômico mundial, em que os interesses e a proteção econômica passaram a ser comuns entre os países, ou seja, o resultado da própria estrutura interna por vezes advém de uma determinada influência internacional. Gerando, portanto, um enorme reflexo no direito penal econômico advindo de sua internacionalização ou da unificação de proteção do bem jurídico que detém um caráter comum entre os Estados. Apesar da necessidade de maior precisão conceitual, no âmbito do direito penal econômico, o bem jurídico como internacional pode ser norteada pela intervenção penal nacional que, não poucas vezes, visa a uma proteção considerada internacionalmente relevante. (Cury, 2020, p. 180)

Adicionalmente, a ascensão dos criptoativos abriu uma nova e complexa fronteira para a criminalidade financeira, especialmente para a lavagem de dinheiro. A natureza descentralizada e o pseudoanonimato de criptomoedas como o Bitcoin são explorados para ocultar a origem ilícita de recursos. Criminosos utilizam *mixers* ou *tumblers*, serviços que misturam fundos de diversas fontes para quebrar o rastro nas *blockchains*, dificultando enormemente a vinculação do dinheiro "sujo" ao crime antecedente. As transações com criptomoedas, que atraem um número crescente de especuladores (traders), ainda levantam divergências entre economis-tas e especialistas em segurança digital. (CURY, 2020).

A Lei nº 9.613/1998, que trata da lavagem de dinheiro, é plenamente aplicável a essas transações, pois seu tipo penal é amplo e abrange a conduta de "ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores". Recentemente, a Lei nº 14.478/2022 (Marco Legal dos Criptoativos) trouxe avanços ao regulamentar as prestadoras de serviços de ativos virtuais (*exchanges*), que passaram a ter o dever de reportar operações suspeitas ao Conselho de Controle de Atividades Financeiras (COAF). Essa medida, embora não altere o tipo penal, fortalece os mecanismos de controle e fornece aos investigadores

informações cruciais para detectar e reprimir a lavagem de dinheiro por meio de criptoativos.

Em suma, a responsabilização penal por crimes financeiros digitais no Brasil é um campo em constante construção. Se por um lado o legislador tem se esforçado para modernizar a legislação material, criando tipos penais específicos e mais severos, por outro, os desafios processuais, probatórios e de cooperação internacional persistem.

A efetividade do combate a essa modalidade criminosa não depende apenas de leis mais duras, mas de um ecossistema integrado que envolve o fortalecimento da capacidade técnica das polícias judiciárias, a especialização de membros do Ministério Público e do Judiciário, a agilização da cooperação internacional e, fundamentalmente, a colaboração do setor privado, que detém a infraestrutura pela qual os crimes são cometidos e por onde as provas transitam. Rogério Greco elucida essa temática de maneira maestral nos seguintes termos:

> Um espanhol, usuário da internet, pode acessar a rede e contatar com uma empresa alemã, vendedora ou prestadora de serviços, graças ao acesso à internet, proporcionado pela filial holandesa de um provedor norte-americano. As fronteiras estatais se diluem na internet. A aldeia global se transformou em realidade. Podemos dizer que as questões legais mais espinhosas que são colocadas no ciberespaço correspondem ao direito internacional privado. (Greco, 2025, p. 424)

3 CONSIDERAÇÕES FINAIS

Os crimes financeiros no ambiente virtual são variados e sofisticados, incluindo, como visto, as fraudes bancárias, *phishing*, *ransomware*, lavagem de dinheiro e pirataria digital. A tecnologia desempenha um papel fundamental nesses delitos, facilitando a realização de transações fraudulentas de forma rápida e quase imperceptível. A utilização de criptomoedas e de redes descentralizadas torna ainda mais difícil rastrear os responsáveis por esses crimes, o que exige das autoridades uma capacidade técnica avançada para investigar e punir os criminosos.

Os impactos na economia global são sérios, afetando diretamente o mercado financeiro e os investidores. A instabilidade causada por fraudes e golpes financeiros pode gerar perdas bilionárias e abalar a confiança dos agentes econômicos,

prejudicando o crescimento econômico e a sustentabilidade do sistema financeiro internacional. Além disso, a reputação das empresas onde os crimes aconteceram pode ser severamente prejudicada, resultando em danos irreparáveis para sua imagem no mercado.

As medidas de prevenção que empresas e indivíduos podem adotar para se protegerem de fraudes e golpes financeiros no ambiente digital incluem a utilização de softwares antivírus atualizados, a verificação da autenticidade dos sites antes de realizar transações online e o cuidado com informações pessoais que são sensíveis. Além disso, é fundamental investir em treinamentos sobre segurança cibernética e promover uma cultura voltada para a proteção dos dados.

É fundamental a implantação de uma cultura de educação financeira e letramento digital nacional, para erradicar esses golpes e fraudes online, sendo essencial conscientizar os indivíduos sobre os riscos associados às transações virtuais, os bancos e instituições financeiras devem não somente oferecer treinamento aos seus colaboradores, mas aos seus clientes de uma forma geral. A disseminação de informações corretas sobre segurança cibernética e boas práticas no uso da web pode contribuir significativamente para reduzir o número de vítimas desses cibercrimes e trazer um ambiente de segurança transacional.

4 REFERÊNCIAS

CUNHA, L. G. S.; CORTIZO, P. C. A evolução dos crimes financeiros e os impactos na sociedade. **Revista de Estudos Jurídicos**, 2024.

FARIAS, P. R. M.; SILVA, F. M.; CAVALCANTI, L. A. S. A importância da conscientização digital na prevenção de fraudes. **Anais do Congresso de Segurança da Informação**, 2023.

FARINHA, G. A. Criptomoedas e a lavagem de dinheiro: desafios para a regulação. In: JORNADA DE ESTUDOS REGULATÓRIOS, 5., 2021, Brasília. **Anais** [...]. Brasília: CADI, 2021.

FREITAS, C. C. G. de; GONÇALVES, J. R. A evolução do direito penal brasileiro relacionado aos crimes cibernéticos. **Revista JRG de Estudos**, 2023. Disponível em: http://www.revistajrg.com/index.php/jrg/article/view/520. Acesso em: 10 out. 2024.

GUIMARÃES, P. V. **A Criminalidade virtual e os desafios do direito brasileiro face ao avanço dos crimes cibernéticos**. 2024. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2024. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7549. Acesso em: 30 out. 2024.

NETO, G. R. Desafios e implicações do Direito Penal na era digital: explorando as profundezas da Deep Web. **Scientia Socialis Aplicadas**, 2023. Disponível em: https://periodicos.ufn.edu.br/index.php/disciplinarumSA/article/view/4689. Acesso em: 01 dez. 2024.

NOGUEIRA, M. A. A. **Crime de uso indevido de informação privilegiada no direito brasileiro**. 2018. Dissertação (Mestrado em Direito) – Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2018. Disponível em: https://pantheon.ufrj.br/handle/11422/6596. Acesso em: 30 out. 2024.

PACCES, A. C.; GIACCHERI, I. de P. A era digital e o governo eletrônico. **Revista de Direito Internacional**, 2017. Disponível em: https://revistas.pucsp.br/DIGE/article/view/35166. Acesso em: 01 dez. 2024.

RICARDO, J. S. Criptoativos: regulamentação e desafios emergentes para o combate aos crimes financeiros. **Revista Reflexão e Crítica do Direito**, 2021. Disponível em: https://revistas.unaerp.br/rcd/article/view/2310. Acesso em: 30 out. 2024.

SILVA, H. E. R.; AMARAL, A. A. R. do. Responsabilidade civil na era digital: desafios e perspectivas. **Revista Acadêmica Online**, 2024. Disponível em: https://revistaacademicaonline.com/index.php/rao/article/view/26. Acesso em: 01 jan. 2025.

SOUSA, M. V. A complexidade da investigação de crimes cibernéticos. **Revista Brasileira de Segurança Pública**, 2022.

NUCCI, Guilherme de S. **Curso de Direito Penal - Vol.2** - 9ª Edição 2025. 9. ed. Rio de Janeiro: Forense, 2025. E-book. pág.276. ISBN 9788530996666. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788530996666/. Acesso em: 11 out. 2025.

GRECO, Rogério. **Curso de Direito Penal Vol.2** - 22ª Edição 2025. 22. ed. Rio de Janeiro: Atlas, 2025. E-book. pág.424. ISBN 9786559776924. Disponível em:

https://app.minhabiblioteca.com.br/reader/books/9786559776924/. Acesso em: 11 out. 2025.

BITENCOURT, Cezar R. **Tratado de Direito Penal - Parte Especial** - Vol.2 - 25ª Edição 2025. 25. ed. Rio de Janeiro: SRV, 2024. E-book. pág.669. ISBN 9788553627615. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788553627615/. Acesso em: 11 out. 2025.

CURY, Rogério. **Direito Penal Econômico**. São Paulo: Almedina Brasil, 2020. E-book. pág.109. ISBN 9786556270531. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786556270531/. Acesso em: 11 out. 2025.

PODER360. **Pix: Golpes crescem 80% e somam R$ 6,5 bilhões em 2024**. Poder360, 25 abr. 2025. Disponível em: https://www.poder360.com.br/poder-economia/golpes-do-pix-crescem-80-e-somam-r-65-bilhoes-em-2024/ Acesso em: 11 out. 2025.

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico** - 9ª Edição 2025. 9. ed. Rio de Janeiro: SRV, 2025. E-book. pág.592. ISBN 9788553624317. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788553624317/. Acesso em: 11 out. 2025.

República Federativa do Brasil
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

Termo de Autenticidade

Eu, **JHÔNATAS GABRIEL ATAÍDE DE SOUZA,** acadêmico regularmente apto(a) a proceder ao depósito do Trabalho de Conclusão de Curso intitulado **"CRIMES FINANCEIROS NA ERA DIGITAL: A EVOLUÇÃO DOS MÉTODOS DOS CIBERCRIMES"**, declaro, sob as penas da lei e das normas acadêmicas da UFMS, que o Trabalho de Conclusão de Curso ora depositado é de minha autoria e que fui instruído pelo meu orientador Professor Dr. Carlos Eduardo Pereira Furlani acerca da ilegalidade do plágio, de como não o cometer e das consequências advindas de tal prática, sendo, portanto, de minha inteira e exclusiva responsabilidade, qualquer ato que possa configurar plágio.

Três Lagoas/MS, 14/10/2025

gov.br Documento assinado digitalmente
JHONATAS GABRIEL ATAIDE DE SOUZA
Data: 14/10/2025 18:34:51-0300
Verifique em https://validar.iti.gov.br

_____

JHÔNATAS GABRIEL ATAÍDE DE SOUZA

República Federativa do Brasil
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

Termo de Depósito e Composição da Banca Examinadora

Eu, professor **CARLOS EDUARDO PEREIRA FURLONI**, orientador acadêmico **JHÔNATAS GABRIEL ATAÍDE DE SOUZA,** autorizo o depósito do Trabalho de Conclusão de Curso intitulado **"CRIMES FINANCEIROS NA ERA DIGITAL: A EVOLUÇÃO DOS MÉTODOS DOS CIBERCRIMES"**.

Informo, também, a composição da banca examinadora e a data da defesa do TCC:

Presidente: Dr. Carlos Eduardo Pereira Furlani

lº avaliador: Dr. Marçal Rogério Rizzo

2º avaliador: Dr. Adailson da Silva Moreira

Data: 31/10/2025

Horário: 16 horas

Três Lagoas/MS, 14/10/2025

Documento assinado digitalmente
gov.br
CARLOS EDUARDO PEREIRA FURLANI
Data: 06/11/2025 23:55:36-0300
Verifique em https://validar.iti.gov.br

_____

CARLOS EDUARDO PEREIRA FURLONI