CRIMES CIBERNÉTICOS COM CRIPTOMOEDAS: ANÁLISE DA LEGISLAÇÃO BRASILEIRA E ESTUDO DE CASOS

CYBER CRIMES WITH CRYPTOCURRENCIES: ANALYSIS OF BRAZILIAN LEGISLATION AND CASE STUDIES

Flavio Granado Filho[1]
Bruna Sozzo[2]

RESUMO

A crescente popularidade das criptomoedas tem sido acompanhada por um aumento alarmante em crimes cibernéticos, com a lavagem de dinheiro emergindo como uma das principais preocupações. As características intrínsecas das criptomoedas, como descentralização e potencial anonimato, as tornam um veículo atrativo para atividades ilícitas. Dada a gravidade desta situação, é crucial estar bem informado sobre as estratégias de segurança que podem ser adotadas para combatê-la. Neste artigo, fazemos uma abordagem ao tema, conduzindo uma análise meticulosa de estudos de casos, revisando literaturas contemporâneas e examinando a legislação brasileira em relação a crimes cibernéticos associados a criptomoedas. Nosso objetivo é elucidar os principais métodos criminosos e, mais importante, fornecer orientações robustas para sua prevenção.

Palavras-chave: cibercrimes; criptomoedas; legislação brasileira;

ABSTRACT

The rising popularity of cryptocurrencies has been met with an alarming surge in cybercrimes, with money laundering emerging as a primary concern. The intrinsic characteristics of cryptocurrencies, such as decentralization and potential anonymity, make them an attractive vehicle for illicit activities. Given the severity of this situation, it is vital to be well informed about the security strategies that can be employed to counteract it. In this article, we delve deeply into the subject, conducting a meticulous analysis of case studies, reviewing contemporary literature, and scrutinizing Brazilian legislation concerning cybercrimes associated with cryptocurrencies. Our goal is to shed light on the primary criminal methods and, most importantly, provide robust guidelines for their prevention.

Keywords: cybercrimes; cryptocurrencies; brazilian legislation.

[1] Centro Universitário Filadélfia de Londrina - UniFil
[2] Centro Universitário Filadélfia de Londrina - UniFil

INTRODUÇÃO

As criptomoedas, tornaram-se cada vez mais relevantes na economia global. Por meio da tecnologia, as criptomoedas oferecem uma maneira descentralizada e segura de realizar transações financeiras sem a necessidade de intermediários. No entanto, esse crescimento também trouxe consigo novas formas de crimes cibernéticos, incluindo a lavagem de dinheiro. As criptomoedas oferecem um certo grau de anonimato, o que as torna atraentes para criminosos que procuram esconder suas atividades ilegais. Diante desse cenário, este artigo traz uma análise sobre os crimes cibernéticos relacionados a criptomoedas e a lavagem de dinheiro resultante desses crimes. Para atingir esse objetivo, realizamos estudos de casos e uma revisão da literatura atual sobre o tema. Além disso, também realizamos uma análise da legislação brasileira relacionada a essas atividades criminosas. Em seguida, discutimos as medidas de segurança que podem ser implementadas para prevenir tais atos ilegais. Com essa análise, espera-se contribuir para o desenvolvimento de medidas mais eficazes na prevenção dos mesmos, bem como um aprofundamento sobre os crimes cibernéticos envolvendo criptomoedas.

É importante destacar que a metodologia adotada neste estudo inclui a análise de casos concretos de crimes envolvendo criptomoedas. Ao realizar as análises, nosso objetivo é elucidar as técnicas utilizadas pelos criminosos e as falhas do sistema atual de prevenção e combate a esses crimes. Assim, podemos identificar os pontos fracos e fortes da legislação brasileira em relação aos crimes cibernéticos envolvendo criptomoedas e propor sugestões de melhorias para a sua prevenção e combate.

Na primeira parte deste trabalho, são discutidos os tipos de crimes cibernéticos que envolvem criptomoedas, tais como fraude com criptomoedas e mineração ilegal. São apresentados estudos de casos que exemplificam esses crimes, a fim de compreender melhor como essas práticas criminosas são realizadas e quais são os prejuízos que elas acarretam. Na segunda parte, realizamos uma análise da legislação brasileira relacionada aos crimes cibernéticos com criptomoedas. Além disso, discutimos leis e normas relevantes para o entendimento do artigo. Finalmente, na conclusão, utilizamos a análise desenvolvida ao longo do trabalho para propor formas de previnir crimes cibernéticos relacionados a cripitomoedas.

METODOLOGIA

Os crimes cibernéticos envolvendo criptomoedas e lavagem de dinheiro têm se mostrado um grande desafio para as autoridades brasileiras. Com o crescimento do uso das criptomoedas, tornou-se mais difícil rastrear transações financeiras e identificar os autores desses crimes. Nesse contexto, o presente estudo busca oferecer uma contribuição significativa para o aprimoramento da legislação brasileira em relação a esse tipo de delito.

Uma das principais contribuições deste estudo é a identificação das principais lacunas na legislação brasileira em relação aos crimes cibernéticos envolvendo criptomoedas e lavagem de dinheiro. A partir dessa identificação, é possível propor ideias efetivas para a prevenção e combate a esses crimes. Entre as sugestões estão medidas de regulamentação mais rigorosas, que permitam maior controle e fiscalização das transações financeiras envolvendo criptomoedas, bem como a criação de mecanismos mais eficazes de investigação e punição.

Outra importante contribuição deste estudo é a conscientização da sociedade sobre a importância da prevenção e combate aos crimes cibernéticos envolvendo criptomoedas e lavagem de dinheiro. Por meio de informações claras e objetivas sobre os riscos e vulnerabilidades envolvendo o uso de criptomoedas, espera-se que este estudo possa contribuir para o aumento da conscientização da população e de autoridades sobre a necessidade de medidas legais mais rigorosas e efetivas para garantir a segurança e integridade do sistema financeiro.

Ademais, espera-se que este estudo possa fomentar o avanço da pesquisa na área de crimes cibernéticos envolvendo criptomoedas. Ao fornecer novas perspectivas e abrir caminho para futuras pesquisas sobre o tema, é possível contribuir para o desenvolvimento de soluções inovadoras para prevenir e combater esses crimes. Espera-se, portanto, que este estudo possa estimular a produção de novos conhecimentos e avanços tecnológicos que possam ser aplicados na prevenção e combate a crimes cibernéticos envolvendo criptomoedas.

Como desdobramentos deste estudo, espera-se que haja maior atenção por parte dos órgãos competentes na regulamentação e fiscalização das transações financeiras envolvendo criptomoedas, além do aumento da conscientização da sociedade

sobre a necessidade de medidas legais mais rigorosas e efetivas para garantir a segurança e integridade do sistema financeiro. Além disso, espera-se que as sugestões apresentadas neste estudo possam ser utilizadas como base para o aprimoramento da legislação brasileira em relação a esses crimes, além de estimular o desenvolvimento de novas pesquisas e soluções tecnológicas para prevenir e combater esses delitos.

Com isso, a pesquisa será realizada de acordo com os pontos abordados abaixo:

• **Artigos Científicos:** Será realizada uma busca minuciosa em bases de dados acadêmicas reconhecidas nacional e internacionalmente, como *Scielo*, *Google Scholar*, *Web of Science*, entre outras. O objetivo é identificar e revisar estudos já publicados sobre crimes cibernéticos relacionados a criptomoedas, bem como sobre medidas de prevenção e combate a esses crimes em diferentes jurisdições.

• **Legislação Vigente:** Estudar-se-á a legislação brasileira vigente relacionada a crimes cibernéticos, lavagem de dinheiro e regulamentação de criptomoedas. Além disso, analisar se há legislações de outros países que tenham obtido sucesso na regulação e combate a crimes envolvendo criptomoedas.

• **Sites Oficiais e Relatórios:** Serão consultados sites de órgãos reguladores financeiros, como Banco Central, Receita Federal e COAF, para compreender melhor o cenário regulatório brasileiro e as preocupações atuais dos órgãos reguladores sobre a temática.

• **Estudos de Casos Específicos:** Será feita uma seleção criteriosa de casos notórios de crimes cibernéticos envolvendo criptomoedas no Brasil. Esses estu- dos de caso terão como objetivo entender as táticas utilizadas pelos criminosos, as lacunas legais que permitiram tais práticas e os desafios enfrentados pelas autoridades para rastrear e punir os responsáveis.

• **Análise e Interpretação de Dados:** Com base nos dados coletados, será feita uma análise qualitativa e quantitativa para identificar padrões, lacunas e oportunidades de melhoria na legislação e nas práticas de combate a crimes envolvendo criptomoedas.

• **Propostas e Sugestões:** A partir dos insights obtidos durante a pesquisa, serão formuladas propostas concretas de medidas legais, regulamentações e práticas que possam ser adotadas para combater eficazmente os crimes cibernéticos relacionados a criptomoedas.

Em resumo, este artigo empregará uma abordagem multifacetada, combinando revisão bibliográfica, análise de legislação e estudos de caso para obter uma visão abrangente e aprofundada sobre o tema e, assim, contribuir efetivamente para o combate a crimes cibernéticos envolvendo criptomoedas no Brasil.

ESTADO DA ARTE

Com a popularização da internet e a evolução da tecnologia, surgiram novas possibilidades e desafios para a sociedade, como o aumento dos crimes cibernéticos envolvendo criptomoedas e a lavagem de dinheiro. No Brasil, a legislação tem se esforçado para coibir esses crimes, mas ainda enfrenta desafios na identificação e punição dos criminosos. Neste capítulo, apresentamos um breve referencial teórico sobre os crimes cibernéticos, as criptomoedas, a legislação brasileira e alguns casos que ilustram os desafios enfrentados na punição dos crimes mencionados.

Cibercrimes

Cibercrimes é a nomeclatura dada aos crimes que envolvem qualquer atividade ou prática ilícita na rede. Gordon e Ford (2006) classificam os cibercrimes em duas categorias: Tipo I e Tipo II que também são conhecidos na literatura como crimes virtuais próprios e impróprios. Os cibercrimes próprios são delitos praticados contra a informática como, por exemplo, a violação de e-mail, danos causados por vírus, pirataria de *softwares* etc. Já os crimes impróprios se encontram tipificados no código penal como a falsidade ideológica, estelionato, calúnias, difamações praticadas em ambiente virtual.

Quando falamos de cibercrimes envolvendo criptomoedas podem ser classificados como próprios quanto impróprios, dependendo da natureza das atividades

ilícitas realizadas. Os crimes próprios são aqueles diretamente relacionados ao uso de criptomoedas, como o roubo de chaves privadas, invasões de carteiras digitais, esquemas de pirâmide baseados em criptomoedas e a manipulação de mercados por meio de práticas ilegais, como *pump and dump*. Por outro lado, os cibercrimes impróprios referem-se a atividades criminosas que utilizam criptomoedas como meio de pagamento ou ocultação de fundos, como o tráfico de drogas e armas, lavagem de dinheiro, extorsões e ransomware. Ambos os tipos de cibercrimes apresentam desafios significativos para as autoridades e requerem esforços conjuntos para combater as ameaças e proteger os usuários e investidores.

Criptomoedas

As criptomoedas são um tipo de moeda digital que se baseia em criptografia para garantir sua segurança e integridade. Elas operam em uma rede descentralizada e são criadas por meio de um processo chamado mineração, que envolve a solução de problemas matemáticos complexos por computadores de alto desempenho. De acordo com Ulrich (2017) a primeira criptomoeda a surgir foi o *Bitcoin*, em 2009, e desde então várias outras foram criadas, como *Ethereum*, *Litecoin*, *Ripple*, entre outras.

Uma das principais características das criptomoedas é a sua descentralização, como afirma Previdi (2014). Diferentemente das moedas tradicionais, como o dólar ou o euro, que são emitidas por governos e bancos centrais, as criptomoedas não são controladas por nenhum órgão central. Isso significa que não há uma autoridade responsável por regular sua emissão, circulação ou valorização. Outra característica das criptomoedas é a sua acessibilidade. Qualquer pessoa com acesso à internet pode comprar, vender ou armazenar criptomoedas. Isso significa que as criptomoedas oferecem uma forma democrática de investimento e uma alternativa aos investimentos tradicionais, que muitas vezes exigem altos valores mínimos para investimento.

Por outro lado, as criptomoedas enfrentam algumas barreiras para sua adoção em larga escala. Uma delas é a sua volatilidade, como aponta Pizzetti (2018). Como o valor das criptomoedas é determinado pela oferta e demanda do mercado, ele pode variar significativamente em curtos períodos de tempo. Isso torna as criptomoedas um investimento arriscado e muitas pessoas ainda têm receio de investir nelas. Além

disso, as criptomoedas ainda não são amplamente aceitas como forma de pagamento. Embora algumas empresas já aceitem criptomoedas como meio de pagamento, a maioria dos estabelecimentos ainda não as reconhecem como uma forma válida de pagamento. Isso limita a sua utilidade no dia a dia das pessoas.

Blockchain e carteiras digitais

O *blockchain* é uma tecnologia de registro de dados que permite o armazenamento de informações de forma segura e descentralizada. Isso significa que os dados não são armazenados em um único local, mas sim distribuídos em vários nós de rede. Essa estrutura torna o *blockchain* muito resistente a fraudes e ataques cibernéticos.

Uma carteira digital é um *software* que permite aos usuários armazenar e gerenciar suas criptomoedas. As carteiras digitais podem ser on-line ou off-line. As carteiras on-line são mais convenientes, mas também são mais vulneráveis a ataques cibernéticos. As carteiras *off-line* são mais seguras, mas também são menos convenientes.

Atualmente existem vários tipos de golpes que podem ocorrer através da *blockchain* e das carteiras digitais. Pode ser citado alguns desses golpes abaixo:

Phishing: Os golpistas enviam e-mails ou mensagens de texto que parecem ser de fontes confiáveis, como *exchanges* de criptomoedas ou carteiras digitais. O e-mail ou mensagem de texto pede ao destinatário para clicar em um link ou fornecer suas informações pessoais, como sua senha ou endereço de carteira. Se o destinatário clicar no link ou fornecer suas informações pessoais, os golpistas poderão roubar suas criptomoedas ou seu dinheiro.

Malware: Os golpistas criam *malware* que rouba criptomoedas de carteiras digitais. O *malware* pode ser instalado em computadores ou dispositivos móveis através de links maliciosos, anexos de e-mail ou *downloads* de sites não seguros.

Scams: Os golpistas criam esquemas fraudulentos que prometem grandes lucros em troca de um investimento em criptomoedas. Esses esquemas geralmente são fraudulentos e os investidores perderão seu dinheiro.

Legislação Brasileira

No Brasil, a legislação criminaliza o uso de criptomoedas para fins ilícitos, como descrito e previsto pela última publicação do Vade Mecum 35ª edição (2023) na Lei nº 9.613/1998, que trata dos crimes de lavagem de dinheiro. Além disso, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, determina a responsabilidade civil e criminal de empresas provedoras de internet em casos de crimes cometidos por seus usuários. Em 2019, foi promulgada a Lei nº 13.964/2019 como descrita no Vade Mecum 28ª edição (2019), conhecida como Pacote Anticrime, que trouxe importantes mudanças na legislação brasileira para combater a corrupção, o crime organizado e os crimes cibernéticos. Entre as mudanças, a lei prevê o agravamento das penas para crimes cometidos com o uso de criptomoedas e a possibilidade de bloqueio de criptomoedas e ativos virtuais em investigações criminais. No entanto, a falta de regulamentação específica sobre criptomoedas e a complexidade das tecnologias envolvidas dificultam a identificação e punição dos criminosos. Além disso, a dificuldade de cooperação internacional é um fator que pode afetar a eficácia da legislação bra- sileira no combate aos crimes relacionados a criptomoedas. Como a tecnologia das criptomoedas é transnacional, a identificação e punição dos criminosos muitas vezes requer a cooperação de outras jurisdições.

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que entrou em vigor em 2020, com o objetivo de proteger a privacidade e os dados pessoais dos cidadãos. Ela estabelece diretrizes para a coleta, armazenamento e compartilhamento de dados, exigindo consentimento explícito dos titulares. A LGPD busca promover segurança e privacidade, mas enfrenta desafios no combate a crimes envolvendo criptomoedas, devido à falta de regulamentação específica e à necessidade de cooperação internacional para identificar e punir os criminosos. Para mais informaçõess sobre a lei acima, consultar Anexo 01.

DESENVOLVIMENTO

Nesta seção, aprofundaremos a discussão sobre as lacunas na legislação brasileira em relação a crimes envolvendo criptomoedas, examinando como essas

aberturas têm contribuído para a impunidade e para a dificuldade na identificação dos responsáveis por atividades ilegais relacionadas a moedas digitais. Além disso, apresentaremos uma série de sugestões concretas para prevenir e combater esses crimes de forma mais eficaz, abordando questões como a regulamentação, a cooperação internacional e as medidas adicionais que podem ser adotadas para aprimorar a responsabilidade civil e criminal das empresas. Ao final desta seção, destacaremos a importância de abordar essas questões de maneira colaborativa e multidisciplinar, a fim de criar um ambiente mais seguro e regulamentado para o uso das criptomoedas, garantindo que elas possam contribuir positivamente para a economia global e, ao mesmo tempo, impedindo seu uso indevido por organizações criminosas.

Estudo de Casos

O caso do Grupo Bitcoin Banco, ocorrido em 2019 no Brasil, exemplifica a dificuldade na identificação e punição de crimes cibernéticos envolvendo criptomoedas. Nesse caso, a empresa prometia retornos financeiros significativos em investimentos em criptomoedas, mas acabou lesando mais de 7 000 clientes. O Grupo Bitcoin Banco teria utilizado uma criptomoeda própria, a NegocieCoins, para desviar fundos de seus investidores. As investigações para identificar os responsáveis pelo crime ainda estão em andamento.

Outro exemplo é o caso da quadrilha que utilizava criptomoedas para lavagem de dinheiro e tráfico de drogas, desarticulada pela Polícia Federal em 2020. A organização criminosa utilizava criptomoedas para ocultar a origem ilícita de seus lucros e transferir dinheiro para o exterior, dificultando a identificação e rastreamento dos valores. A ação da Polícia Federal resultou na prisão de diversos membros da organização, mas a investigação ainda está em curso para identificar outros envolvidos e apreender os valores desviados.

Embora o Brasil tenha avançado na regulamentação dos crimes cibernéticos envolvendo criptomoedas, ainda é necessário um maior esforço para identificar e punir os criminosos. A complexidade das tecnologias envolvidas e a falta de regulamentação específica são fatores que dificultam a investigação e ação contra

esses crimes.

A cooperação internacional é uma ferramenta crucial para combater organizações criminosas que utilizam criptomoedas em suas atividades ilegais. Isso ocorre porque, ao contrário das transações financeiras tradicionais, as transações com criptomoedas não são regulamentadas por um órgão centralizado e podem ocorrer de forma anônima, o que torna difícil rastrear e identificar as partes envolvidas em transações suspeitas.

No âmbito internacional, já existem iniciativas para promover a cooperação entre países na luta contra o uso indevido de criptomoedas. Um exemplo é o Grupo de Ação Financeira contra a Lavagem de Dinheiro (GAFI), que estabeleceu diretrizes para regulamentar as criptomoedas e prevenir o seu uso em atividades ilegais.

Mesmo assim, é preciso estar atento aos casos de empresas fraudulentas que utilizam criptomoedas para lesar investidores. É necessário que a sociedade e as autoridades estejam atualizadas e preparadas para lidar com os desafios impostos pelas criptomoedas e suas implicações para a segurança financeira e jurídica do país.

Discussão

Nos últimos anos, as criptomoedas têm experimentado um aumento exponencial em popularidade, tornando-se uma inovação financeira revolucionária. No entanto, com a rápida adoção dessas moedas digitais, surgem inúmeros desafios regulatórios, legais e técnicos. Enquanto muitos países têm se esforçado para atualizar suas legislações e abordar de forma efetiva os problemas emergentes associados ao uso dessas moedas digitais, o Brasil enfrenta um cenário de atraso e incertezas nessa fronteira. Os desafios são multifacetados: desde a falta de uma definição legal clara sobre o que constitui uma criptomoeda, até problemas práticos na identificação de indivíduos envolvidos em atividades ilícitas relacionadas a esses ativos. Esse panorama, caracterizado por lacunas regulatórias, problemas técnicos e ausência de especialização, dificultando a ação eficaz das autoridades. Alguns destes principais desafios podem ser notados abaixo:

• **Falta de Regulamentação Específica:** O Brasil carece de uma regulamentação específica para criptomoedas, o que deixa espaço para

interpretações diversas e cria incerteza jurídica em relação ao tratamento desses ativos. Isso dificulta a aplicação consistente da lei em casos envolvendo criptomoedas.

• **Falta de Definição Legal:** A legislação brasileira não fornece uma definição clara e abrangente do que são criptomoedas, o que pode dificultar a identificação e a classificação desses ativos em diferentes contextos legais.

• **Problemas de Identificação de Envolvidos:** A natureza pseudônima das transações com criptomoedas torna difícil a identificação dos envolvidos em crimes, como lavagem de dinheiro e fraudes. Isso cria desafios substanciais para a aplicação da lei.

• **Falta de Requisitos de Conformidade (KYC/AML):** Até recentemente, as exchanges de criptomoedas no Brasil não eram obrigadas a implementar políticas de "Conheça seu Cliente"(KYC) e medidas contra a lavagem de dinheiro (AML), o que facilitava o anonimato dos usuários e a realização de atividades ilícitas. KYC significa "Conheça Seu Cliente". É um processo que instituições financeiras e outros negócios utilizam para verificar a identidade de seus clientes. O objetivo do KYC é prevenir roubo de identidade, fraude, lavagem de dinheiro e outras atividades ilegais. Durante o processo KYC, os clientes geralmente precisam fornecer diversos documentos e informações para comprovar sua identidade. Isso pode incluir documentos de identificação emitidos pelo governo, comprovante de endereço e outras documentações relevantes.

• **Falta de Punições Adequadas:** As penalidades previstas na legislação brasileira para crimes envolvendo criptomoedas muitas vezes não são proporcionais à gravidade desses delitos, o que pode desencorajar a aplicação da lei e a busca pela punição dos infratores.

• **Desafios de Jurisdição:** Crimes envolvendo criptomoedas podem cruzar fronteiras e envolver jurisdições diferentes. A falta de acordos de cooperação internacional específicos pode dificultar a investigação e a persecução de crimes transnacionais.

• **Vulnerabilidades Técnicas:** A legislação muitas vezes não aborda as vulnerabilidades técnicas das criptomoedas, como *hacks* de *exchanges* e roubo de chaves privadas, deixando as vítimas com poucos recursos legais para recuperar

seus fundos.

• **Falta de Especialização:** A falta de especialização por parte das autoridades e tribunais em relação às criptomoedas pode resultar em interpretações inadequadas das leis existentes e dificultar a resolução eficaz de casos.

Diante do crescente protagonismo das criptomoedas no cenário financeiro global, é imperativo que o Brasil, como uma das maiores economias emergentes, esteja preparado para lidar com os desafios associados a essa inovação. Os problemas destacados, desde questões de regulamentação até vulnerabilidades técnicas, sublinham a necessidade urgente de uma abordagem proativa, informada e holística por parte das autoridades competentes. É essencial que o país avance na construção de um quadro regulatório claro, coerente e abrangente que possa não apenas proteger os consumidores e garantir a integridade do mercado, mas também fomentar a inovação e o crescimento sustentável. Adicionalmente, investir em capacitação e especialização pode proporcionar às autoridades as ferramentas necessárias para enfrentar os desafios apresentados pelas criptomoedas. A evolução é inevitável, e o Brasil deve estar posicionado na vanguarda dessa transformação, garantindo segurança, transparência e justiça para todos os envolvidos.

Propostas e Medidas

Em um mundo cada vez mais digitalizado, as criptomoedas se consolidam como um avanço tecnológico disruptivo e uma forma inovadora de realizar transações financeiras. Com seu uso crescente, também surgem desafios e preocupações associadas, desde a legitimidade das transações até questões de segurança. Portanto, é essencial adotar abordagens regulatórias e estratégicas robustas que possam alinhar a adoção das criptomoedas com a segurança, transparência e confiabilidade requeridas por usuários e instituições. A seguir, delineamos uma série de propostas e medidas destinadas a fortalecer o ecossistema de criptomoedas no país, abrangendo desde questões regulatórias até iniciativas educacionais e tecnológicas.

É importante salientar que a eficácia dessas medidas apontadas abaixo pode variar de acordo com o contexto legal e regulatório de cada país, por isso, é desta-

cada a relevância de um comitê em forma de uma cooperação internacional para uma possível padronização e assertividade nos casos de delitos e infrações envolvendo as criptomoedas.

- **Regulamentação Abrangente:** Desenvolver regulamentações específicas para o uso de criptomoedas, incluindo requisitos de identificação de usuários, relatórios de transações suspeitas e conformidade com padrões de segurança cibernética.
- **Aprimoramento da Educação e Conscientização:** Implementar programas de educação pública para aumentar a conscientização sobre os riscos associados ao uso de criptomoedas e fornecer orientações sobre como evitar golpes.
- **Cooperação Internacional:** Promover a cooperação internacional entre agências reguladoras e aplicadoras da lei para facilitar o compartilhamento de informações e investigações transfronteiriças.
- **Monitoramento de Transações Suspeitas:** Estabelecer sistemas de monitoramento de transações para identificar atividades suspeitas, incluindo análises de padrões incomuns ou volumes anormalmente altos de transações.
- **Responsabilidade das Exchanges:** Exigir que as exchanges de criptomoedas implementem políticas de KYC (*Know Your Customer*) para verificar a identidade dos usuários e relatar transações suspeitas às autoridades competentes.
- **Legislação Anti-Lavagem de Dinheiro (AML):** Reforçar as leis de AML para abranger transações com criptomoedas, garantindo que as empresas cumpram as obrigações de relatórios e due diligence (uma investigação minuciosa realizada antes de uma transação, como uma aquisição ou investimento, para confirmar detalhes e identificar possíveis riscos. Esse processo, com origens no mundo legal e financeiro, visa evitar surpresas indesejadas após a finalização da transação. A due diligence pode abranger áreas como finanças, leis, operações e conformidade. A realização adequada desse procedimento protege contra perdas, assegura a responsabilidade fiduciária e previne complicações legais.).
- **Auditorias e Conformidade de Empresas:** Realizar auditorias regulares nas exchanges de criptomoedas para garantir que elas estejam em conformidade com as regulamentações e padrões de segurança.

• **Investigação Forense Digital:** Desenvolver equipes especializadas em investigação forense digital para rastrear atividades criminosas relacionadas a criptomoedas e identificar os responsáveis.

• **Transparência Blockchain:** Promover a transparência na blockchain, permitindo que as transações sejam rastreadas enquanto se mantém o anonimato dos usuários quando apropriado.

• **Penalidades mais Rígidas:** Aumentar as penalidades para crimes envolvendo criptomoedas para desencorajar atividades ilegais e garantir uma punição adequada.

• **Desenvolvimento de Tecnologias de Segurança:** Investir em pesquisa e desenvolvimento de tecnologias de segurança cibernética para proteger as carteiras de criptomoedas e as exchanges contra ataques.

Assim, para combater o uso indevido de criptomoedas por organizações criminosas, é necessário que as autoridades de diferentes países cooperem entre si. Essa cooperação pode envolver o compartilhamento de informações e inteligência, a realização de investigações conjuntas e a criação de estratégias para prevenir e combater o uso de criptomoedas em atividades ilegais.

Além disso, é importante que os países adotem medidas para regulamentar o uso de criptomoedas e aumentar a transparência nas transações. Isso pode incluir a exigência de identificação dos usuários em transações com criptomoedas e a criação de sistemas de monitoramento para detectar transações suspeitas.

Existem vários cuidados que podem ser adotados para evitar golpes e fraudes ao realizar investimentos e compras em criptomoedas, um ponto importante é sempre fazer uma pesquisa completa sobre a criptomoeda e a empresa por trás dela antes de investir. Estando atento e desconfiando de promessas de ganhos financeiros absurdos em um curto período de tempo. É importante lembrar que os investimentos em criptomoedas são voláteis e arriscados, portanto, não há garantia de lucros. Os esquemas *Ponzi* são fraudes que prometem retornos altos e rápidos, mas são ilegais e insustentáveis. Se um investimento parecer bom demais para ser verdade, é provavelmente uma fraude. Os *phishing scams* são esquemas de fraude que tentam obter informações confidenciais do usuário, como senhas e chaves privadas, através de

e-mails ou mensagens falsas. Verifique sempre a autenticidade das informações antesde compartilhar informações pessoais. As ICOs (*Initial Coin Offerings*) são eventos de arrecadação de fundos que permitem que as empresas vendam suas criptomoedas para investidores. Verifique se a ICO é legítima, pesquisando o histórico da empresa e os detalhes do projeto antes de investir. E por ultimo mas não menos importante, atentar-se onde as criptomoedas são armazenadas (carteiras digitais), é preciso garantir que elas estejam armazenadas de forma segura. As carteiras *off-line* (ou *"cold wallets"*) são geralmente consideradas mais seguras do que as carteiras *on-line* (ou *"hot wallets"*), que estão conectadas à internet.

No entanto, a cooperação internacional pode ser dificultada pela falta de regulamentação específica sobre criptomoedas em outros países e pela falta de uniformidade nas leis e nas práticas de investigação em relação às criptomoedas. Além disso, o uso de criptomoedas pode ser utilizado para mascarar a identidade dos criminosos, dificultando ainda mais a identificação e punição.

Embora a legislação brasileira tenha avançado no combate aos crimes envolvendo criptomoedas, a falta de cooperação internacional pode limitar a sua eficácia. Portanto, é necessário um esforço conjunto de diversos países e órgãos internacionais para estabelecer uma regulamentação uniforme e garantir a cooperação internacional efetiva na identificação e punição dos criminosos que utilizam criptomoedas em atividades ilícitas.

Para tornar a punição de crimes envolvendo criptomoedas ainda mais rigorosa, é possível que o Poder Legislativo adote medidas adicionais para enfrentar essa questão. Uma dessas mendidas seria a criação de leis mais específicas para regulamentar o uso de criptomoedas em atividades criminosas, a fim de que possam ser identificadas com mais facilidade.

Outra possibilidade seria a criação de uma comissão especializada em investigar e punir crimes relacionados a criptomoedas. Essa comissão poderia ser composta por especialistas em tecnologia e finanças, bem como por representantes do Poder Judiciário e da Polícia Federal, para que fosse possível uma atuação mais eficiente na identificação e punição dos criminosos.

Aprimorar a legislação sobre a responsabilidade civil e criminal das empresas provedoras de internet também seria uma medida importante. As empresas poderiam

ser obrigadas a colaborar com as autoridades na investigação de crimes envolvendo criptomoedas e a fornecer informações necessárias para a identificação dos criminosos.

Em resumo, a punição mais rigorosa para crimes envolvendo criptomoedas passa por uma combinação de fatores, que incluem a criação de leis específicas, a criação de uma comissão especializada e o aprimoramento da legislação sobre a responsabilidade civil e criminal das empresas provedoras de internet. Dessa forma, será possível identificar e punir de forma adequada aqueles que utilizam criptomoedas em atividades criminosas.

Para o uso da *Blockchain*, é crucial estar ciente dos riscos associados, bem como das carteiras digitais. Para se blindar contra potenciais golpes e ameaças, considere as seguintes medidas de segurança:

- **Não compartilhamento de dados pessoais:** Nunca compartilhe suas informações pessoais com ninguém que você não conheça ou confie;
- ***Software* antivírus**: Instale um software antivírus em seu computador e disposi- tivo móvel e mantenha-o sempre atualizado;
- **Só use carteiras digitais de fontes confiáveis e reconhecidas**: Existem sites especializados e comunidades que avaliam e classificam carteiras digitais com base na experiência do usuário e em critérios técnicos. Alguns exemplos são o CryptoCompare e o CoinGecko, além disso, considere o tipo de carteira (carteira de hardware, desktop, móvel, web). Carteiras de *hardware*, como *Ledger Nano S* e *Trezor*, são consideradas uma das opções mais seguras.
- **Evitar investir em esquemas suspeitos**: O investimento em criptomoedas, embora promissor, vem com riscos, especialmente devido à volatilidade do mercado e à falta de regulação uniforme. Muitos golpistas atraem investidores com promessas de "lucro garantido", muitas vezes mascarando esquemas Ponzi ou pirâmides financeiras. Para proteger-se, é crucial abordar tais promessas com ceticismo, realizar pesquisas aprofundadas, buscar transparência nos projetos e se manter informado sobre as tendências do mercado. A diversificação de investimentos também é aconselhável para mitigar riscos.
- **Se suspeitar que foi vítima de algum golpe, é crucial denunciar o incidente às autoridades competentes imediatamente:** Comece registrando um

boletim de ocorrência na delegacia de polícia mais próxima. Eles podem direcioná-lo para um departamento especializado, se houver. Alguns países têm órgãos ou agências reguladoras financeiras que lidam com fraudes e golpes. Por exemplo, nos EUA, pode-se entrar em contato com a Comissão de Valores Mobiliários (SEC) para denunciar fraudes relacionadas a investimentos, além disso, mante- nha sempre *softwares* antivírus e de proteção atualizados em seus dispositivos, e considere usar serviços de monitoramento que alertem sobre atividades suspeitas em suas contas.

Embora a *Blockchain* e as criptomoedas ofereçam oportunidades inovadoras, é essencial adotar uma postura proativa em relação à segurança. Ao seguir as medidas acima, os usuários podem navegar pelo universo das criptomoedas com confiança e proteção.

CONCLUSÃO

As criptomoedas, sem dúvida, reinventaram o universo financeiro no século XXI, oferecendo sistemas financeiros mais rápidos e transparentes. No entanto, o Brasil, como parte integrante do cenário financeiro global, enfrenta desafios de integridade e segurança, em especial quando abordamos o tema "Crimes Cibernéticos com Criptomoedas". Uma análise detalhada da legislação brasileira neste contexto revela tanto avanços quanto áreas carentes de atenção.

Em primeiro lugar, é essencial reconhecer que a natureza dinâmica e global das criptomoedas demanda uma abordagem legislativa ágil. A legislação brasileira precisa ser robusta, mas flexível, capaz de se adaptar às novas modalidades de crimes cibernéticos relacionados a criptomoedas que emergem rapidamente. As propostas e medidas delineadas anteriormente, incluindo regulamentação abrangente e monitoramento de transações suspeitas, são imperativas para criar uma barreira legislativa contra ações criminosas.

Além disso, a cooperação internacional é crucial. Os crimes cibernéticos não respeitam fronteiras e, muitas vezes, envolvem atores de diversos países. O Brasil deve fortalecer seus laços com agências reguladoras internacionais, promovendo o compartilhamento de informações e facilitando investigações transfronteiriças. Um esforço coordenado no âmbito global pode ser um poderoso dissuasor contra atividades

ilícitas envolvendo criptomoedas.

A transparência é a espinha dorsal de qualquer sistema que busca combater a ilegalidade. Assim, incentivar a transparência na *blockchain*, permitindo que transações sejam rastreadas mantendo o anonimato adequado dos usuários, é essencial. É imperativo que a legislação brasileira fortaleça os mecanismos que possibilitem a identificação rápida e eficaz de padrões suspeitos ou irregulares, ao mesmo tempo que se protege a privacidade legítima dos cidadãos.

Em relação às medidas punitivas, o sistema legal brasileiro precisa estabelecer penalidades mais rigorosas para crimes envolvendo criptomoedas. A gravidade desses crimes, que podem afetar milhares de pessoas e desestabilizar sistemas financeiros, justifica a necessidade de uma resposta legislativa firme. Esta abordagem não só atuará como um desincentivo para os infratores, mas também reforçará a confiança do público nas criptomoedas como um meio legítimo de transação.

Educação e conscientização também são fundamentais. Embora o foco esteja, compreensivelmente, nos aspectos legislativos e regulatórios, é essencial que o público em geral, bem como os profissionais do setor, estejam cientes dos riscos associados e saibam como identificar e prevenir possíveis ameaças. Investir em programas educacionais e de conscientização, portanto, não é apenas uma medida preventiva, mas um pilar para o desenvolvimento seguro das criptomoedas no Brasil.

Concluindo, enquanto as criptomoedas representam uma inovação revolucionária, elas também introduzem novos desafios no combate aos crimes cibernéticos. A legislação brasileira, embora tenha feito avanços significativos, ainda tem um longo caminho a percorrer. Através de uma combinação de regulamentação rigorosa, cooperação internacional, medidas punitivas apropriadas e educação, o Brasil pode não apenas enfrentar, mas também liderar globalmente na abordagem de crimes cibernéticos relacionados a criptomoedas.

REFERÊNCIAS

ANDRADE, A. G. C. de; CASTRO, R. R. M. de. Lavagem de dinheiro no Brasil: evolução legislativa e criminalidade organizada. **Revista de Direito Penal**, n. 27, p. 1-13, 2007.

CAMPOS, L.; MONTEIRO, R.; RODRIGUES, V. **Criptomoedas**: um estudo sobre a tecnologia, o mercado e a regulação. São Paulo: Novas Edições Acadêmicas, 2018.

CHRISTIN, N.; HOULE, J. Tracking Ransomware End-to-End. **IEEE Security and Privacy**, v. 17, n. 6, p. 40-47, 2019.

FRANKENFIELD, J. **What Are Cryptocurrencies?** 2023. Disponível em: https://www.investopedia.com/terms/c/cryptocurrency.asp.

GORDON, S.; FORD, R. On the Definition and Classification of Cybercrime. **Springer: J Comput Virol**, v. 2, p. 13–20, 2006.

KARLOV, D. S.; DERKACH, A. S. Cryptocurrency as an object of criminological analysis: typology of illegal actions. **International Journal of Law and Management**, v. 62, n. 6, p. 1078-1091, 2020.

KSHETRI, N. Blockchain's roles in meeting key supply chain management objectives. **International Journal of Information Management**, v. 39, p. 80-89, 2018.

MORAES, V.; SALOMÃO, R. **Criptomoedas**: aspectos técnicos, econômicos, jurídicos e regulatórios. Rio de Janeiro: Elsevier, p. 12-19, 2020.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. **White Paper: Bitcoin**, p. 1-9, 2008.

PIZZETTI, F. V. **A volatilidade das criptomoedas**: um estudo com utilização de modelos GARCH. Dissertação (Mestrado em Economia) - Universidade do Extremo Sul Catarinense, p 12-55, 2018.

PREVIDI, G. de S. **Descentralização monetária**: um estudo sobre o Bitcoin. Porto Alegre: UFRGS Repositório Digital, p. 7-50, 2014.

RANSBOTHAM, S.; MITRA, S. Blockchain: Promise, Practice, and Application to Cybersecurity. **Journal of Management Information Systems**, v. 36, n. 3, p. 675-702, 2019.

RASS, S.; IVANOV, M. Cryptocurrency Transactions as a Tool for Cybercrime. **Journal of Cybersecurity**, v. 5, n. 1, p. 1-13, 2019.

TURCHAK, O. Cryptocurrencies and Cybercrime: a Review. **Journal of Money Laundering Control**, v. 21, n. 4, p. 436-450, 2018.

ULRICH, F. **Bitcoin**: A Moeda na Era Digital. São Paulo: Instituto Ludwig Von Mises Brasil, p. 5-92, 2014.

VASEK, M. *et al.* Crime and Crypto: An Analysis of the Cryptocurrency-Enabled Cybercrime Landscape. **ACM Transactions on Internet Technology**, v. 21, n. 2, p. 1-28, 2021.

VADE Mecum: Constituição Federal e Códigos. 35. ed. São Paulo: Saraiva, 2023.

VADE Mecum: Constituição Federal e Códigos. 28. ed. São Paulo: Saraiva, 2019.

ANEXO 01

LEI Nº 9.613 DE 03 DE MARÇO DE 1998

"Dispõe sobre os crimes de lavagem ou ocultação de bens, direitos e valores, a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta lei; cria o conselho de controle de atividades financeiras - coaf, e dá outras providências."

LEI Nº 12.737 DE 30 DE NOVEMBRO DE 2012

"Dispõe sobre a tipificação criminal de delitos informáticos; altera o decreto-lei nº 2.848, de 7 de dezembro de 1940 – código penal; e dá outras providências."

LEI Nº 12.965 DE 23 DE ABRIL DE 2014

"Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil."

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

"Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)."

RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018

"Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil."

LEI Nº 13.964 DE 24 DE DEZEMBRO DE 2019

"Aperfeiçoa a legislação penal e processual penal"

INSTRUÇÃO NORMATIVA RFB Nº 1.888/2019

"Esta Instrução Normativa institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB)."

LEI Nº 14.478 DE 21 DE DEZEMBRO DE 2022

"Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições."