

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
WIDENER UNIVERSITY DELAWARE LAW SCHOOL
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE Mestrado em Ciência Jurídica – CMCJ
ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO
LINHA DE PESQUISA: DIREITO, JURISDIÇÃO E INTELIGÊNCIA ARTIFICIAL
PROJETO DE PESQUISA: DIREITO E INTELIGÊNCIA ARTIFICIAL
DISSERTAÇÃO EM REGIME DE DUPLA TITULAÇÃO

A LAVAGEM DE DINHEIRO E A EVASÃO DE DIVISAS PELO CRIPTOATIVO

EDUARDO HENRIQUE TENSINI

Itajaí-SC, junho de 2023

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
WIDENER UNIVERSITY DELAWARE LAW SCHOOL
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ
ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO
LINHA DE PESQUISA: DIREITO, JURISDIÇÃO E INTELIGÊNCIA ARTIFICIAL
PROJETO DE PESQUISA: DIREITO E INTELIGÊNCIA ARTIFICIAL
DISSERTAÇÃO EM REGIME DE DUPLA TITULAÇÃO

A LAVAGEM DE DINHEIRO E A EVASÃO DE DIVISAS PELO CRIPTOATIVO

EDUARDO HENRIQUE TENSINI

Dissertação submetida ao Curso de Mestrado em
Ciência Jurídica da Universidade do Vale do Itajaí –
UNIVALI, como requisito parcial à obtenção do título
de Mestre em Ciência Jurídica. Em dupla titulação
com a *Widener University Delaware Law School*.

Orientador: Professor Doutor Orlando Luiz Zanon Junior

Itajaí-SC, abril de 2023

AGRADECIMENTOS

Gostaria de expressar meus sinceros agradecimentos às pessoas e aos professores, servidores e amigos da Univali e Delaware Law School, que tornaram possível a realização desta dissertação de mestrado.

À minha família, sempre presente em todos os momentos da minha vida, apoiando e incentivando a minha jornada acadêmica, agradeço o amor, paciência, compreensão e suporte incondicional fornecidos. Sem a ajuda de vocês, esta conquista não seria possível.

Ao meu professor orientador, Doutor Orlando Luiz Zanon Junior, que dedicou seu tempo, conhecimento e habilidades em guiar-me ao longo deste trabalho. Sua paciência, motivação e sabedoria foram fundamentais para o sucesso deste estudo. Agradeço pelas críticas construtivas, conselhos valiosos e incentivos dados.

Ao meu tio, Antônio Carlos Rosa, advogado, que exerce a profissão com louvor e amor.

E por fim, agradeço a Deus pela oportunidade de estar aqui hoje, pela saúde, discernimento e perseverança que me foram dados. Sem a Sua orientação, nada seria possível. Obrigado por me guiar em cada passo deste caminho, pela força para superar as dificuldades e pelas bênçãos que me foram concedidas.

A todos que, de alguma forma contribuíram para a realização deste trabalho, meu muito obrigado.

DEDICATÓRIA

Dedico esta dissertação aos meus amados pais, Henrique e Márcia, que sempre me apoiaram e me deram forças para buscar os meus sonhos, mesmo nos momentos mais difíceis. Agradeço por todo o amor, dedicação e incentivos proporcionadas ao longo da minha vida. Sem vocês, eu não seria quem hoje sou.

À minha esposa, agradeço por estar ao meu lado, me amparando em cada passo deste caminho. Obrigado por compartilhar comigo suas ideias, paciência e amor. Sua presença foi fundamental para a realização deste trabalho.

À minha querida avó, Sônia Alexandrina Rosa, que sempre me inspirou com sua sabedoria e bondade, mas que hoje descansa ao lado do Pai, agradeço pelo exemplo de coragem, perseverança e amor pela vida.

A todos vocês, meu eterno agradecimento. Esta conquista é nossa!

TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando a Universidade do Vale do Itajaí, a Coordenação do Curso de Mestrado em Ciência Jurídica, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Itajaí-SC, abril 2023

**EDUARDO HENRIQUE
TENSINI:06501922909**

Assinado de forma digital por
EDUARDO HENRIQUE
TENSINI:06501922909
Dados: 2023.06.01 15:42:27 -03'00'

**Eduardo Henrique Tensini
Mestrando**

PÁGINA DE APROVAÇÃO

MESTRADO

Conforme Ata da Banca de Defesa de Mestrado, arquivada na Secretaria do Programa de Pós-Graduação *Stricto Sensu* em Ciência Jurídica PPCJ/UNIVALI, em 20/04/2023, às 10h, o mestrando Eduardo Henrique Tensini fez a apresentação e defesa da Dissertação, sob o título "A LAVAGEM DE DINHEIRO E A EVASÃO DE DIVISAS PELO CRIPTOATIVO".

A Banca Examinadora foi composta pelos seguintes professores: Doutor Orlando Luiz Zanon Junior (UNIVALI), como presidente e orientador, Doutor Alejandro Knaesel Arrabal (FURB), como membro, Doutor Alexandre Morais da Rosa (UNIVALI), como membro e Doutor Gilson Jacobsen (UNIVALI), como membro suplente. Conforme consta em Ata, após a avaliação dos membros da Banca, a Dissertação foi aprovada.

Por ser verdade, firmo a presente.

Itajaí (SC), 20 de abril de 2023.



PROF. DR. PAULO MÁRCIO DA CRUZ
Coordenador/PPCJ/UNIVALI

ROL DE ABREVIATURAS E SIGLAS

AML	Anti-Money Laundering
ANOREG	Associação dos Notários e Registradores do Brasil
BC	Banco Central
BCB	Banco Central do Brasil
BCCI	Bank of Credit and Commerce International
BSA	Bank Secrecy Act - Lei de Sigilo Bancário Norte Americano
CFTC	Commodity Futures Trading Commission
CIA	Central Intelligence Agency
CMN	Conselho Monetário Nacional
COAF	Conselho de Controle de Atividade Financeiras
CVM	Comissão de Valores Mobiliários
DEA	Drug Enforcement Administration
DeFi	Decentralized Finance
Dex	Decentralized Exchanges
DHS	Department of Homeland Security
DLT	Distributed Ledger Technology
DOC	Documento de ordem de crédito
DOJ	Department of Justice
EUA	Estados Unidos da América
FBI	Federal Bureau of Investigation
FED	Federal Reserve Bank
FinCEN	Financial Crimes Enforcement Network
FSB	Financial Stability Board
GAFI	Grupo de Ação Financeira
GAO	Government Accountability Office
HC	Habeas Corpus
ICOs	Initial Coin Offering
IRS	Internal Revenue Service
KYC	Know Your Customer
MPRS	Ministério Público do Estado do Rio Grande do Sul
MPSC	Ministério Público do Estado de Santa Catarina
NFT	Non-Fungible Token

OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ONU	Organização das Nações Unidas
OTC	Over The Counter
P2P	Peer-to-peer
PF	Polícia Federal
PIB	Produto Interno Bruto
PIC	Procedimento Investigatório Criminal
PIX	Pagamento Instantâneo Brasileiro
PL	Projeto de Lei
RFB	Receita Federal do Brasil

ROL DE CATEGORIAS

Criptoativo: Os criptoativos são símbolos de valores que possuem existência exclusivamente em registros digitais. Os ativos digitais abrangem diversos tipos de ativos, sendo que os criptoativos englobam todos eles. A negociação desses símbolos ocorre diretamente entre pessoas ou empresas, sem a necessidade de uma instituição financeira intermediária. De acordo com a Receita Federal, um criptoativo é uma forma digital de representar valor, com sua própria unidade de conta, cujo preço pode ser expresso em moeda local ou estrangeira. Ele é negociado eletronicamente, utilizando criptografia e tecnologias de registros distribuídos. Os criptoativos podem ser utilizados como investimento, para transferência de valores ou acesso a serviços, mas não são considerados moeda de curso legal. Esses ativos são intangíveis, ou seja, não possuem uma forma física. Entre os diversos ativos digitais que englobam a categoria criptoativo, encontram-se as criptomoedas, tornando-as um subconjunto específico de criptoativos. Outros exemplos de ativos desse tipo incluem propriedade intelectual, patentes e marcas. Criptoativo é um ativo digital que se estabeleceu em um sistema de pagamento online que emprega criptografia para proteger as transações, em vez de depender de uma autoridade central. Existem vários tipos de criptoativos no mercado hoje. Algumas das variedades mais populares são as criptomoedas Bitcoin, Ether (Ethereum), Tether, Binance Coin e USD Coin. As criptomoedas são classificadas como moedas ou tokens. Tokens são ativos digitais mantidos no banco de dados blockchain, enquanto moedas como Bitcoin e *altcoins* possuem seu próprio blockchain. Os tokens ERC-20¹ seguem um padrão que permite aos desenvolvedores projetar tokens utilizáveis que rodam na rede Ethereum. As *altcoins* servem para outros usos além da moeda digital, enquanto as *stablecoins* são criptomoedas cujos valores estão atrelados aos preços de outros ativos. Assim, criptoativo é categoria, subdivido em vários ativos digitais que possuem

¹ Os tokens ERC-20 são um tipo de ativo digital ou criptomoeda que segue um conjunto de padrões conhecido como padrão ERC-20. O termo "ERC-20" significa "Ethereum Request for Comment 20", que se refere à proposta técnica específica ou protocolo de padronização desenvolvido para tokens na blockchain Ethereum.

características descentralizada, baseada na tecnologia blockchain, não emitido por uma autoridade central, tornando-o teoricamente imune à intervenção estatal.²

Criptomoeda: Criptomoeda é uma subcategoria de criptoativo e é definida como uma forma de moeda digital ou virtual que utiliza criptografia para assegurar transações seguras. Ao contrário das moedas convencionais, as criptomoedas não são controladas por uma autoridade central para emissão ou regulação. Em vez disso, são baseadas em um sistema descentralizado que registra transações e introduz novas unidades. As criptomoedas operam como um sistema de pagamento digital que dispensa a necessidade de bancos para verificar e confirmar transações. Funcionam em um modelo ponto a ponto, possibilitando que indivíduos enviem e recebam pagamentos de qualquer lugar. Em vez de existirem fisicamente, as transações com criptomoedas são registradas apenas como registros digitais em um banco de dados online que documenta as transações específicas. Quando há uma transferência de fundos em criptomoeda, as transações são registradas em um livro-razão público (blockchain). As criptomoedas são armazenadas em carteiras digitais, permitindo que os usuários tenham controle sobre seus próprios ativos e possam utilizá-los em diversas transações online.³

Direito Penal Econômico: O Direito Penal Econômico é considerado uma vertente do Direito Penal, que se dedica ao estudo, regulamentação e aplicação das leis que regem os crimes cometidos contra a ordem econômica. O Direito Penal Econômico tem como objetivo salvaguardar a atividade econômica presente e desenvolvida no contexto de uma economia de livre mercado. Ele faz parte do Direito Penal como um todo, não possuindo autonomia científica, mas sim metodológica ou didático-pedagógica, devido à especificidade do seu objeto de proteção e à natureza particular da intervenção penal. Ao definir o Direito Penal Econômico, JESCHECK⁴ descreve que trata-se de um ramo do Direito Penal que visa coibir condutas que prejudicam o conjunto da economia como um todo. Com efeito, é uma ramificação

² ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasoç. 2014.

³ KASPERSKY. **O que é criptomoeda e como funciona?** Disponível em: <<https://www.kaspersky.com.br/resource-center/definitions/what-is-cryptocurrency>>, acesso em 28/05/2023.

⁴ JESCHECK, Hans-Heinrich; WEIGEND, Thomas. **Tratado de derecho penal: Parte general**. 5. ed. atual. e ampl. Trad. Miguel Olmedo Cardenete. Granada: Colmares, 2002.

que se concentra em proteger a ordem socioeconômica através do controle estatal da economia, sendo uma forma intensa de intervenção estatal. Diferente do Direito Financeiro ou do Direito Tributário, o Direito Penal Econômico é uma especialização do Direito Penal. Os crimes econômicos intentam afetar bens e interesses coletivos, como o funcionamento regular da econômica nacional, circulação e consumo de riqueza. Desse modo, o Direito Penal Econômico consiste em um conjunto de regras que tem como objetivo punir condutas que, no contexto das relações econômicas, colocam em risco bens ou interesses juridicamente protegidos, utilizando para isso as penalidades próprias. Logo, o Direito Penal Econômico atua como um sistema normativo que protege a política econômica do Estado, proporcionando meios para que esta possa ser efetivamente realizada.⁵⁶

Evasão de divisas: Evasão de divisas é um crime contra o sistema financeiro nacional, através do qual o agente envia divisas ao exterior, sem declará-las à repartição federal competente, repercutindo, em regra, na ausência de pagamento de tributos devidos. A evasão ocorrerá quando, de alguma forma, as reservas monetárias são remetidas ao exterior, geralmente a paraísos fiscais, em nome das pessoas físicas ou jurídicas ou, ainda, para *offshores* lá constituídas.⁷

Lavagem de dinheiro: O crime de lavagem de dinheiro caracteriza-se por um conjunto de operações comerciais ou financeiras que buscam a incorporação na economia de cada país, de modo transitório ou permanente, de recursos, bens e valores de origem ilícita e que se desenvolvem por meio de um processo dinâmico que envolve, teoricamente, três fases independentes que, com frequência, ocorrem simultaneamente⁸. De acordo com CALLEGARI e WEBER⁹ a expressão utilizada no Brasil para definir o delito é Lavagem de Dinheiro. A palavra lavar vem do latim *lavare*, e significa expurgar, purificar, reabilitar, daí a ideia de tornar lícito o dinheiro

⁵ CALLEGARI, André Luís. Direito penal econômico e lavagem de dinheiro: aspectos criminológicos. Porto Alegre: Livraria do Advogado, 2003.

⁶ PIMENTEL, Manoel Pedro. **Direito penal econômico**. São Paulo: Revista dos Tribunais, 1973.

⁷ NUNES, Leandro Bastos. **Evasão de Divisas**. Editora Juspodivm, 2017.

⁸ BRASIL. FAZENDA. **Prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo**. Disponível em: <<http://www.fazenda.gov.br/assuntos/prevencao-lavagem-dinheiro>>, acesso em 27/01/2022.

⁹ CALLEGARI, André Luís; WEBER, Ariel Barazzetti. **Lavagem de dinheiro**. 2. ed. São Paulo: Atlas, 2017. p. 20.

advindo de atividades ilegais e reinseri-lo no mercado como se lícito fosse. Levando em conta que o delito representa a transformação. Outros países utilizam palavras que etimologicamente significam limpeza.

Non fungible token: Um token não fungível (NFT) é um ativo digital único sem existência física ou valor intrínseco. Os NFTs, ao contrário das criptomoedas fungíveis como o Bitcoin, não podem ser duplicados, trocados ou subdivididos, tornando-os não intercambiáveis. Os NFTs são emitidos em redes blockchain como a Aptos e podem ser acessados por meio de carteiras como a Petra. Eles têm um valor monetário baseado em sua popularidade e podem representar tesouros digitais, arte e outros produtos únicos. Os NFTs podem ser gerados, armazenados e movidos entre redes blockchain, e sua propriedade e histórico de transações são mantidos no blockchain sem o uso de um intermediário terceirizado.¹⁰

Token de pagamento: Um token de pagamento é um tipo de ativo digital ou criptomoeda que se destina a ser usado como meio de troca de bens e serviços. Os tokens de pagamento são projetados principalmente para facilitar transações e pagamentos entre as partes. Para proteger e verificar as transações, esses tokens são construídos em blockchain ou tecnologia de contabilidade distribuída. Eles podem ser usados para transferir valor eletronicamente de maneira descentralizada, eliminando a necessidade de intermediários como bancos ou processadores de pagamento. Exemplos de tokens de pagamento populares incluem Bitcoin (BTC) e Litecoin (LTC).

Token de utilidade: Um token de utilidade é uma espécie de criptoativo gerado em um blockchain que serve a um propósito específico dentro de seu ecossistema. Os tokens de utilidade, ao contrário das criptomoedas típicas, como o Bitcoin, não se destinam a ser um meio de comércio ou uma reserva de valor. Em vez disso, eles fornecem aos consumidores acesso a serviços ou produtos em uma plataforma baseada em blockchain e podem fornecer recursos adicionais, como direitos de voto, prêmios de jogos e pagamento de taxas de rede. Os tokens de utilidade são

¹⁰ WEBSTER. **Non fungible token.** Disponível em: <<https://www.merriam-webster.com/dictionary/non-fungible%20token>>, acesso em 28/05/2023.

pré-minerados e específicos para seu ecossistema. Basic Attention Token (BAT), Chainlink (LINK) e 0x (ZRX) são exemplos de tokens de utilidade populares.¹¹

Token Referenciado: Um token referenciado a ativo, também conhecido como asset-backed token, é uma representação digital de um ou mais ativos, sejam eles tangíveis ou intangíveis. Esses tokens podem abranger diferentes tipos, como os "security tokens", as stablecoins, os non-fungible tokens (NFTs) e outros ativos que são objeto de operações de "tokenização".

¹¹ ACADEMY. **What is a Utility Token?** Disponível em: <<https://academy.bit2me.com/en/que-es-utility-token/>>, acesso em 28/05/2023.

SUMÁRIO

RESUMO.....	XVI
RESUMO EM LINGUA ESTRANGEIRA	XVII
INTRODUÇÃO	18
CAPÍTULO 1	23
O AVANÇO TECNOLÓGICO E O DIREITO PENAL ECONÔMICO	23
1.1 SUSCINTA INTRODUÇÃO DO DIREITO PENAL ECONÔMICO E SUAS PREOCUPAÇÕES COM O RISCO SISTÊMICO	23
1.2 CONTEXTUALIZAÇÃO HISTÓRICA E JURÍDICA DA LAVAGEM DE CAPITAIS NO MUNDO, EM ESPECIAL NOS ESTADOS UNIDOS DA AMÉRICA E BRASIL	34
1.3 DEFINIÇÃO DA CONDUTA EVASÃO DE DIVISAS	41
1.4 CONCEITUAÇÃO JURÍDICA E TECNOLÓGICA DOS CRIPTOATIVOS	45
1.4.1 O CONTROLE DESCENTRALIZADO	49
1.4.2 EXCHANGES	51
1.4.3 LEI 14.478/22 – MARCO LEGAL DO CRIPTOATIVO	52
1.4.4 PARECER DE ORIENTAÇÃO CVM 40	53
1.4.5 BLOCKCHAIN	55
CAPÍTULO 2	58
A LIGAÇÃO DA TECNOLOGIA BLOCKCHAIN E TIPOS PENAIS.....	58
2.1 FASE INVESTIGATÓRIA: A IMPORTÂNCIA DO MONITORAMENTO POLICIAL DO MERCADO NÃO REGULADO DOS CRIPTOATIVOS	58
2.2 O AUMENTO DA POPULARIZAÇÃO DOS CRIPTOATIVOS E A CORRELAÇÃO COM A ATIVIDADE CRIMINAL.....	67
2.3 O FINANCIAMENTO DE NARCÓTICOS NA DEEP WEB ATRAVÉS DA CRIPTOMOEDA	81
2.4 A MODALIDADE DE TRANSFERÊNCIA DE BITCOIN P2P E O DESAPARECIMENTO DE BARREIRAS FINANCEIRAS GOVERNAMENTAIS ...	91
CAPÍTULO 3	97
INTERVENÇÕES LEGAIS NO AVANÇO DO MERCADO ILÍCITO DE CRIPTOATIVOS.....	97
3.1 O ENTENDIMENTO DOS TRIBUNAIS SUPERIORES SOBRE OS TIPOS PENAI QUE ENVOLVEM CRIPTOATIVOS	97

3.2 A RELAÇÃO ENTRE OS JULGADOS NACIONAIS E A JURISDIÇÃO AMERICANA.....	110
3.3 PREVENÇÃO E COMBATE A LAVAGEM DE CAPITAL ATRAVÉS DO CRIPTOATIVO	121
CONSIDERAÇÕES FINAIS	136
REFERÊNCIA DAS FONTES CITADAS.....	147

RESUMO

Cuida-se de pesquisa com intuito de apurar como a prática criminosa de lavagem de dinheiro processa-se pelos criptoativos. Ademais, inferir se a conduta de evasão de divisas pode ser tipificada pelo criptoativo e quais as dissemelhanças regulamentárias e legislativas entre a jurisdição norte americana e brasileira. Com efeito, a presente Dissertação está inserida na Linha de Pesquisa Direito, Jurisdição e Inteligência artificial. Foi destacado, durante a investigação, que os criptoativos transformaram o setor financeiro, criando oportunidades para lavagem de dinheiro e evasão de divisas. As transações envolvendo criptoativos, especialmente criptomoedas são anônimas e, ao contrário do sistema bancário tradicional, podem ser difíceis de rastrear e inacessíveis ao judiciário, tornando-se atraentes para criminosos que buscam ocultar suas atividades financeiras. O capítulo 1 ocupou-se em definir os conceitos operacionais. No capítulo 2 evidenciou-se que as criptomoedas se volveram numa ferramenta notável para lavagem de dinheiro, evasão fiscal e financiamento de atividades terroristas. Além disso, destacou-se que são utilizadas para comprar bens ilícitos e serviços ilegais. Destarte, no capítulo 3 consignou-se que à medida que os governos e autoridades legais obtêm informações sobre o uso de criptoativos para atividades criminosas, medidas são tomadas para reprimir aqueles que utilizam essa nova tecnologia para lavagem de dinheiro e evasão fiscal. Ademais, identificou-se que criptoativos e financiamento criminal são temas correlatos, porquanto com surgimento de moedas digitais como Bitcoin e Ethereum, empreendedores do submundo criminoso empregaram novos métodos para financiar atividades ilegais, ocultar bens e burlar a aplicação da lei. Explorou-se que, as criptomoedas, tipo de criptoativo, são frequentemente utilizadas para apoiar atividades ilegais, como a venda de substâncias ilícitas na *deep web* e *dark web*, fraudes monetárias e financiamento ao terrorismo. Ainda, revelou-se as dessemelhanças entre as jurisdições, especialmente o sistema regulamentário americano e brasileiro. Afinal, atingiu-se que a lavagem de dinheiro ocorre com o criptoativo, notadamente com a criptomoeda, e que a evasão de divisas, considerando o Parecer nº 40 da CVM e a depender do caso concreto, pode ser tipificado. Ainda, pormenorizou-se as dissimilitudes entre a aplicação da lei no território norte americano e brasileiro. Para alcançar as conclusões citadas, o presente trabalho utilizou o método indutivo na fase de investigação, o método cartesiano na fase de tratamento de dados e a base lógica indutiva para compor o relatório dos resultados da dissertação.

Palavras-chave: Lavagem de dinheiro, Evasão de Divisas, Criptoativo, Direito Penal Econômico.

RESUMO EM LINGUA ESTRANGEIRA

This research aims to find out how the criminal practice of money laundering is carried out by crypto assets. It also infers whether the conduct of currency evasion can be typified by the crypto asset and what are the regulatory and legislative dissimilarities between the North American and Brazilian jurisdictions. This Dissertation is part of the Line of Research Law, Jurisdiction and Artificial Intelligence. It was highlighted during the investigation that crypto assets have transformed the financial sector, creating opportunities for money laundering and currency evasion. Transactions involving cryptoassets, especially cryptocurrencies, are anonymous and, unlike traditional banking, can be difficult to trace and inaccessible to the judiciary, making them attractive to criminals looking to hide their financial activities. Chapter 1 defines the operational concepts. Chapter 2 shows that cryptocurrencies have become a notable tool for money laundering, tax evasion and financing of terrorist activities. It also highlights the use of cryptocurrencies to purchase illicit goods and illegal services. Chapter 3 states that as governments and legal authorities obtain information about the use of crypto assets for criminal activities, measures are taken to repress those who use this new technology for money laundering and tax evasion. It was also identified that the themes of crypto assets and criminal financing are related, since with the emergence of digital currencies such as Bitcoin and Ethereum, entrepreneurs in the criminal underworld have employed new methods to finance illegal activities, hide assets and evade law enforcement. The study explores how cryptocurrencies, a type of cryptoasset, are often used to support illegal activities, such as the sale of illicit substances on the deep web and dark web, currency fraud and terrorist financing. The dissimilarities between the jurisdictions – especially the American and Brazilian regulatory systems – are highlighted. In conclusion, it was found that money laundering occurs with cryptoassets, notably with cryptocurrencies, and that currency evasion, considering CVM Opinion No. 40 and depending on the specific case, can be typified. The dissimilarities between the application of the law in North America and Brazil are detailed. To reach the aforementioned conclusions, this work uses the inductive method in the investigation phase, the Cartesian method in the data treatment phase and the inductive logic base to compose the report of results.

Keywords: Money Laundering, Currency Evasion, Cryptoasset, Economic Criminal Law.

INTRODUÇÃO

O objetivo institucional da presente Dissertação é a obtenção do título de Mestre em Ciência Jurídica pelo Curso de Mestrado em Ciência Jurídica da Univali com dupla titulação na Widener University – Delaware Law School.

O seu objetivo científico é identificar, analisar e compreender como a evolução tecnológica, através da tecnologia blockchain e criptoativos, se correlaciona a delitos econômicos. Ademais, analisar se as organizações criminosas se adaptaram ao novo modelo de negócios e se as respostas do Estado, tanto no Brasil quanto nos Estados Unidos, acompanharam essa evolução. Por último, detalhar o crime de lavagem de dinheiro, suas etapas e discutir se a conduta de evasão de divisas está relacionada a esse assunto, considerando a posição dos tribunais superiores.

A importância temática da pesquisa advém da carência de regulamentação clara e específica sobre criptoativos em diversas nações, o que dificulta o rastreamento e monitoramento das transações e fluxo de recursos nestas moedas digitais pelas autoridades competentes. A lavagem de dinheiro e evasão de divisas não afetam apenas o ramo do Direito Penal, mas a integridade do sistema financeiro como um todo, podendo ainda serem utilizadas para financiar atividades criminosas como o tráfico de drogas, terrorismo e corrupção.

Para a pesquisa foram levantadas as seguintes hipóteses:

a) Quais fases caracterizam a lavagem de dinheiro pelo criptoativo?

A lavagem de dinheiro, enquanto fenômeno criminoso, consiste na conduta do agente de ocultar ou dissimular o produto proveniente da prática ilícita, e trata-se de uma prática antiga. A lavagem de capitais é tradicionalmente descrita como um processo que envolve três etapas (colocação, ocultação e integração), em que um indivíduo, seja ele pessoa física ou jurídica, procura disfarçar a origem ilícita dos recursos para que aparentem ser lícitos.

A primeira etapa desse processo, conhecida como colocação, envolve a inserção do dinheiro ilegal no sistema financeiro. Essa etapa pode ser realizada de diversas maneiras, tais como através da compra de bens como propriedades, imóveis ou obras de arte, por exemplo. A terceira e última fase é a integração, momento em que o autor do crime insere o produto do ilícito no mercado. A fase de ocultação é uma das etapas da lavagem de dinheiro em que o perpetrador busca esconder a origem ilícita dos recursos por meio de transações complexas e obscuras. Quando se trata de lavagem de dinheiro com criptoativos, essa fase pode envolver a utilização de tecnologias como a blockchain para dificultar a rastreabilidade das transações.

Dessa forma, é possível identificar que a aquisição de criptoativos com o intuito de lavar dinheiro deve, em tese, passar por pelo menos duas fases, ou seja, a ocultação ou dissimulação e a integração.

b) A conduta prevista no art. 22 da Lei n.º 7.492/86, denominada evasão de divisas, pode ser atribuída ao criptoativo?

Conforme o disposto no artigo 22 da Lei nº 7.492/1986, constitui crime a realização de operação de câmbio não autorizada com o intuito de promover a evasão de divisas do país. Tal conduta é sancionada com a pena de reclusão, de dois a seis anos, além de multa. O parágrafo único do referido artigo dispõe que incorre na mesma pena quem, sem autorização legal, promove a saída de moeda ou divisa para o exterior ou mantém depósitos não declarados à repartição federal competente.

Nesse sentido, o legislador estabelece que a prática criminosa ocorre quando há remessa de reservas monetárias para o exterior, conforme o termo utilizado pelo dispositivo legal em questão. Todavia, considerando que a lei penal em branco exige complementação normativa, a omissão do legislador quanto ao conceito jurídico do criptoativo no Brasil impede a caracterização do crime em questão, tendo em vista que não há clareza quanto à natureza jurídica dessa modalidade de ativo digital.

c) Qual é a dissemelhança entre o ordenamento jurídico brasileiro e norte-americano concernente à prevenção e combate ao crime econômico, especialmente àquele praticado com ativos digitais?

Existem algumas diferenças significativas entre o ordenamento jurídico brasileiro e norte-americano em relação à prevenção e combate ao crime econômico, especialmente aquele praticado com ativos digitais. Em primeiro lugar, é importante destacar que os Estados Unidos têm uma legislação mais abrangente e específica em relação a crimes financeiros, incluindo a lavagem de dinheiro e o uso de criptomoedas para fins ilícitos.

Nos Estados Unidos, a Financial Crimes Enforcement Network (FinCEN) é responsável por regulamentar e fiscalizar atividades financeiras que possam estar relacionadas a crimes econômicos. Além disso, as agências reguladoras e as autoridades de aplicação da lei têm amplos poderes para investigar e processar indivíduos e empresas envolvidos em crimes financeiros.

Já no Brasil, embora existam leis que tratam de crimes financeiros, como a Lei de Lavagem de Dinheiro e a Lei de Crimes contra o Sistema Financeiro Nacional, ainda há uma lacuna regulatória em relação às criptomoedas. Embora o Banco Central e a Comissão de Valores Mobiliários (CVM) tenham emitido algumas orientações sobre o uso de criptomoedas, ainda não há uma regulamentação específica para o setor.

Outra diferença importante é que nos Estados Unidos as autoridades de aplicação da lei têm mais recursos e apoio para investigar crimes financeiros. O Departamento de Justiça e a Securities and Exchange Commission (SEC), por exemplo, têm poderes amplos para investigar e processar crimes financeiros envolvendo ativos digitais.

Os resultados do trabalho de exame das hipóteses estão expostos na presente dissertação, de forma sintetizada, como segue.

Principia-se, no Capítulo 1, com o avanço tecnológico e o Direito Penal Econômico, mediante a inquirição de conceitos jurídicos acerca do Direito

Penal Econômico, lavagem de dinheiro, evasão de divisas e criptoativos, almejando definir o contexto histórico do crime econômico e as ramificações digitais atuais.

O Capítulo 2 particulariza a ligação da tecnologia blockchain e os tipos penais. Como efeito, irá analisar a fase investigatória policial, a correlação de atividades criminais com ativos digitais, operações transnacionais de casos práticos que apuraram o financiamento criminal através do ativo digital, explorando-se, por derradeiro, a facilidade da fuga de capital na era digital.

O Capítulo 3 dedica-se à elucidação das intervenções governamentais no mercado ilícito de criptoativos. Desse modo, averiguar-se-á os precedentes jurídicos brasileiros e norte-americanos, analisando-se suas relações, sendo, finalmente, ventilados os métodos e técnicas de repressão e combate à lavagem de dinheiro pelo meio de criptoativos.

Por último, com fito de evitar restringir a pesquisa apenas a criptomoedas, é relevante ressaltar que o título deste trabalho aborda a prática de crimes relacionados a criptoativos, que é uma categoria ampla que inclui subdivisões como criptomoedas (tokens de pagamento), tokens de utilidade e tokens referenciados a ativos.

Assim, o presente Relatório de Pesquisa se encerra com as Considerações Finais, nas quais são apresentados aspectos destacados da Dissertação, seguidos de estimulação à continuidade dos estudos e das reflexões acerca da prática de ilícitos penais auxiliados pelo avanço tecnológico, especialmente pelas moedas digitais.

Quanto à Metodologia empregada, registra-se que, na Fase de Investigação¹² foi utilizado o Método Indutivo¹³, na Fase de Tratamento de Dados

¹² “(...) momento no qual o Pesquisador busca e recolhe os dados, sob a moldura do Referente estabelecido (...)” PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. 14 ed. ver., atual. e ampl. Florianópolis: Empório Modara, 2018. p. 112-113.

¹³ “(...) pesquisar e identificar as partes de um fenômeno e colecioná-las de modo a ter uma percepção ou conclusão geral (...)”. PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 114.

o Método Cartesiano¹⁴, e, o Relatório dos Resultados expresso na presente Dissertação é composto na base lógica indutiva.

Nas diversas fases da Pesquisa, foram acionadas as Técnicas do Referente¹⁵, da Categoria¹⁶, do Conceito Operacional¹⁷ e da Pesquisa Bibliográfica¹⁸.

¹⁴ Sobre as quatro regras do Método Cartesiano (evidência, dividir, ordenar e avaliar) veja LEITE, Eduardo de oliveira. **A monografia jurídica**. 5 ed. São Paulo: Revista dos Tribunais, 2001. p. 22-26.

¹⁵ “(...) explicitação prévia do(s) motivo(s), do(s) objetivo(s) e do produto desejado, delimitando o alcance temático e de abordagem para a atividade intelectual, especialmente para uma pesquisa.” PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 69.

¹⁶ “(...) palavra ou expressão estratégica à elaboração e/ou à expressão de uma ideia.” PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 41.

¹⁷ “(...) uma definição para uma palavra ou expressão, com o desejo de que tal definição seja aceita para os efeitos das ideias que expomos (...)”. PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 58.

¹⁸ “Técnica de investigação em livros, repertórios jurisprudenciais e coletâneas legais”. PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 217.

Capítulo 1

O AVANÇO TECNOLÓGICO E O DIREITO PENAL ECONÔMICO

1.1 SUSCINTA INTRODUÇÃO DO DIREITO PENAL ECONÔMICO E SUAS PREOCUPAÇÕES COM O RISCO SISTÊMICO

A incursão sobre o surgimento e o conceito de crime econômico culminou de uma noção que timidamente ocorreu no início do século XX. Porém, fortaleceu-se e tornou-se presente no final do mesmo século e ascendeu no início do século subsequente.

BONGER¹⁹²⁰ foi um dos primeiros pesquisadores que fez distinção entre crime de rua (comum) e crime econômico, incluindo na segunda categoria os crimes cometidos por comerciantes e empresários em relação às propriedades como resultado da maximização da lógica especulativa e da capitalização.

Mais tarde, SUTHERLAND²¹²² conceituou o termo colarinho branco como sendo intimamente relacionado com classes sociais do alto escalão, evidenciando que existiam crimes que, em tese, deveriam ser punidos pela lei penal e que até aquela época a criminologia não tinha prestado atenção científica. Nesse sentido, enquanto BONGER considerou o ilícito econômico como crime sobre a

¹⁹ Willem Adriaan Bonger (1876-1940): Willem Bonger foi um estudioso holandês mais conhecido por sua aplicação do marxismo à criminologia em sua obra *Criminalidade e condições econômicas*, publicada pela primeira vez em 1905. Essa não foi apenas a primeira tentativa de criar uma criminologia marxista, mas Bonger também foi a figura central no estabelecimento da criminologia na Holanda. Sua visão sofisticada das causas socioeconômicas do crime no capitalismo mantém sua relevância até hoje, em particular suas noções de egoísmo e desmoralização.

²⁰ BONGER, Willem. **Criminalité et conditions économiques**. University of Michigan Library: 1905.

²¹ Edwin Sutherland, (nascido em 13 de agosto de 1883, Gibbon, Nebraska, EUA—falecido em 11 de outubro de 1950, Bloomington, Indiana), criminologista americano, mais conhecido por seu desenvolvimento da teoria da associação diferencial do crime. Em reconhecimento à sua influência, o prêmio anual mais importante da Sociedade Americana de Criminologia é dado em seu nome.

²² SUTHERLAND, Edwin. **White-collar criminality**. *American Sociological Review*, 5(1), 1–12: 1940.

propriedade resultante da maximização da lógica especulativa e da capitalização, SUTHERLAND considerou este delito como um crime de colarinho branco praticado por aqueles que detinham poder sobre o capital.

Os doutrinadores BONGER e SUTHERLAND queriam demonstrar que, além do crime dito clássico ou crime comum, existiam condutas, praticadas no âmbito financeiro, que mereciam o apreço legislativo.

Esses crimes foram definidos por serem atos ilícitos cometidos por um indivíduo ou grupo de indivíduos que objetivam obter vantagem financeira ou profissional. Nesse diapasão, o principal motivo do infrator é o ganho econômico. Crimes financeiros praticados no meio digital, evasão fiscal, furto digital, venda de substâncias controladas (pela *deep web*) e abusos de ajuda econômica (pacote de incentivo fiscal) são apenas alguns dos exemplos de crimes econômicos.

O crime econômico, enfoque eminente de países em desenvolvimento, gera obstáculos na progressão econômica. Essa conduta afeta diretamente o sistema, sendo certo que o risco sistêmico é aquele que atinge o mercado e sociedade como um todo. Recursos que poderiam apoiar o crescimento de um país são perdidos por meio de atos criminosos como: corrupção, evasão fiscal, lavagem de dinheiro, evasão de divisas, *insider trader* e crimes contra o sistema financeiro. As consequências destes delitos afetam o desenvolvimento dos países e é particularmente grave para países economicamente frágeis como o Brasil. O crime econômico, incluindo fluxos financeiros ilícitos, desvia recursos essenciais que fortificariam os serviços públicos, desde segurança e justiça até serviços sociais básicos, como saúde e educação.

SOUZA e AZEVEDO²³ afirmam que:

Um dos maiores desafios contemporâneos para o enfrentamento dos crimes praticados no âmbito da atuação empresarial se encontra na delimitação de critérios para imputação da responsabilidade penal dos membros da empresa. As teorias

²³ SOUZA, Artur de Brito Gueiros; AZEVEDO, Juliana de. **Inovações no direito penal econômico: prevenção e repressão da criminalidade empresarial**. Brasília: ESMPU, 2018. Santa Rosa Câmara. p. 35.

tradicionais para imputação de autoria e participação não respondem adequadamente ao problema em razão das peculiaridades das organizações empresárias, especialmente daquelas mais complexas.

A preocupação global dos crimes interfinanceiros, aqueles cometidos no âmbito mundial, é nítida. Praticamente todas as organizações internacionais, que buscam reprimir esse tipo de criminalidade, emitiram diretrizes e padrões para combater crimes relacionados a economia e finanças. O Banco Mundial, por exemplo, tem regras claras para financiar projetos de desenvolvimento. Em 1997, a OCDE²⁴ publicou sua Convenção Antissuborno e, desde então, lançou diversos princípios e iniciativas para combater a economia paralela, o crime econômico e fiscal, incluindo o plano de ação de 15 pontos de erosão de base e transferência de lucro (BEPS).

Contudo, foi na década de 20, no crash da bolsa de valores de Nova Iorque, em 1929, que o Estado passou a tomar medidas intervencionistas na economia²⁵, para então, de certa forma, regular e fiscalizar o mercado financeiro. Com a admissão estatal intervencionista para corrigir eventuais deficiências ou imperfeições do mercado, abriram-se precedentes fiscalizatórios. Os possíveis abusos empresariais que pudessem ter abalos significativos na sociedade estavam agora tipificados em uma legislação penal. Portanto passou-se a criminalizar determinadas condutas que pudessem prejudicar a ordem social ou econômica. Sendo assim, o direito Penal Econômico transformou-se em um microsistema

24 A Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) constitui foro composto por 37 países dedicado à promoção de padrões convergentes em vários temas, como questões econômicas, financeiras, comerciais, sociais e ambientais. Suas reuniões e debates permitem troca de experiências e coordenação de políticas em áreas diversas da atuação governamental. A OCDE busca coordenar definições, medidas e conceitos, o que contribuiria para a comparação entre países que enfrentam problemas similares. Ademais de fomentar a formação de enfoques comuns para políticas públicas, essas características permitem à OCDE tratar de temas controversos, de definição difícil em organismos de vocação universal, como as Nações Unidas e na OMC. (ITAMARATY, O Brasil e a OCDE. Disponível em <<http://www.itamaraty.gov.br/pt-BR/politica-externa/diplomacia-economica-comercial-e-financeira/15584-o-brasil-e-a-ocde>>, acesso em 04/10/2021.

25 PARKER, Selwyn. **The Great Crash: How the Stock Market Crash of 1929 Plunged the World into Depression**. Piatkus Books; Digital original edition: 2008.

dentro do Direito Penal. Os crimes econômicos por muito tempo passaram à margem da percepção social, com embaraço para a vulnerabilidade na imputação.

SOUZA e AZEVEDO destacam que

Com o avançar dessa complexidade em matéria penal, o Direito Penal Econômico alça voos antes inimagináveis, propondo o enfrentamento, em bases técnicas, da prevenção, responsabilização e penalização dos agentes econômicos em decorrência de atos ilícitos praticados no âmbito da atividade empresária.²⁶

Deixando estatísticas de lado, as razões para se preocupar com o crime econômico talvez seja óbvio para muitos. A essência da fraude é a quebra de confiança, sendo esta, a própria base do comércio e da sociedade civil. O crime econômico, portanto, compromete as relações interpessoais básicas, o desenvolvimento econômico e, em alguns casos, inclusive, a estabilidade dos governos. Pode-se compilar uma longa lista de fatores que afetaram drasticamente a economia brasileira no decorrer dos anos, mas o objetivo deste estudo é discutir os riscos do crime econômico e a incorrência para a ameaça sistêmica. Sendo então, o objetivo deste capítulo abordar condutas ilícitas que estão relacionadas a oferta de criptoativos, haja vista que a convergência de computadores e comunicações torna-se fator dominante no comércio.

Entrementes, crimes econômicos e financeiros são todas as ações conducentes a infligir danos em fundos públicos, atividades de produção, distribuição, circulação e consumo de mercadorias e serviços, bem como as relações relativas ao fornecimento, planejamento, treinamento e fabricação, para o apoio à indústria, crédito, seguro, transporte, comércio, empresas e sociedades cooperativas.²⁷

²⁶ SOUZA, Artur de Brito Gueiros; AZEVEDO, Juliana de. **Inovações no direito penal econômico: prevenção e repressão da criminalidade empresarial**. Brasília: ESMPU, 2018. Santa Rosa Câmara. p. 53.

²⁷ GRABOSKY, Peter. **The prevention and control of economic crime**. Disponível em: <<http://press-files.anu.edu.au/downloads/press/p228301/pdf/ch091.pdf>> acesso em 04/10/2021.

Os crimes econômicos referem-se a atos ilegais cometidos por um indivíduo ou grupo de indivíduos para obter uma vantagem financeira ou profissional. Em tais delitos, o principal motivo do criminoso é o ganho econômico.

Verbera-se, deste modo, consoante OLIVARES²⁸, o crime do mundo global é, por excelência, o econômico – não obstante outras condutas, como os casos de tráfico de pessoas, imigração ilegal e crimes contra humanidade também serem frutos da globalização.

Por sua vez, AMARAL²⁹ descreve que:

Uma característica do Direito Penal Econômico é a criminalização de condutas que não afetam um bem jurídico individual determinado (como vida, patrimônio, honra), mas conceitos indeterminados e classificados como bens jurídicos supraindividuais (bom funcionamento do sistema financeiro nacional, boas condições de concorrência e livre iniciativa etc.), à luz das teorias penais contemporâneas.

Sendo assim, o Direito Penal Econômico não tem como objetivo assegurar um direito individual, mas sim o direito coletivo (de forma abstrata), que em muitos casos afeta tão somente o Estado, a exemplo do que foi dito pelo autor: “*o bom funcionamento do sistema financeiro nacional ou as condições de concorrência e a livre iniciativa*”.

MASI³⁰, discorre que:

Um critério racional para delimitar o âmbito do Direito Penal Econômico passa pela distinção entre bens jurídicos individuais e supraindividuais, como, por exemplo o crédito, o consumo, o sistema financeiro, o mercado de capitais etc. A delimitação de um critério material para definir um delito econômico, necessariamente

²⁸ QUINTERO OLIVARES, Gonzalo. **El derecho penal ante la globalización. Reflexiones sobre las leyes penales y los penalistas españoles**. Madrid: Civitas, 2004, p. 15. e ss.

²⁹ AMARAL, Thiago Bottino. **Direito Penal Econômico**. FGV, 2015. Disponível em: <https://direitorio.fgv.br/sites/direitorio.fgv.br/files/u100/direito_penal_economico_2015-1.pdf>, acesso em 20/12/2021.

³⁰ MASI, Carlo Velho. **Direito Penal Econômico: do que estamos falando? Canal Ciências Criminais, 2016**. Disponível em: <<https://canalcienciascriminais.com.br/direito-penal-economico-do-que-estamos-falando/>>, acesso em 20/12/2021.

gira em torno do conceito de bem jurídico-penal, entendido como um interesse social protegido pela norma.

Com base na interpretação atual da Constituição da República Federativa do Brasil, ao analisar os dispositivos que regulam tanto a Constituição Econômica em termos materiais quanto formais, conclui-se que a intervenção do Estado na vida econômica e social é justificada somente quando busca alcançar objetivos mais amplos de bem-estar coletivo, especialmente no que diz respeito às necessidades individuais.³¹

Para LUCAS³²:

O bem jurídico protegido por esse setor do Direito Penal tem um caráter supraindividual, tem um conteúdo econômico-empresarial e, somente em certos casos, aparecem alguns componentes de índole individual (ainda que com estreita relação com os interesses econômicos genericamente considerados). Isso permite afirmar que o Direito Penal não protege ou tutela a realização do fenômeno econômico em si, mas protege a integridade da ordem e, por isso, qualquer conduta que produza a ruptura desta ordem trará como consequência necessária uma sanção.

Logo, o Direito Penal Econômico é uma especialidade do Código Penal, não de uma Lei Financeira ou Tributária. Os normativos legais para a proteção de infrações financeiras são uma ordem financeira geral, uma parte substancial da ordem financeira pública, uma vez que tais violações prejudicam os bens ou interesses pessoais expressos nas atividades em andamento do processo econômico da produção, circulação e consumo de ativos. Nesse sentido, o crime financeiro ocorre em situações em que o lucro, prestígio ou progresso são perseguidos de forma ilegal.

O aumento significativo de todas as formas de crimes econômicos e financeiros na era da globalização, a natureza transnacional desses crimes, a

³¹ FIGUEIREDO, Leonardo Vizeu. **Lições de direito econômico**. Rio de Janeiro: Forense, 2017. ed. 7.

³² LUCAS, Ana Paula. **Direito Penal Econômico**, *Revista Saber Direito*. Disponível em <http://www.stf.jus.br/repositorio/cms/portaITvJustica/portaITvJusticaNoticia/anexo/SABER_DIREITO_AULA_Ana_Claudia_Lucas.doc>, acesso em 20/10/2021.

integração dos mercados financeiros mundiais e o crescimento do crime organizado transnacional, torna as implicações desses crimes verdadeiramente globais e, conseqüentemente, de difícil identificação.

PEDROSO³³ dispõe que:

De mais a mais, é possível ainda ilustrar (exemplificativamente) outras situações que trouxeram o direito penal econômico para o epicentro do mundo globalizado: a) o uso de informações privilegiadas nos crimes contra o sistema financeiro; b) a sonegação previdenciária, que pelo aumento da expectativa de vida das pessoas tende a resultar em uma verdadeira crise num futuro próximo; c) a pirâmide financeira, que ganhou outra dimensão pós Bernard Madoff, uma vez que trouxe um prejuízo acumulado (estimado em 65 bilhões de dólares) a seus investidores; e d) por fim, a industrialização, que pelo avanço tecnológico e do domínio econômico instável, nos trouxe uma sociedade de riscos – que contribui para uma incerteza social e uma crescente insegurança.

No que diz respeito a grande parte dos crimes econômicos, é difícil atribuir a responsabilidade a um único perpetrador ou a alguns. O culpado, em tese, costuma ser um coletivo, uma pessoa jurídica, uma empresa. Os crimes econômicos são, na maioria das vezes, praticados por um meio empresarial.

Contudo, o estado deverá intervir na gestão empresarial econômica apenas em ato de exceção, quando houver evidências de prática irregular ou crime econômico. PEDROSO³⁴ afirma que:

Desta sorte, partindo-se da premissa de que o bem jurídico a ser tutelado é a ordem econômica, é necessário professar que o Estado, principal responsável pelo direito de punir, só vem a se preocupar ao abuso do poder econômico se presentes atos ilícitos capazes de ocasionar graves danos ao mercado e, conseqüentemente, a sua livre concorrência – mesmo que a criminalidade econômica, qualquer que seja ela, cause à

³³ PEDROSO, Fernando Gentil Gizzi de Almeida; HERNANDES, Luiz Eduardo Camargo Outeiro. **Direito Penal Econômico**. Salvador: Editora Juspodivm.,2017. p. 37

³⁴ PEDROSO, Fernando Gentil Gizzi de Almeida; HERNANDES, Luiz Eduardo Camargo Outeiro. **Direito Penal Econômico**. Salvador: Editora Juspodivm, 2017. p. 41

coletividade efeitos colaterais econômicos e sociais potencialmente mais lesivos que aqueles trazidos pelo Direito Penal Clássico.

Por sua vez, PRADO³⁵ descreve que:

Embora admitida e, muitas vezes, necessária, a intervenção penal nesse campo se apresenta, com frequência excessiva, mais como *prima ratio* do que como *ultima ratio*, em constante fricção com os princípios da intervenção mínima e da fragmentariedade, o que de resto muitas vezes só põe em evidência o descompasso com a verdadeira missão do Direito Penal do Estado democrático e social de Direito.

O Direito Penal Econômico abrange uma ampla gama de crimes, desde crimes financeiros cometidos por instituições financeiras, evasão fiscal, lavagem de capitais, crimes cometidos por funcionários públicos (como suborno, peculato, tráfico de influências etc.) entre muitos outros.

Acredita-se que o crime econômico gere dano social imensurável e irreparável. Isso porque não atinge estritamente as instituições democráticas, mas também mina o tesouro do Estado ao cortar os recursos disponíveis para a implementação de políticas públicas. Os mais vulneráveis são os que mais precisam dessas políticas, de modo que se tornam uma das principais vítimas da corrupção e do crime econômico. Ao mesmo tempo, os danos sociais gerados por essas atividades criminosas costumam ser invisíveis: além da indignação geral, é bastante complexo ter uma consciência precisa sobre os verdadeiros efeitos desses crimes.

AMARAL³⁶ define os fatores que influenciam o cometimento de crimes econômicos e dispõe que:

Os criminosos econômicos, então, são resultado de três fatores: motivação, oportunidade e consciência da baixa probabilidade de serem punidos. Presentes estes três requisitos (que são como

³⁵ PRADO, Luiz Regis. **Direito penal econômico: ordem econômica, relações de consumo, sistema financeiro, ordem tributária, sistema previdenciário**. São Paulo: Revista dos Tribunais, 2004. p. 5.

³⁶ AMARAL, Thiago Bottino. **Direito Penal Econômico**. Editora: FGV, 2015. p. 16.

justificativas para sua conduta), o criminoso econômico agirá. Quando os valores dominantes no grupo são propícios ao cometimento de uma infração, o indivíduo, independentemente de sua classe social ou da sua constituição biológica, violará a lei. Vivemos, então, uma situação paradoxal que opõe o espaço ocupado pelo crime econômico no cenário do Direito Penal e comportamento social.

Além disso, a repressão seletiva e ineficaz deste tipo de crimes e dos seus responsáveis, evidencia a impunidade estrutural do nosso sistema judicial em relação a essa atividade criminosa. Claro, isso está ligado ao fato de que os crimes econômicos são frequentemente cometidos por atores poderosos, ligados ao poder político e econômico. O crime econômico é gerado a partir de um poder oculto que define as relações entre economia e política. A liberalização financeira e as reformas de mercado empreendidas no Brasil nas últimas décadas, deixaram como resultado um processo gradual de ruptura institucional do Estado pelos principais grupos econômicos. Essa ruptura se expressa em uma poderosa influência desses atores econômicos nos processos de tomada de decisão, na implementação de políticas públicas e na distribuição de recursos econômicos e sociais.

LUCAS³⁷ esclarece que,

Ainda no âmbito da definição de Direito Penal, o professor Jorge de Figueiredo Dias aponta para as tentativas ofertadas pela criminologia – a partir de Sutherland, com o conceito de *White collar crime*; pela criminalística – com a ideia de violação da confiança que deve fundar o fenômeno econômico; por um critério misto – que aceita a violação da confiança, mas agrega a lesão a um bem jurídico (a ordem econômica); e, por fim, pela dogmática jurídico-penal, em Baumann, para quem o Direito Penal Econômico é a soma das normas jurídicas penais que se situam no espaço coberto pelo Direito Econômico, definindo, este, como o ‘conjunto de normas que regulam a vida e as atividades econômicas e dos preceitos que de alguma forma se relacionam com a produção e distribuição dos bens econômicos’. Embora esse conceito seja criticável por sua extrema amplitude, tem sido considerado. Assim,

³⁷ LUCAS, Ana Paula. **Direito Penal Econômico**, *Revista Saber Direito*. Disponível em <http://www.stf.jus.br/repositorio/cms/portaITvJustica/portaITvJusticaNoticia/anexo/SABER_DIREITO_AULA_Ana_Claudia_Lucas.doc>, acessado em 20/10/2021. pp. 1-2.

Direito Penal Econômico é o conjunto de normas que tem por objeto sancionar, com as penas que lhe são próprias, as condutas que, no âmbito das relações econômicas, ofendam ou ponham em perigo bens ou interesses juridicamente relevantes.

Desta maneira, o baixo risco e os altos lucros associados ao crime econômico o torna uma atividade atraente para grupos de crime organizado. A probabilidade de que a fraude seja detectada e processada é baixa, devido à complexidade das investigações exigidas. Isso é particularmente verdadeiro para casos de fraude que podem ser descobertos apenas por meio da cooperação internacional e crimes na Internet, para os quais é necessário estabelecer jurisdição.

Os grupos/associações criminosas que operam em nível internacional se beneficiam das diferenças legislativas nacionais. Vulnerabilidades individuais e organizacionais, como a falta de consciência por parte das vítimas e a baixa percepção de risco por parte dos grupos-alvo, são fatores habilitadores para a maioria dos tipos de fraude.

De outro lado, há também, uma consciência cada vez maior de que certos atos do setor financeiro, que antes eram considerados apenas práticas comerciais inadequadas, podem, na verdade, ser criminosos. O investimento imprudente generalizado, a deturpação das demonstrações financeiras e a conspiração para manipular as taxas de juros interbancárias se enquadram na definição de crimes contra a economia popular.³⁸

É importante ressaltar que muitas iniciativas fraudulentas podem ter origem no outro lado do globo³⁹, contudo, há poucos remédios disponíveis para prevenir que o crime econômico transnacional seja evitado. Nada obstante, o Brasil obter capacidade de mobilizar a lei estrangeira, as chances de localizar o infrator, obter a extradição, montar uma acusação ou recuperar uma compensação pode

³⁸ GUARAGNI, Fábio André. BACH, Marion. MARIA SOBRINHO, Fernando Martins. **Direito Penal Econômico Administrativização do direito penal, criminal compliance e outros temas contemporâneos**. Londrina, PR: Thoth, 2017.

³⁹ TRANSPARENCY.ORG. **Corruption perceptions index**. Disponível em: <<https://www.transparency.org/en/cpi>>, acesso em 23/12/2021.

demorar. Problemas específicos surgem quando crimes financeiros são cometidos contra uma empresa local ou agência governamental, por uma pessoa situada em um país estrangeiro. Pode ser difícil conseguir assistência para a aplicação da lei no país estrangeiro, já que seus recursos são limitados e suas prioridades podem estar em outro lugar. Ainda há que se falar nos problemas adicionais os quais refletem na dificuldade de exercício nacional da soberania sobre os fluxos de capital e informação. Podem surgir questões jurisdicionais da transmissão online transfronteiriça, por exemplo, quando envolvem criptoativos e a real localização da sua custódia.⁴⁰

Mesmo que as agências policiais estrangeiras estejam dispostas e possam ajudar, a coleta de evidências no país aliado pode ser problemática. A distância será mais um impedimento substancial para a investigação. O custo de enviar força policial ao exterior para ajudar em uma investigação, ou o custo de emitir rogatórias para oitiva de testemunhas no exterior, pode ser proibitivo. Mesmo assim, muitas vezes existem impedimentos legais que devem ser superados⁴¹. Outrossim, as próprias leis do país externo podem conter conflitos com o Brasil e provavelmente não serão instantaneamente hospitaleiras a todas as evidências obtidas em seu solo.

Conquanto, a exemplo de objeto de pesquisa, os criptoativos evidenciam a problemática da vasta diferenciação de regulamentação das moedas digitais ao redor no mundo, deixando claro que, por vezes, o distanciamento legal é superior ao territorial. Em nações onde um grau de reflexão tem sido dado a essas questões, arranjos de assistência mútua podem ser alcançados com nações selecionadas para a coleta de evidências em seus solos, e legislação especial pode

⁴⁰ REUTERS. **Cryptocurrency crime surges, losses hit \$4.4 billion by end-September: CipherTrace report.** Disponível em: <<https://www.reuters.com/article/us-crypto-currencies-crime-idUSKBN1Y11WH>>, acesso em 13/12/2021.

⁴¹ SAADI, Ricardo Andrade. **Cooperação jurídica internacional em matéria penal.** Disponível em: <<https://www.justica.gov.br/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/arquivos/cartilha-penal-09-10-14-1.pdf>>, acesso em 13/12/2021.

ser promulgada para prever a admissibilidade em seus próprios tribunais de provas tomadas no exterior, como já declarado como necessidade mundial pelo GAFI.⁴²

Disto isto, as enormes perdas associadas à fraude financeira de alto nível minam os sistemas de seguridade social e desestabilizam os sistemas econômicos, indicando claramente uma falha de autorregulação. Por exemplo, a fraude de investimentos, depende de técnicas de engenharia social para manipular indivíduos a divulgarem informações confidenciais ou pessoais que podem ser usadas para fins fraudulentos - o que a torna particularmente difícil de combater. Este tipo de fraude pode ser altamente lucrativo.

Outra crescente utilização de oferta de ativos é a mercantilização de criptoativos através de sistemas que remuneram a captação de novos clientes. Sendo conseqüentemente um sistema autossustentável do qual os integrantes iniciais angariam fundos dos integrantes posteriores, o que, será pormenorizadamente esclarecido no capítulo subsequente.

Assim sendo, dando conta da nítida importância do direito penal econômico, perfaz-se necessário que no próximo subcapítulo seja abordado a origem da conduta de lavagem de capitais, uma vez que é considerado pelos doutrinadores e autoridades o fundamento básico de financiamento de empreendimentos ilícitos.

1.2 CONTEXTUALIZAÇÃO HISTÓRICA E JURÍDICA DA LAVAGEM DE CAPITAIS NO MUNDO, EM ESPECIAL NOS ESTADOS UNIDOS DA AMÉRICA E BRASIL

Em que pese o termo lavagem de dinheiro tenha origem na década de 20 nos Estados Unidos da América, o termo em si de transgredir normas sociais e legais para obter ganhos ou benefícios ilícitos, ocultando e/ou dissimulando a sua verdadeira origem pode ter surgido no século XVII, através da pirataria realizada

⁴² FATF/GAFI. **Padrões internacionais de combate à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação, as recomendações do GAFI.** Disponível em: <<http://www.fazenda.gov.br/orgaos/coaf/arquivos/as-recomendacoes-gafi>>, acesso em 03/12/2021.

em embarcações na Inglaterra⁴³. Por outro lado, há ainda quem defenda que a conduta nasceu quando a igreja católica proibiu a usura, na idade média.

Todavia, é inegável que durante o período da Lei Seca nos Estados Unidos da América (1920-1933) enormes quantias de dinheiro foram lavadas. É interessante notar que quando Al Capone, o gângster mais notório naquela época, foi indiciado pela primeira vez em 1931, não foi sob a acusação de violar a Lei Volstead⁴⁴ que criou a Lei Seca (que proíbe também o transporte e venda de bebidas com mais de 0,5% de álcool), nem pelos inúmeros assassinatos cometidos por ele e sua organização, mas, sim pela evasão de impostos federais durante os anos fiscais de 1925-1929 que ele foi processado. Na época, este foi o mais próximo que um procurador dos EUA chegou de indiciar alguém por lavagem de dinheiro.

O termo lavagem de dinheiro nasceu nos Estados Unidos⁴⁵, na década de 20, uma vez que as organizações criminosas utilizavam de lavanderias para ocultar o proveito do crime.

Também é interessante notar que, onde as forças policiais armadas perseguiram interminavelmente essas organizações sem sucesso, foram as pessoas atrás das mesas, sem armas, que efetivaram a persecução penal da organização mundialmente conhecida de Al Capone.

De acordo com KALIN e MULLER⁴⁶:

It is a coincidence that Switzerland, by strengthening its bank secrecy laws in the early 1930s, more with the aim of helping people hide away money in fear of the Nazi regime than for other reasons,

⁴³ MENDRONI, Marcelo Batlouni. **Tópicos essenciais de lavagem de dinheiro**. São Paulo: Revista dos Tribunais, maio 2001, citado por Castellar, João Carlos. Lavagem de Dinheiro – a questão do bem jurídico. Rio de Janeiro: Revan, 2004, p. 82-83

⁴⁴ Volstead Act, formalmente National Prohibition Act, lei americana promulgada em 1919 (entrou em vigor em 1920) para dar cumprimento à Décima Oitava Emenda, proibindo a fabricação e venda de bebidas alcoólicas.

⁴⁵ FINANCIACRIMEACADEMY. **Money Laundering History: Know The Important Origin Of Money Laundering**. Disponível em: <<https://financialcrimeacademy.org/money-laundering-history-the-origin/>>, acesso em 27/05/2023.

⁴⁶ MULLER, Christian. KALIN, John. Goldsworth. **Anti-money-laundering: international law and practice** / edited by Wouter H. Editora: John Wiley & Sons; Illustrated edição: 2007. p. 3.

came into the view of people who wanted to hide money for all kinds of legitimate and less legitimate reasons at that time. Not that Switzerland was alone in having bank secrecy rules, but it already had for a long time a well-established name for being discreet. Tax evasion not being a crime in Switzerland at the time, money could be safely put away without too many questions being asked. Only two directors of the bank in question had to know the identity of the client. For all others it was a numbered account or an account with a certain agreed code. Putting away money, however, was one thing, but using this money in a way that it could help to make 'business' grow was another.

BONFIM e BONFIM⁴⁷ afirmam que:

A expressão money laundering foi usada judicialmente pela primeira vez nos Estados Unidos, em 1982, num caso em que se postulava a perda de dinheiro procedente de tráfico de entorpecentes. O termo era empregado originalmente pelas organizações mafiosas que usavam lavanderias automáticas para investir dinheiro e encobrir sua origem ilícita.

A lavagem de dinheiro é, simultaneamente com os crimes ambientais, a essencial representação típica decorrente do erudito de expansão do Direito Penal Brasileiro. Cada conduta de ocultação de recursos, por si apenas, não ocasiona violação expressiva ao bem jurídico tutelado. Porém, o branqueamento de grandes quantias de ativos oriundos da profissão criminal possui o potencial de advir uma inquestionável pane no sistema econômico de um país, senão do mundo inteiro. Não obstante, o tipo penal de lavagem ter no escopo, assentir a responsabilização do pequeno lavador, procura também a estabilidade de todo o setor financeiro.⁴⁸

É claro que o instrumento jurídico da conspiração – lavagem de dinheiro e sua origem é, por natureza, limitado em sua eficácia por causa de uma intenção compartilhada. Isso é difícil de provar quando o manuseio do dinheiro do

⁴⁷ BONFIM, Márcia Monassi Mougnot; BONFIM, Edilson Mougnot. **Lavagem de Dinheiro**. 2. Ed. Malheiros Editores, 2005.

⁴⁸ BACH, Fábio André Guarangi; SOBRINHO, Fernando Martins Maria. **Direito penal econômico administrativização do direito penal, criminal compliance e outros temas contemporâneos**. Londrina, PR: Thoth, 2017.

crime é silenciosamente tolerado por provedores de serviços financeiros, como os bancos. Essa tolerância era mais ou menos a prática financeira diária nas décadas de 1950 e 1960: a saída de dinheiro (lícito) para os paraísos fiscais ao redor dos Estado Unidos continuou inabalável. Essa mobilidade financeira teve várias origens. Houve um fluxo constante de dinheiro saindo do país com destino a paraísos fiscais, como Bahamas e Panamá. Isso não era apenas dinheiro ilícito oriundo do crime, mas também de fontes legais, embora não relatado ao *Inland Revenue Service* (os EUA tiveram, na maior parte do tempo, de 1960 a 1982, uma saída líquida de capital.⁴⁹

Em 1991, pelo Decreto 154/91, o Brasil ratificou a Convenção de Viena que comprometia o país a implementar tipo penal que criminalizasse a conduta de lavar capitais de origem do tráfico ilícito de entorpecente.

A lavagem de dinheiro, como acontecimento criminológico, consistente na conduta do transgressor de ocultar ou dissimular o produto do crime, é sem dúvida muito antiga. Porém, como forma criminosa própria, com tipificação e penalização na legislação, é surpreendentemente atual. Com resultado, a maior parte das leis criminalizando tal tipicidade data das décadas de 80 e 90 do século XX. A título de exemplo, a lei norte-americana é de 1986, a francesa, de 1987, a argentina, no que se refere à lavagem de produto de tráfico de drogas, de 1989, enquanto a lavagem do produto de demais crimes, de 2000, a suíça, de 1990. A lavagem de dinheiro foi criminalizada no Brasil pela Lei n. 9.613, de 1998.⁵⁰

De acordo com CALLEGARI⁵¹ e WEBER:

[...] a expressão utilizada para definir o delito aqui tratado é Lavagem de Dinheiro. A palavra lavar vem do latim *lavare*, e significa expurgar, purificar, reabilitar, daí a ideia de tornar lícito o dinheiro advindo de atividades ilegais e reinseri-lo no mercado como se lícito fosse. Levando em conta que o delito representa a

⁴⁹ FINANCIALCRIMEACADEMY. **Money Laundering History: Know The Important Origin Of Money Laundering.** Disponível em: <<https://financialcrimeacademy.org/money-laundering-history-the-origin/>>, acesso em 27/05/2023.

⁵⁰ MORO, Sergio Fernando. **Crime de lavagem de dinheiro.** São Paulo: Saraiva, 2010.

⁵¹ CALLEGARI, André Luís; WEBER, Ariel Barazzetti. **Lavagem de dinheiro.** São Paulo: Atlas, 2014. p. 24.

“transformação”, outros países utilizam palavras que etimologicamente significam limpeza.

Nesse diapasão, o Órgão⁵² Fiscal Brasileiro define:

O crime de lavagem de dinheiro caracteriza-se por um conjunto de operações comerciais ou financeiras que buscam a incorporação na economia de cada país, de modo transitório ou permanente, de recursos, bens e valores de origem ilícita e que se desenvolvem por meio de um processo dinâmico que envolve, teoricamente, três fases independentes que, com frequência, ocorrem simultaneamente.

Por outro lado, com intuito de estender a possibilidade delitiva, em 2012, a Lei nº 9.613, de 1998, foi alterada pela Lei nº 12.683, de 2012, trouxe importantes avanços para a prevenção e combate à lavagem de dinheiro, tais como: A extinção do rol taxativo de crimes antecedentes, admitindo-se agora como crime antecedente da lavagem de dinheiro qualquer infração penal; A inclusão das hipóteses de alienação antecipada e outras medidas assecuratórias que garantam que os bens não sofram desvalorização ou deterioração; Inclusão de novos sujeitos obrigados tais como cartórios, profissionais que exerçam atividades de assessoria ou consultoria financeira, representantes de atletas e artistas, feiras, dentre outros; aumento do valor máximo da multa para R\$ 20 milhões.⁵³

Para MORO⁵⁴:

O crime tornou-se um fenômeno de caráter internacional. Grupos criminosos organizados fixam sua sede em um país, comandam crimes praticados em outro e ocultam o produto de sua atividade em um terceiro. Nesse contexto, a cooperação jurídica internacional constitui recurso necessário para investigações e persecuções exitosas, devendo também ser reavaliados conceitos de soberania nesse novo mundo, sob pena de fracasso. Quando os países não

⁵² BRASIL. FAZENDA. **Prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo**. Disponível em: <<http://www.fazenda.gov.br/assuntos/prevencao-lavagem-dinheiro>>, acesso em 17/12/2021.

⁵³ BRASIL. FAZENDA. **Fases da lavagem de dinheiro**. Disponível em: <<https://www.fazenda.gov.br/assuntos/prevencao-lavagem-dinheiro#fases-da-lavagem-de-dinheiro>>, acesso em 20/09/2022.

⁵⁴ MORO, Sergio Fernando. **Crime de lavagem de dinheiro**. São Paulo: Saraiva, 2010. p. 16.

cooperam em matéria criminal, quem ganha é o criminoso e não o País não cooperante. A cooperação é relevante para todos os crimes, não só a lavagem. É, todavia, o crime de lavagem e a política a ele subjacente, colocando o confisco do produto do crime como estratégia prioritária de investigação e persecução, que conferiram à cooperação jurídica internacional uma nova relevância.

Tradicionalmente a lavagem de capitais é descrita como um procedimento de três etapas: colocação, ocultação e integração - em que um indivíduo, seja pessoa física ou jurídica, disfarça a substância inaugural dos recursos para simular que lhe parecem legítimos. O primeiro passo neste processamento, chamado de colocação envolve a ilegalidade do recurso no sistema financeiro. Isso pode ser realizado de inúmeras maneiras, a colocação pode ocorrer por meio da compra de propriedades, imóveis ou obras de arte, por exemplo.⁵⁵

BATLOUNI⁵⁶, elucida que:

Existem basicamente duas opções após obter o dinheiro de origem criminosa: Aplicar diretamente no sistema financeiro. Transferir para outro local. Nessa etapa, utilizam-se as atividades comerciais e as instituições financeiras, tanto bancárias, como não bancárias, para introduzir montantes em espécie, geralmente divididos em pequenas somas, no circuito financeiro legal. Na maioria das vezes, o agente criminoso movimenta o dinheiro entre contas bancárias/aplicações financeiras, de pessoas físicas e jurídicas ou em países com regras mais permissivas e naqueles que possuem um sistema financeiro liberal (paraísos fiscais e centros *offshore*). A introdução de dinheiro em espécie é normalmente direcionada para a instalação de atividades comerciais que, tipicamente, também trabalham com dinheiro vivo. Assim, os recursos ilícitos se misturam aos recursos obtidos em atividades legais e são posteriormente depositados em bancos.

⁵⁵ BATLOUNI, Marcelo. **Crime de lavagem de dinheiro**. Editora Atlas: 2018, 4ª edição.

⁵⁶ BATLOUNI, Marcelo. **Crime de lavagem de dinheiro**. Editora Atlas: 2018, 4ª edição. p. 83

Para MORO⁵⁷, na colocação, o resultado do crime é desvinculado de sua procedência material, na segunda fase, o numerário é movimentado a partir de várias transações de modo a dificultar ou impossibilitar o rastreamento, e pela terceira é finalmente reintegrado em negócios ou em bens, com a simulação de investimentos lícitos.

MORO⁵⁸ frisa que “a conversão de produto de crime antecedente em ativos lícitos é crime de lavagem, desde que o agente tenha a intenção específica de ocultação ou dissimulação”. Em outras palavras, BATLOUNI⁵⁹, acentua que:

Nessa segunda etapa, o agente desassocia o dinheiro de sua origem – passando-o por uma série de transações, conversões e movimentações diversas. Tanto mais eficiente a lavagem quanto mais o agente afastar o dinheiro de sua origem. Quanto mais operações, tanto mais difícil a sua conexão com a ilegalidade e tanto mais difícil a sua prova. Se por um lado a realização de diversas operações (transações financeiras, movimentações etc.) é muito mais custosa e traduz significativa prejuízo decorrente de cada uma delas, é meio que se afigura mais seguro pela “distância” que o agente lavador atribui ao dinheiro, bem ou valor – produto de crime.

Assim sendo, nesta fase, a intenção do infrator lavador é distanciar o dinheiro da sua origem ilícita, afastando-o quanto possível, ocultando-o e/ou dissimulando-o, para que tome características de origem legal.

Por último, próximo do exaurimento do crime, é identificada a terceira e última fase, definida por BATLOUNI⁶⁰ quando:

O agente cria justificações ou explicações aparentemente legítimas para os recursos lavados e os aplica abertamente na economia legítima, sob forma de investimentos ou compra de ativos. Nesta última etapa, o dinheiro é incorporado formalmente aos setores regulares da economia. Essa integração permite criar organizações

⁵⁷ MORO, Sergio Fernando. **Crime de lavagem de dinheiro**. São Paulo: Saraiva, 2010.

⁵⁸ MORO, Sergio Fernando. **Crime de lavagem de dinheiro**. São Paulo: Saraiva, 2010. p. 36.

⁵⁹ BATLOUNI, Marcelo. **Crime de lavagem de dinheiro**. Editora Atlas: 2018, 4ª edição. p. 84

⁶⁰ BATLOUNI, Marcelo. **Crime de lavagem de dinheiro**. Editora Atlas: 2018, 4ª edição. p. 86.

de fachada que prestam serviços entre si. As organizações criminosas buscam investir em negócios que facilitem suas atividades e, uma vez formada a cadeia, torna-se cada vez mais fácil legitimar o dinheiro ilegal. Integração é, portanto, o estágio final para a transformação de dinheiro sujo em dinheiro aparentemente lícito.

É indefinidamente árduo para as autoridades conseguirem rastrear os recursos de origem ilícita nessa fase do procedimento da lavagem, uma vez que já passaram por outras duas etapas e a essa altura estarão com feição significativamente limpa.⁶¹

Logo, o crime de lavagem de dinheiro é um fenômeno que afeta a sociedade global significativamente. O objetivo do legislador em tipificar tal conduta é de prevenir, aniquilar e desmantelar os fundos que financiam organizações criminosas. É cediço que o sucesso no crime de lavagem é um dos fatores que contribui para o crescimento do crime organizado. O intuito deste trabalho acadêmico é identificar os novos meios utilizados, tal qual criptomoeda e NFT, na lavagem que possam dificultar o rastreio e apreensão destes bens. No próximo subcapítulo será levantado o tipo penal evasão de divisas que, em tese, acompanha intimamente a lavagem de dinheiro, uma vez que fronteiras, atualmente, não são barreiras eficazes a combater a prática criminal.

1.3 DEFINIÇÃO DA CONDUTA EVASÃO DE DIVISAS

Crimes fiscais, lavagem de dinheiro e outros crimes financeiros ameaçam os interesses estratégicos, políticos e econômicos de países desenvolvidos e em desenvolvimento. Eles também minam a confiança dos cidadãos na capacidade de seus governos de fazer com que os contribuintes paguem seus impostos e podem privar os governos das receitas necessárias para o desenvolvimento sustentável.

Logo, prática comum que busca evadir finanças para o exterior é a utilização de contas *offshore*. Contas *offshore* são contas que existem fora do país

⁶¹ BATLOUNI, Marcelo. **Crime de lavagem de dinheiro**. Editora Atlas: 2018, 4ª edição.

de origem, permitindo, em tese, a maximização do capital, com a redução tributária, e transações em diferentes moedas. As contas *offshore* operam em outra jurisdição, o que significa que estão fora do poder/julgamento legal do seu país de residência. Insta destacar que, possuir contas *offshore* não é prática ilegal. Normalmente, ter uma conta *offshore* significa que os indivíduos desfrutam de benefícios fiscais, pois o dinheiro evita tributação em seu país de origem e pode não haver impostos semelhantes a pagar no país em que a conta está configurada.

Todavia, para o envio lícito de capital e recursos a contas *offshore* ou outros meios de carteira financeira é necessário que o dinheiro seja declarado e tenha saída legal do país de origem. Para cumprir obrigações legais, bancos e provedores de transferência de dinheiro exigem o envio de informações necessárias antes de permitir qualquer transação. Os requisitos podem variar por banco ou serviço de transferência de dinheiro.

A conduta criminal ocorre quando o criminoso deixa de declarar o envio de remessas. Assim, evadir divisas é crime. A conduta é tipificada como um ilícito contra o sistema financeiro nacional, através do qual o agente envia divisas ao exterior, sem declará-las à repartição federal competente, repercutindo, em regra, na ausência de pagamento de tributos devidos. A evasão ocorrerá quando, de alguma forma, as reservas monetárias são remetidas ao exterior, geralmente para paraísos fiscais, em nome das pessoas físicas ou jurídicas ou, ainda, para *offshores* constituídas em paraísos fiscais.⁶²

O crime de evasão de divisa tem previsão legal no art. 22 da lei 7.492/1986, e conforme PRADO⁶³ o objetivo da tipificação desta conduta é:

[...] evitar que a moeda, a divisa e os depósitos saiam do país ou nele deixem de entrar e, conseqüentemente, impedir que o Brasil tenha sua economia prejudicada, pois é por meio deles que o país procura manter seus compromissos (v.g., o pagamento da dívida externa). Igualmente, objetiva-se no parágrafo único desse dispositivo evitar que o particular mantenha depósitos não

⁶² NUNES, Leandro Bastos. **Evasão de Divisas**. Editora Juspodivm, 2017.

⁶³ PRADO, Luiz Regis. **Direito Penal Econômico**. Rio de Janeiro: Forense, 2019, 8. ed. p. 246.

declarados à repartição federal competente, como forma de sonegar os impostos devidos e se livrar da fiscalização.

O artigo descreve:

Art. 22. Efetuar operação de câmbio não autorizada, com o fim de promover evasão de divisas do País:

Pena - Reclusão, de 2 (dois) a 6 (seis) anos, e multa.

Parágrafo único. Incorre na mesma pena quem, a qualquer título, promove, sem autorização legal, a saída de moeda ou divisa para o exterior, ou nele mantiver depósitos não declarados à repartição federal competente.

Entretantes, necessário é especificar o tipo penal, para PRADO⁶⁴ moeda:

[...] é a representação concreta do dinheiro. Consiste numa terceira mercadoria, convencional e representativa do valor de troca dos bens e mercadorias, destinando-se a decompor a troca em compra e venda". 184 Depósitos são quantias em dinheiro confiadas a um banco por uma pessoa ou empresa. Repartição pública é qualquer órgão da Administração Pública federal, estadual ou municipal.

Considerando o disposto na norma incriminadora, infere-se que a conduta de manter moeda ou divisa no exterior, ou seja, apenas em depósito, é vedada e tipificada criminalmente, posto que a intenção do legislador foi de salvaguardar a fuga de capital sem o devido procedimento. Assim, o Estado, através do sistema de pagamentos e cambial tem condições de equalizar possíveis entraves cambiais.

O bem jurídico é conceituado por TÓRTIMA⁶⁵ da seguinte forma:

Considerando-se o momento histórico da edição da lei nº 7.492/86, marcado por gravíssimo desequilíbrio do nosso balanço de

⁶⁴ PRADO, Luiz Regis. **Direito Penal Econômico**. Rio de Janeiro: Forense, 2019, 8. ed. p. 246. p. 247.

⁶⁵ TÓRTIMA, José Carlos. **Crimes Contra o Sistema Financeiro**. Editora Lumen Juris: 2011. p. 132.

pagamentos, pode-se considerar que a ênfase do escopo da tutela da norma abrigada no art. 22 e no seu parágrafo único é preservação das reservas cambiais do País, com todos os seus reflexos no equilíbrio do sistema financeiro nacional, em particular, e da própria economia como um todo. Quando a última parte do disposto no parágrafo único, que trata da manutenção clandestina de ativos no exterior, a preocupação do legislador está também voltada para a proteção do patrimônio fiscal, ameaçado pela incógnita manutenção do exterior de recursos amealhados através de ganhos tributáveis, mas não efetivamente oferecidos à tributação. Como já observamos alhures, a questão das reservas cambiais como bem jurídico resguardado pelas normas penais contidas no art. 22 e seu parágrafo único, deve se achar no centro de qualquer discussão que se proponha a uma correta interpretação de seu sentido teleológico.

Como se nota, o crime é material, uma vez que pressupõe a efetiva comprovação da saída da moeda ou divisas ao exterior, sem a respectiva declaração às repartições federais competentes.⁶⁶

Calha consignar que, este dispositivo se trata de lei penal em branco, uma vez que exige norma complementar. As expressões que indicam essa indispensabilidade são: operação de câmbio não autorizada, saída de moeda ou divisa para o exterior sem autorização legal, depósitos não declarados à repartição federal competente.⁶⁷

A Resolução nº 4.844/2020 do Conselho Monetário Nacional divulgou relevantes impactos ao art. 22 da lei 7.492/1986. A resolução em questão alterou o art. 26 da Resolução nº 3.568 de 2008 do Banco Central que dispõe sobre o mercado de câmbio e dá outras providências. A nova redação do art. 26 foi alterada para:

Art. 26. A movimentação ocorrida em conta de depósito de pessoas físicas ou jurídicas residentes, domiciliadas ou com sede no exterior, de valor igual ou superior a R\$100.000,00 (cem mil reais),

⁶⁶ NUNES, Leandro Bastos. **Evasão de Divisas**. Editora Juspodivm, 2017.

⁶⁷ PRADO, Luiz Regis. **Direito Penal Econômico**. Rio de Janeiro: Forense, 2019, 8. ed. p. 246.

deve ser registrada no Sisbacen, na forma estabelecida pelo Banco Central do Brasil.

Parágrafo único. O Banco Central do Brasil poderá estabelecer situações nas quais será requerida a prestação de informações sobre movimentações de valores abaixo do limite estabelecido no caput.

REBOUÇAS⁶⁸ esclarece que:

O tipo penal do artigo 22 da Lei 7.492/1986 constitui uma norma penal em branco, complementada por atos normativos infralegais emanados do Conselho Monetário Nacional. Um desses atos é precisamente a Resolução 3.568/2008, agora modificada. Assim, o crime não se configura pela ausência de registro de operação cambial de qualquer valor, mas somente daquele ato de câmbio que envolva montante superior ao limite regulamentar.

Por fim, dado o avanço tecnológico observa-se que o ilícito é de alta complexidade e de difícil prevenção. A possibilidade de enviar remessas de dinheiro através de ativos digitais é mais do que realidade. O objetivo do tipo penal é evitar que o País tenha severo impacto econômico pela rápida fuga de capital. Logo, ao se estabelecer que seja possível a transferência de recursos para qualquer lugar no mundo com apenas um click (compra de um criptoativo), percebe-se a preocupação estatal. A última passagem deste capítulo introdutório tratará dos criptoativos e sua tecnologia, objetivando, por fim, identificar o avanço tecnológico e os riscos criminais decorrentes de tal fato.

1.4 CONCEITUAÇÃO JURÍDICA E TECNOLÓGICA DOS CRIPTOATIVOS

Nos primórdios da civilização humana, a aquisição de bens e serviços se concluía através da troca de mercadorias. Quando o homem primitivo começou a criar gado doméstico, uma das primeiras formas de troca incluía o rebanho, ovelhas, bem como vegetais e grãos cultivados. A primeira moeda conhecida foi idealizada pelo rei Alyattes na Lídia, agora parte da Turquia, em 600 a.C. Esta

⁶⁸ REBOUÇAS, Sérgio. **Evasão de divisas e retroatividade da Resolução 4.844/2020 do CMN.** <Disponível em: <https://www.conjur.com.br/2020-ago-17/opiniao-evasao-divisas-retroatividade-resolucao-cmn>>, acesso em 20/09/2021.

moeda senhoreava a imagem de um leão que rugia. Por volta de 1661 d. C as moedas evoluíram para notas (papel moeda) impressas por um banco central. O primeiro cartão de crédito foi lançado em 1946⁶⁹. A tecnologia vestível⁷⁰ foi criada para inovar o mundo transacional, uma vez que já é possível utilizar pulseiras, relógios, celulares e outros dispositivos para efetuar os pagamentos.⁷¹ A última onda tecnológica foi a implementação das transferências de recursos através de chaves PIX, deixando de lado o antigo TED e DOC.

Atualmente, o criptoativo é o centro das atenções, sendo a Bitcoin, a precursora de implementação deste meio de pagamento como uma nova forma de moeda. O criptoativo foi criado para ser a solução de problemas relacionado à independência financeira pessoal e interferência estatal. O que invocou, quase inadvertidamente, uma enorme propriedade de investimento. À medida que as moedas se tornaram mais populares, seus valores começaram a avultar em um progresso constante ao longo da metade desta década. Criptoativos, ou moedas virtuais, são meios digitais de troca, criados e usados por indivíduos ou grupos privados. A imensa maioria dos criptoativos não é regulamentada, tampouco fiscalizada pelos países, consideradas, portanto, alternativas - meios de troca que existem fora dos limites da política monetária estatal.⁷²

Para ANTONOPOULOS⁷³ criptoativo é definido como:

[...] um conjunto de conceitos e tecnologias que formam a base de um ecossistema de dinheiro digital. Unidades de moeda chamadas bitcoins são usadas para armazenar e transmitir valor entre os participantes na rede Bitcoin. Usuários Bitcoin comunicam-se entre

⁶⁹ INVESTOPEDIA. **Roots of Money.** Disponível em: <https://www.investopedia.com/articles/07/roots_of_money.asp>, acesso em 27/05/2023.

⁷⁰ São dispositivos inteligentes que o usuário literalmente veste e usa como se fosse um acessório. O potencial das tecnologias vestíveis é imensurável. A exemplo a Wearable (pulseiras de pagamento).

⁷¹ TELEGRAPH. **The history of money from barter to bitcoin.** Disponível em: <<https://www.telegraph.co.uk/finance/businessclub/money/11174013/The-history-of-money-from-barter-to-bitcoin.html>>, acesso em 03/09/2021.

⁷² FORBES. **A short history of bitcoin an cryptocurrency everyone should read.** Disponível em: <<https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-cryptocurrency-everyone-should-read/#2341a4773f27>>, acesso em 03/09/2021.

⁷³ ANTONOPOULOS, Andreas. **Mastering Bitcoin - Unlocking Digital Currencies.** Editora: Sebastopol: O'Reilly, 2015.

si utilizando o protocolo bitcoin principalmente através da Internet, mas outras redes de transporte também podem ser usadas. A implementação da pilha do protocolo bitcoin, está disponível como software de código aberto, pode ser executada em uma ampla variedade de dispositivos de computação, incluindo laptops e smartphones, o que torna a tecnologia de fácil acesso.

Bitcoin é o criptoativo disruptivo e o primeiro a ser amplamente utilizado neste novo modelo de transferência e pagamentos financeiros. No entanto, existem centenas de criptoativos e outras tantos surgem a cada dia. O criptoativo começou a atrair alguma atenção em certas comunidades online pela maneira engenhosa como deixou bancos e outras instituições financeiras fora da equação. Sendo realmente um método de pagamento ponto a ponto entre as partes. A moeda opera em uma rede descentralizada, e o processo criptográfico que existia nas primeiras tentativas de moeda digital foi refinado.⁷⁴

O nascimento da era digital das moedas origina de um artigo chamado “Bitcoin - Um Sistema de Caixa Eletrônico Ponto a Ponto” (publicado em 31 de outubro de 2008) veiculado em um fórum de discussão sobre criptografia por alguém que se autodenomina Satoshi Nakamoto, cuja verdadeira identidade permanece um mistério até hoje.⁷⁵

Embora a Bitcoin tenha sido o primeiro criptoativo estabelecido, houve tentativas anteriores de criar moedas online com livros-razão protegidos por criptografia. A exemplo disto, foram o B-Money e Bit Gold, que foram formulados, mas nunca totalmente desenvolvidos.

Para ULRICH⁷⁶ a:

Bitcoin é uma moeda digital peer-to-peer (par a par ou, simplesmente, de ponto a ponto), de código aberto, que não depende de uma autoridade central. Entre muitas outras coisas, o

⁷⁴ LEWIS, Antony. **The Basics of Bitcoins and Blockchains**. Editora: Mango; Illustrated Edition, 2018.

⁷⁵ NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>, acesso em 10/09/2021.

⁷⁶ ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasoç. 2014. p. 17.

que faz o Bitcoin ser único é o fato de ele ser o primeiro sistema de pagamentos global totalmente descentralizado. Ainda que à primeira vista possa parecer complicado, os conceitos fundamentais não são difíceis de compreender.

Em prossecução ao desenvolvimento da definição do conceito de criptoativo, o autor⁷⁷ de forma clara e coesa, define a criptoativo como:

[...] uma forma de dinheiro, assim como o real, o dólar ou o euro, com a diferença de ser puramente digital e não ser emitido por nenhum governo. O seu valor é determinado livremente pelos indivíduos no mercado. Para transações online, é a forma ideal de pagamento, pois é rápido, barato e seguro. Você lembra como a internet e o e-mail revolucionaram a comunicação? Antes, para enviar uma mensagem a uma pessoa do outro lado da Terra, era necessário fazer isso pelos correios. Nada mais antiquado. Você dependia de um intermediário para, fisicamente, entregar uma mensagem. Pois é, retornar a essa realidade é inimaginável. O que o e-mail fez com a informação, o Bitcoin fará com o dinheiro. Com o Bitcoin você pode transferir fundos de A para B em qualquer parte do mundo sem jamais precisar confiar em um terceiro para essa simples tarefa. É uma tecnologia realmente inovadora. [...] Em definitivo, o Bitcoin é a maior inovação tecnológica desde a internet, é revolucionário, sem precedentes e tem o potencial de mudar o mundo de uma forma jamais vista. À moeda, ele é o futuro. Ao avanço da liberdade individual, é uma esperança e uma grata novidade.

É importante delinear que ao falar sobre o primeiro criptoativo, o autor considera o Bitcoin como um meio de troca digital, do mesmo efeito de uma comunicação por e-mail no sistema financeiro nacional. Ressalta-se que hoje, o meio de troca mais utilizado no mundo, são as compensações de pagamento através do cartão de crédito, conhecidos como Visa, Mastercard e American Express. Contudo, para o funcionamento destes meios de pagamentos, torna-se necessário um terceiro intermediário, ou seja, uma empresa prestadora de serviço que faça o manejo de tais incumbências. No modelo ponto a ponto empregado na tecnologia de criptoativos, o terceiro apenas existe para reforçar a confiança da

⁷⁷ ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasoç. 2014. P. 15.

transação, não sendo necessária sua intervenção se as partes a que se sujeitam a troca não a optarem. ULRICH⁷⁸ expõe que o universo jurídico recebeu o criptoativo da seguinte guisa:

A definição jurídica da criptoativo assenta como uma unidade monetária, considerados bem incorpóreo que, em certos mercados, têm sido aceitos em troca de bens e serviços. Conjecturasse dizer que essas transações constituem uma permuta, e de modo algum uma venda com pagamento em dinheiro, pois a moeda, em cada jurisdição, é definida por força de lei, sendo uma prerrogativa de exclusividade do estado.

Em 2010 o Bitcoin foi avaliado pela primeira vez – e como nunca havia sido negociado, apenas minerado, era impossível atribuir um valor monetário às unidades da criptoativo emergente. Naquele ano, alguém decidiu vender a sua cota pela primeira vez - trocando 10.000 unidades por duas pizzas. Se o comprador tivesse mantido em sua carteira esses Bitcoins, aos preços de hoje, valeriam mais de R\$ 1.165.570,00⁷⁹ (um bilhão, cento e sessenta e cinco milhões e quinhentos e setenta mil).

1.4.1 O controle descentralizado

Os criptoativos são marcados pelo descontrole estatal, um mercado atípico e descentralizado – volvendo-se em uma esfera financeira distinta do controle regulamentário. O fornecimento e o valor dos criptoativos são controlados pelas atividades de seus usuários e por protocolos altamente complexos incorporados em seus códigos de controle, não por decisões de bancos centrais ou outras autoridades regulatórias. Em particular, as atividades dos mineiros - usuários de criptoativos que aproveitam grande quantidade de poder de computação para registrar transações, recebendo unidades de criptoativos recém-criados e taxas de

⁷⁸ ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasoc. 2014. p. 15.

⁷⁹ Cotado ao valor de mercado de 06/03/2023, sendo uma unidade de bitcoin R\$ 116.557,00.

transação pagas por outros usuários em troca - são críticas para a estabilidade e funcionamento regular das moedas.⁸⁰

É importante ressaltar que, os criptoativos podem ser trocados por moedas fiduciárias em mercados online especiais, o que significa que cada uma tem uma taxa de câmbio variável com as principais moedas mundiais (como o dólar americano, libra esterlina, euro europeu e iene japonês). As trocas de criptomoedas são um tanto vulneráveis a hackers e representam o local mais comum para o roubo de moeda digital por hackers e cibercriminosos⁸¹.

Não obstante a maioria das moedas digitais tenham a característica por fornecimento finito, há exceções. Outrossim, seus códigos-fonte contêm instruções que descrevem o número preciso de unidades que poderão existir. Com o tempo, torna-se mais difícil para os mineiros produzir unidades de criptoativo, até que o limite superior seja alcançado e a nova moeda deixe de ser cunhada. O suprimento finito dos criptoativos os tornam inerentemente deflacionários, mais parecidos com ouro e outros metais preciosos - dos quais há suprimentos finitos - do que moedas fiduciárias, das quais os bancos centrais podem, em teoria, produzir suprimentos ilimitados.⁸²

Devido à sua independência política e segurança de dados essencialmente impenetrável, os usuários de criptoativos desfrutam de benefícios não disponíveis para usuários de moedas fiduciárias tradicionais, como o dólar americano e os sistemas financeiros que essas moedas suportam. Por exemplo, enquanto um governo pode facilmente congelar ou até mesmo confiscar uma conta bancária localizada em sua jurisdição, é muito difícil para ele fazer o mesmo com

⁸⁰ LEWIS, Antony. **The Basics of Bitcoins and Blockchains**. Publisher: Mango; Illustrated Edition, 2018.

⁸¹ Crime cibernético é uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Alguns cibercriminosos são organizados, usam técnicas avançadas e são altamente capacitados em termos técnicos, outros são hackers novatos. KASPERSKY, Dicas de como se proteger contra crimes cibernéticos, disponível em: <<https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>>, acesso em 06/09/2021.

⁸² BURNISKE, Chris; TATAR, Jack. **Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond**. Publisher: McGraw-Hill Education; 1st Edition, 2017.

fundos mantidos em criptoativos - mesmo se o titular for um cidadão ou residente legal.

Por outro lado, os criptoativos vêm com uma série de riscos e desvantagens, como iliquidez e volatilidade do valor, que não afetam muitas moedas fiduciárias. Além disso, os criptoativos são frequentemente usados para facilitar as transações do mercado negro, de modo que muitos países os veem com desconfiança ou animosidade total. E embora alguns proponentes apregoem os criptoativos como investimentos alternativos potencialmente lucrativos, poucos (se houver) profissionais financeiros os consideram adequados para outra coisa, que não pura especulação.

Por fim, cabe destacar que, recentemente⁸³ (26/04/2022), em votação simbólica, o Plenário do Senado aprovou a regulamentação do mercado nacional de criptomoedas. A proposta conseqüentemente tornou-se a Lei nº 14.478/2022 que criou diretrizes para a “prestação de serviços de ativos virtuais” e regulamenta o funcionamento das empresas prestadoras desses serviços. A lei citada será esmiuçada no subcapítulo 1.4.3.

1.4.2 Exchanges

Exchanges são definidas como um mercado digital onde os comerciantes podem comprar e vender criptoativos usando diferentes moedas fiduciárias ou *altcoins*⁸⁴. A Exchange é uma plataforma online que atua como um intermediário entre compradores e vendedores do criptoativo.⁸⁵

As plataformas de troca de criptoativos combinam compradores com vendedores. Como em uma bolsa de valores tradicional, os comerciantes podem optar por comprar e vender bitcoins inserindo uma ordem de mercado ou uma

⁸³ SENADO. **Senado aprova mercado de criptomoedas com incentivo para energia**. Disponível em: <<https://www12.senado.leg.br/noticias/materias/2022/04/26/senado-aprova-mercado-de-criptomoedas-com-incentivo-para-energia-renovavel>>, acesso em: 01/05/2022.

⁸⁴ Altcoins são as outras criptoativos lançadas após o sucesso do Bitcoin. O termo *altcoins* se refere a todas as criptoativos que não sejam Bitcoin. No início de 2020, havia mais de 5.000 criptoativos. De acordo com a CoinMarketCap, as altcoins representaram mais de 34% do mercado total de criptoativos em fevereiro de 2020.

⁸⁵ INVESTOPEDIA, **Bitcoin Exchange**. Disponível em: <<https://www.investopedia.com/terms/b/bitcoin-exchange.asp>>, acesso em 07/09/2021.

ordem de limite. Quando uma ordem de mercado é selecionada, o negociante está autorizando a negociação de suas moedas pelo melhor preço disponível no mercado online. Com uma ordem de limite definida, o *trader* direciona a troca para negociar moedas por um preço abaixo ou acima da oferta atual, a depender, se está comprando ou vendendo.

1.4.3 Lei 14.478/22 – marco legal do criptoativo

O Projeto de Lei nº - 4.401/2021⁸⁶, que busca regulamentar as criptomoedas no Brasil, foi sancionado em 21 de dezembro de 2022 pela Presidência da República. A lei estabelece diretrizes para a prestação de serviços de ativos virtuais e regulamenta as empresas que oferecem esses serviços. Além disso, altera o Código Penal para incluir o crime de fraude com o uso de ativos virtuais, valores mobiliários e ativos financeiros. Também modifica a Lei nº 7.492/1986 e a Lei nº 9.613/1998, incluindo as empresas de ativos virtuais em suas disposições.

O objetivo principal do marco legal é regular o mercado de criptoativos no país e fornecer conceitos claros para a definição de ativos virtuais. A lei define ativo virtual como qualquer representação digital de valor que possa ser negociada ou transferida eletronicamente e utilizada para pagamentos ou fins de investimento. A definição exclui moedas nacionais e estrangeiras, moedas eletrônicas, instrumentos que fornecem acesso a produtos ou serviços específicos e representações de ativos previstos em lei ou regulamento.

Os ativos virtuais abrangidos pela lei são os tokens de pagamento, usados para comprar produtos e serviços. Os tokens de utilidade⁸⁷, que dão acesso

⁸⁶ BRASIL. Lei nº 14.478/2022, 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. Brasília, DF: Diário Oficial da União, 2022.

⁸⁷ De acordo com TOMCZAK: Utility tokens are a type of cryptocurrency token that is designed to provide access to a service or product offered by a blockchain-based platform. They are not intended to be used as a store of value, but rather serve a specific purpose within the platform's ecosystem. Utility tokens are typically used for making payments, accessing certain features or services, or participating in governance and decision-making processes within the platform. The value of utility tokens is often directly tied to the usage and demand for the platform's services. Examples of utility tokens include MATIC, LINK, BNB, UNI, MANA, ENJ, AR, and BAT. TOMCZAK, Tomasz. **Crypto-assets and crypto-assets' subcategories under MiCA Regulation**. Capital Markets Law Journal, Volume 17, Issue 3, July 2022, Pages 365–382.

a produtos ou serviços, são excluídos da lei. Os tokens não fungíveis (NFTs⁸⁸), que representam itens exclusivos e insubstituíveis, como obras de arte digitais, não são abrangidos pelo marco regulatório.

Em resumo, a Lei nº - 14.478/2022 estabelece diretrizes para a regulamentação de criptomoedas no Brasil, define conceitos para ativos virtuais, prevê crimes relacionados a ativos virtuais e inclui empresas de ativos virtuais nas disposições de leis existentes. A lei se concentra em "tokens de pagamento" e não abrange os tokens de utilidade e os NFTs.

A nova lei estabelece as diretrizes a serem observadas na prestação de serviços virtuais, que serão elaboradas pelo órgão regulador a ser definido pelo Poder Executivo. O futuro órgão regulador deverá levar em conta critérios como livre iniciativa, livre concorrência, boas práticas de governança, transparência nas operações, segurança da informação e proteção de dados pessoais, proteção e defesa dos consumidores e usuários, poupança popular, solidez e eficiência das operações e prevenção à lavagem de dinheiro e ao financiamento ao terrorismo.

Acredita-se que o Banco Central do Brasil (BCB) seja o órgão responsável por regular o mercado de criptomoedas, dado seu papel na economia nacional e na autorização de instituições financeiras que buscam integrar o Sistema Financeiro Nacional (SFN).

1.4.4 Parecer de Orientação CVM 40

O Parecer de Orientação CVM 40 foi uma minuta regulamentária emitida pela Comissão de Valores Mobiliários (CVM) em 2022 que busca orientar investidores, emissores e intermediários sobre a aplicação da legislação brasileira aos criptoativos.

⁸⁸ NFT é um token não fungível que pode ser visto como uma unidade de informação digital (token) que é armazenada em um blockchain e não são inerentemente intercambiáveis com outros ativos digitais (não fungível). A não fungibilidade do ativo se caracteriza pelo registro da NFT no blockchain, que identifica quem é o real proprietário daquele ativo. Os tokens não fungíveis podem representar digitalmente qualquer ativo, incluindo ativos somente online, como arte digital e ativos reais, como imóveis. Outros exemplos de ativos que os NFTs podem representar incluem itens do jogo, como avatares, colecionáveis digitais e não digitais, nomes de domínio e ingressos para eventos.

O parecer inicia definindo o que é criptoativo, esclarecendo que se trata de representações digitais de valor que utilizam criptografia e tecnologia de registros distribuídos (DLT - *Distributed Ledger Technology*), como a blockchain, para garantir a sua integridade e segurança. Em seguida, o documento discorre sobre as principais características dos criptoativos, como a descentralização, a ausência de regulamentação específica, a volatilidade de preços e a falta de lastro em ativos tangíveis.

Uma das principais conclusões do Parecer de Orientação CVM 40 é que alguns criptoativos podem ser considerados valores mobiliários e, portanto, estarão sujeitos à regulamentação da CVM. De acordo com o documento, a análise deve ser feita caso a caso, levando em consideração critérios como a existência de uma oferta pública, a expectativa de lucros por parte dos investidores e a atuação de emissores e intermediários no mercado.

Outra questão abordada pelo parecer é a responsabilidade dos intermediários que atuam no mercado de criptoativos. Segundo a CVM, os intermediários que realizam a custódia, intermediação ou distribuição de criptoativos podem estar sujeitos à regulamentação da autarquia e devem adotar medidas de segurança e compliance para evitar atividades ilícitas, como a lavagem de dinheiro e o financiamento ao terrorismo.

O Parecer de Orientação CVM 40 também chama a atenção para os riscos associados ao investimento em criptoativos, como a falta de transparência das emissões, a ausência de garantias de liquidez e a falta de proteção dos investidores em caso de insolvência dos emissores. Por fim, o documento conclui que a regulamentação de criptoativos é um tema complexo e que a CVM continuará acompanhando a evolução do mercado e adotando medidas necessárias para proteger os investidores e garantir a integridade do mercado.⁸⁹

⁸⁹ CVM. **Parecer de Orientação CVM 40.** Disponível em: <<https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/pareceres-orientacao/anexos/Pare040.pdf>>, acesso em 05/03/2022.

1.4.5 Blockchain

O blockchain de um criptoativo (também definido como cadeia de blocos) é o livro-mestre que registra e armazena todas as transações e atividades anteriores, validando a propriedade de todas as unidades da moeda em qualquer momento. O registro de todo o histórico de transações de um criptoativo é o período amarelhado em uma blockchain e tem um comprimento finito - contendo um número limitado de transações - que aumenta com o tempo.

As tecnologias de blockchain estão cada vez mais populares, com o potencial de se tornarem uma poderosa força disruptiva. Indivíduos e organizações podem se beneficiar do blockchain com sua capacidade de aumentar a troca segura de dados e tornar essa transação mais simples e fácil entre entidades.

Cópias idênticas do blockchain são armazenadas em cada nó da rede de software do criptoativo - a rede de mineração de servidores descentralizados, administrada por indivíduos especializados em programação, ou grupos de indivíduos conhecidos como mineradores, que registram e autenticam continuamente as transações de criptoativos.⁹⁰

Uma transação de criptoativo tecnicamente não é finalizada até que seja adicionada ao blockchain, o que geralmente ocorre em minutos. Depois que a transação é finalizada, geralmente é irreversível. Ao contrário dos processadores de pagamento tradicionais, como PayPal e cartões de crédito, a maioria dos criptoativos não possui funções de reembolso ou estorno integradas, embora alguns criptoativos mais novos tenham recursos de reembolso rudimentares.

Durante o intervalo de tempo entre o início e a finalização da transação, as unidades não estão disponíveis para uso por nenhuma das partes. Em vez disso, eles são mantidos em uma espécie de *escrow*⁹¹ - limbo, para todos os efeitos e propósitos. O blockchain, portanto, evita gastos duplos ou a

⁹⁰ BURNISKE, Chris; TATAR, Jack. **Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond**. Editora: McGraw-Hill Education; 1st Edition, 2017.

⁹¹ Escrow é um acordo financeiro no qual duas partes contratam um "terceiro" (que não é o comprador nem o vendedor) para reter temporariamente dinheiro, papelada ou outros ativos para uma transação em seu nome antes que a transação seja finalizada.

manipulação do código do criptoativo a fim de impossibilitar que as mesmas unidades monetárias sejam duplicadas e enviadas a vários destinatários.

Cada detentor de criptoativo tem uma chave privada que autêntica sua identidade e permite a troca de unidades. Os usuários podem criar suas próprias chaves privadas, que são formatadas como números inteiros entre 1 e 78 dígitos, ou usar um gerador de números aleatórios para criar uma. Assim que tiverem uma chave, eles podem obter e dispor do criptoativo. Sem a chave, o detentor não pode gastar ou converter seu criptoativo - tornando seus bens inúteis a menos que a chave seja recuperada.

Embora seja um recurso de segurança crítico que reduz a possibilidade do furto e o uso não autorizado, também é draconiano. Perder sua chave privada é o equivalente digital a jogar um maço de dinheiro em um incinerador de lixo. Embora você possa criar outra chave privada e começar a acumular criptoativos novamente, não é possível recuperar os acervos protegidos por sua antiga chave perdida. Usuários experientes de criptoativos são, portanto, loucamente protetores de suas chaves privadas, normalmente armazenando-as em vários locais digitais (embora geralmente não conectados à Internet, para fins de segurança) e analógicos (ou seja, em papel).⁹²

Os desenvolvedores de criptoativos constroem esses protocolos com base em matemática avançada e princípios de engenharia da computação que os tornam virtualmente impossíveis de quebrar e, portanto, de duplicar ou falsificar as moedas protegidas. Esses protocolos também mascaram as identidades dos usuários de criptoativos, tornando as transações e os fluxos de fundos difíceis de serem atribuídos a indivíduos ou grupos específicos.

Dito isto, o capítulo 2 investigará o entrelaçamento entre o Direito Penal Econômico, a lavagem de dinheiro e a evasão de divisas pelo criptoativo. Portanto, será levantada a fase inquisitorial (antecedente à ação penal) e a importância do monitoramento do mercado não regulado de criptoativos, bem como se o aumento da popularização de criptoativos possui correlação a atividades

⁹² ELROM, Elad. **The Blockchain Developer**. Publisher: Apress; 1st ed. Edition, 2019.

criminais. Por fim, serão examinadas as diversas informações sobre aquisição e financiamento de atividades ilícitas pela *deep web/darknet* e o desaparecimento das barreiras fiscais e econômicas com o modelo deste meio.

Capítulo 2

A LIGAÇÃO DA TECNOLOGIA BLOCKCHAIN E TIPOS PENAIS

2.1 FASE INVESTIGATÓRIA: A IMPORTÂNCIA DO MONITORAMENTO POLICIAL DO MERCADO NÃO REGULADO DOS CRIPTOATIVOS

Um dos principais objetivos de toda investigação criminal é fornecer qualificação adequada das supostas atividades ilícitas às disposições correspondentes do direito penal, ou seja, definir os elementos do crime à subsunção da norma. Embora grande parte da prática atual a esse respeito seja moldada por legislação, normas, doutrina e jurisprudência, novas formas de atividade criminosa – o uso criminoso de moedas virtuais é um exemplo – podem exigir a necessidade em repensar e reajustar os instrumentos substantivos atualmente disponíveis. Portanto, o objetivo deste capítulo é identificar opções que estão sendo aplicadas no Brasil e outros procedimentos disponíveis no direito alienígena para abordar os elementos do crime de lavagem de dinheiro no contexto das moedas virtuais.

A fase investigatória é comandada pela polícia judiciária. A sua natureza é administrativa e antecede a jurisdição penal. O Código de Processo Penal preceitua no art. 4º que:

Art. 4º A polícia judiciária será exercida pelas autoridades policiais no território de suas respectivas circunscrições e terá por fim a apuração das infrações penais e da sua autoria.

Parágrafo único. A competência definida neste artigo não excluirá a de autoridades administrativas, a quem por lei seja cometida a mesma função.

PACELLI e FISCHER⁹³ descrevem que:

⁹³ PACELLI, Eugênio. FISCHER, Douglas. **Comentários ao Código de Processo Penal e sua**

Os procedimentos de investigação de fatos alegadamente criminosos não são considerados, em linguagem técnica, fase processual. Daí falar-se na natureza administrativa do inquérito policial, que, mesmo após a Constituição da República, de 1988, é o meio como qual o Estado busca o esclarecimento do caso penal, valendo-se, para tanto, dos ritos e formas legais previstas, por primeiro, no Código de Processo Penal, mas, também, em legislações esparsas. No modelo brasileiro, no qual convivem pelo menos duas espécies de jurisdição criminal comum, quais sejam a Justiça Federal e a Justiça Estadual, a polícia judiciária também obedece a essa lógica, o mesmo ocorrendo em relação ao Ministério Público. Assim, há a polícia judiciária dos Estados e a polícia judiciária federal, bem como o Ministério Público dos Estados e o Ministério Público da União. Em matéria penal, há também a jurisdição militar, o Ministério Público Militar, tanto da União quanto dos Estados, e as respectivas polícias judiciárias. No âmbito da Justiça Militar da União, tal função é exercida, em regra, pelas Forças Armadas. Ver, no ponto, o disposto no art. 144, incisos e parágrafos, da Constituição da República.

O inquérito policial é marcado por fomentar provas de materialidade e autoria ao Ministério Público. Destina-se à formação da *opinio delicto* daquele a quem a Lei atribui essa função. Todavia, deve-se observar que a investigação prévia não é imprescindível para o oferecimento da denúncia. O inquérito policial e o procedimento investigatório criminal (PIC), instaurado pelo *parquet*, são meios de colheita de provas, por exemplo, através do contraditório diferido. Contudo, crimes contra a ordem econômica ou financeira, em especial no meio digital, necessitam de celeridade investigativa interveniente que, de certo modo, inutilize a cadeia das fases da lavagem ou da possível evasão de divisas. Nesse sentido, o controle da fuga do capital, a transposição entre contas de terceiro, a colocação de recursos no sistema financeiro ou, até mesmo, a reintegração do capital ilícito deve ser assistida de forma não intermitente pelas autoridades.

A notícia de fato, a *notitia criminis* e a denúncia anônima de operações, comumente estimulam a origem investigatória. Outrossim, as

investigações administrativas realizadas pelos órgãos financeiros também são essenciais para o controle da lavagem de capital.

A exemplo disso, o COAF⁹⁴, em 2021, investigou cerca de 674⁹⁵ mil pessoas (físicas e jurídicas), supostamente envolvidas em esquemas de lavagem de dinheiro, sendo que 4 mil delas tinham envolvimento com criptomoedas.

Estimou-se⁹⁶ que US\$ 8.6 bilhões de dólares foram lavados em 2021 através do criptoativo. A informação foi noticiada pelo Chainalysis⁹⁷ e descreve que:

Overall, cybercriminals have laundered more than \$33 billion worth of crypto since 2017, Chainalysis estimated, with most of the total over time moving to centralized exchanges.

The firm said the sharp rise in money laundering activity in 2021 was not surprising, given the significant growth of both legitimate and illegal crypto activity last year.

Além do COAF, o Ministério da Justiça informou⁹⁸ que em 2022, agentes do FBI, da polícia federal dos EUA, da CIA, da central de inteligência do

⁹⁴ O significado de COAF é Conselho de Controle de Atividades Financeiras. A Lei nº 13.974, de 7 de janeiro de 2020, reestruturou o Conselho de Controle de Atividades Financeiras (Coaf), criado pela Lei nº 9.6134, de 3 de março de 1998, vinculando-o administrativamente ao Banco Central do Brasil. As competências do Coaf não foram alteradas. O Coaf é constituído no modelo administrativo. Em outras palavras, a UIF realiza trabalhos de inteligência financeira, não sendo de sua competência, por exemplo, realizar investigações, bloquear valores, deter pessoas, realizar interrogatórios e outras atividades dessa natureza.

⁹⁵ COINTELEGRAPH. **COAF investiga 674 mil pessoas por lavagem de dinheiro e 4 mil casos envolvem Bitcoin.** Disponível em: <<https://cointelegraph.com.br/news/coaf-investiga-674-mil-pessoas-por-lavagem-de-dinheiro-e-casos-tambem-envolvem-bitcoin>>, acesso em 23/06/2022.

⁹⁶ REUTERS. **Crypto money laundering rises 30% in 2021 -Chainalysis.** <<https://www.reuters.com/technology/crypto-money-laundering-rises-30-2021-chainalysis-2022-01-26/>>, acesso em 23/06/2022.

⁹⁷ Chainalysis é a plataforma de dados blockchain. Eles fornecem dados, software, serviços e pesquisas para agências governamentais, bolsas, instituições financeiras e empresas de seguros e segurança cibernética em mais de 70 países. Os dados impulsionam o software de investigação, conformidade e inteligência de mercado que tem sido usado para resolver alguns dos casos criminais mais importantes do mundo e aumentar o acesso do consumidor à criptomoeda com segurança.

⁹⁸ EXAME. **Polícia brasileira recebe treinamento do FBI sobre crimes com criptomoedas.** Disponível em: <<https://exame.com/future-of-money/policia-brasileira-recebe-treinamento-do-fbi-sobre-crimes-com-criptomoedas/>>, acesso em 23/06/2022.

governo norte-americano, e da *Homeland Security Investigations*⁹⁹ estiveram no Brasil para ministrar um curso com técnicas para prevenção, investigação e combate aos crimes envolvendo criptomoedas para 80 profissionais das forças de segurança brasileiras.

Essas investigações criminais administrativas são pautadas pela competência dada a administração pública, no exercício do poder de polícia, a zelar pela legalidade. PACELLI e FISCHER¹⁰⁰ pontuam que:

Investigações criminais administrativas: Embora reservada à autoridade policial a primazia na investigação criminal, agora realçada em cores mais vivas pela Lei nº 12.830/13, não só ela promove atividade de tal natureza, sobretudo nas hipóteses em que a ilicitude do fato não é exclusivamente penal. É que a Administração Pública, no exercício do poder de polícia, há de zelar pela regularidade e legalidade de diversos atos realizados pelo Poder Público, e, eventualmente, por particulares contra os interesses da Administração. Assim, e, por exemplo, a Fazenda Pública, estadual e federal, cuida do acompanhamento e fiscalização dos recolhimentos dos tributos devidos, do mesmo modo que a Previdência e Seguridade Social zelam pela arrecadação das contribuições sociais. E nesse mister podem e devem realizar procedimentos investigativos sempre que houver risco de violação às exigências legais. Na mesma linha, o Banco Central em relação às suas atividades fiscalizadoras e todas as demais entidades da Administração Pública de cujo exercício das funções resulte atividade e/de poder de polícia. Assim, as empresas públicas, as sociedades de economia mista, as autarquias, enfim, podem e devem instaurar procedimentos investigativos para o fim de apurar a prática de ilegalidades, seja por particulares (contra os interesses da Administração de que cuidam), seja pelos próprios servidores, no que respeita, sobretudo, à responsabilidade administrativa. E, evidentemente, tais procedimentos deverão ser

⁹⁹ Homeland Security Investigation (HSI) is the principal investigative arm of the U.S. Department of Homeland Security, responsible for investigating transnational crime and threats, specifically those criminal organizations that exploit the global infrastructure through which international trade, travel and finance move. HSI's mission is to investigate, disrupt and dismantle terrorist, transnational and other criminal organizations that threaten or seek to exploit the customs and immigration laws of the United States. <<https://www.ice.gov/about-ice/homeland-security-investigations>>

¹⁰⁰ PACELLI, Eugênio. FISCHER, Douglas. **Comentários ao Código de Processo Penal e sua jurisprudência**. – 9. ed. rev. e atual. – São Paulo: Atlas, 2017. p. 22.

encaminhados ao Ministério Público sempre que houver fundada suspeita de que os fatos então apurados possam se caracterizar também como ilicitude penal.

Em suma, a importância investigatória é cristalina, o embasamento do procedimento pré-processual é a prova vital da persecução penal. Os crimes cometidos no ambiente virtual, especialmente a lavagem de capital, e outros delitos vinculados ao criptoativo, são particularmente complexos. A cadeia percorrida pelo *iter criminis* da cripto transgressão é infinitamente mais ágil em relação a um delito comum. As barreiras nacionais – fronteiras, não são empecilhos para esta modalidade, sendo que por vezes, a ocultação do capital ocorre através da transferência entre diversas exchanges ao redor do mundo. Conseqüentemente, o Delegado de Polícia Civil ZUMAS¹⁰¹ argumenta que:

O investigador que, durante o cumprimento de um mandado de busca e apreensão no ano de 2020, depara-se com um pedaço de papel muito bem guardado contendo os dizeres: monkey – ball – garden – pencil – flower – door – bottle – lamp – air – book – rug – bag e não tem a menor idéia do que significa, deve se preocupar. Não se trata aqui de dizer O QUE FAZER, mas sim de PORQUE SABER O QUE FAZER. Apontamos a gritante necessidade de conhecimento mínimo necessário para conduzir investigações contemporâneas. O mínimo treinamento no assunto possibilitaria o investigador deduzir que aquela sequência de 12 palavras aleatórias poderia conduzir aos fundos do criminoso no ambiente das criptomoedas. Nem um centavo sequer poderia ser encontrado naquela residência, mas aquela sequência mnemônica de palavras aleatórias poderia representar, literalmente, milhões. E vamos mais longe, extorsões e outros delitos praticados por meio de aplicativos de mensageria parecem situações corriqueiras, porém caso a vantagem ilícita seja demandada com o fornecimento de uma wallet de criptomoedas, até mesmo o investigador mais experiente precisa ter cuidado. A privacidade proporcionada pelas transações em criptomoedas, sem a necessidade de um terceiro de confiança (como uma instituição financeira) e sequer de uma conta bancária vinculada a dados de pessoas ou empresas tem sido amplamente

¹⁰¹ ZUMAS, Vytautas Fabiano Silva. **Criptomoedas, crime e investigação**. Disponível em: <<https://www.direitonet.com.br/artigos/exibir/11637/Criptomoedas-criptocrime-e-criptoinvestigacao>>, acesso em 23/06/2022.

utilizada por criminosos para obtenção do proveito dos crimes praticados.

Desse modo, em que pese não exista, até então, regulamentação e efetiva fiscalização direcionada ao mercado de criptoativos no ordenamento jurídico, crimes através deste meio estão sendo praticados. Pirâmides financeiras, esquemas de ponzi, organização criminosa, lavagem de dinheiro, evasão de divisas, crimes contra a ordem econômica e contra consumidores são exemplos de condutas já conhecidas pela sociedade brasileira.

Para combater a crescente criminosa, o Ministério Público de Santa Catarina criou o CyberGaeco¹⁰² para defrontar crimes que envolvam bitcoin e criptomoedas. O CyberGaeco é uma unidade especializada em investigações de crimes cibernéticos, que já havia sido implementada no Estado de São Paulo pelo MPSP. Em informação ao canal COINTELEGRAPH¹⁰³, o MPSC¹⁰⁴ afirma que:

A Procuradoria aponta também que a prática de infrações penais em meios virtuais e de informática é um fenômeno que tende a crescer na mesma proporção em que aumenta a dependência humana a estes meios e que os efeitos das atividades das organizações criminosas que agem no ciberespaço são refletidos, direta ou indiretamente, em centenas de milhares de vítimas.

Além disso aponta que o contínuo desenvolvimento de ferramentas tecnológicas que permitem o anonimato na internet e o trânsito de moedas virtuais, tais como Bitcoins, Ethereum, Ripple, Bitcoin Cash, EOS, Litecoin, Cardano, Stellar, IOTA, TRON e outras criptomoedas de difícil rastreamento, acabam potencializando as

¹⁰² COINTELEGRAPH. **Ministério Público de Santa Catarina cria o CyberGaeco para combater crimes que envolvam bitcoin e criptomoedas.** Disponível em: <<https://cointelegraph.com.br/news/public-ministry-of-santa-catarina-creates-cybergaeco-to-fight-crimes-involving-bitcoin-and-cryptocurrencies>>, acesso em 03/08/2022.

¹⁰³ COINTELEGRAPH. **Ministério Público de Santa Catarina cria o CyberGaeco para combater crimes que envolvam bitcoin e criptomoedas.** Disponível em: <<https://cointelegraph.com.br/news/public-ministry-of-santa-catarina-creates-cybergaeco-to-fight-crimes-involving-bitcoin-and-cryptocurrencies>>, acesso em 03/08/2022.

¹⁰⁴ MPSC. **MPSC alinha parceria com MPSP para replicar em Santa Catarina o Cyber GAECO.** Disponível em: <<https://mpsc.mp.br/noticias/mpsc-alinhava-parceria-com-mpsp-para-replicar-em-santa-catarina-o-cyber-gaeco>>, acesso em 03/08/2022.

condutas criminosas e a efetividade das ações realizadas por meio da dark web.

Na mesma toada, o MPRS¹⁰⁵ criou um grupo especializado em combater crimes praticados na internet. Portanto, com o grave aprimoramento das condutas criminosas relacionadas à tecnologia, ponto central de combate é o aprimoramento e criação de grupos especializados, conforme menção, que sejam treinados e qualificados para identificar a origem de atividades suspeitas e possam impedir a propagação do crime em tempo real.

Por outro lado, a preocupação com a prática criminosa é global. O GAFI, entidade intergovernamental, emite pareceres e recomendações para que os países membros sigam e implementem no direito interno normas que possibilitem o combate, a prevenção e a persecução à lavagem de dinheiro. Três etapas são listadas pelo GAFI¹⁰⁶ como importantes para a prevenção, combate e investigação de crimes relacionados como criptoativos. São elas: *due diligence*, monitoramento de endereços de carteiras virtuais e compliance obrigatório e interno nas exchanges.

A *due diligence* do cliente é reconhecida como uma das principais medidas no combate à lavagem de dinheiro criptográfica. Durante o processo de *due diligence* do cliente, a empresa deve realizar duas coisas: identificar a entidade que se apresenta como cliente em potencial (ou seja, obter informações sobre a identidade e documentação de suporte) e verificar as informações fornecidas pelo cliente potencial durante a identificação.

Além do *due diligence*, quando se discute cripto anti-lavagem, ponto crucial é o monitoramento de endereços de carteiras com quem as transferências de cripto são realizadas por um determinado cliente. Para fazer isso, as exchanges estão empregando o que é conhecido como soluções de monitoramento on-chain,

¹⁰⁵ MPRS. **Cybergaeco: MPRS cria grupo especializado em combater crimes praticados na internet.** Disponível em: <<https://www.mprs.mp.br/noticias/53708/>>, acesso em 03/08/2022.

¹⁰⁶ FATF. **Virtual Currencies: Key Definitions and Potential AML/CFT Risks.** Disponível em <<https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html>>, acesso em 23/06/2022.

como as fornecidas por Crystal¹⁰⁷, Elliptic¹⁰⁸ ou Chainanalysis. Cada um desses provedores reúne as informações e permite rastrear as transferências no blockchain e avaliar onde o ativo passou de uma pessoa para outra. Claro, nem todas as criptomoedas podem ser rastreadas, como será visto em um subcapítulo posterior, e cada solução terá um ou outro lado forte. Por exemplo, a plataforma Crystal fornecerá uma avaliação da representação visual de uma carteira específica e ficará acima da Elliptic, em termos de visualização de quebra da criptografia, enquanto a Elliptic pode ser melhor em termos de rastreamento de uma transferência de valor singular.

Para um programa bem-sucedido de combate à lavagem de dinheiro criptográfico, além da especialização das forças policiais e órgãos competentes, os provedores também precisam combater a última etapa, ou seja, a integração. No entanto, os VASPs¹⁰⁹, especificamente aqueles que interagem com moedas fiduciárias (já que completariam o ciclo e é muito mais fácil gastar moeda fiduciária do que criptos), devem ter medidas adicionais para evitar que criminosos tenham a possibilidade de utilizar seus produtos do crime. Para fazer isso, limites poderiam ser impostos – o que significa que sempre que a pessoa deseja converter suas criptomoedas em fiat¹¹⁰ ou gastar acima de um determinado limite, ela é impedida de fazê-lo sem acionar o alerta. O próprio alerta notificaria o COAF e os levaria a fazer uma revisão da atividade de tal cliente, conduzindo a mais questionamentos e investigações de todas as atividades e, possivelmente, término do relacionamento/congelamento de ativos e, em teoria, seria gerado um relatório à unidade nacional de inteligência financeira. Ademais, além dos limites, o departamento de *compliance* dos VASPs deverão realizar uma revisão contínua das atividades dos clientes, como é feito por instituições financeiras (API, análise de perfil de investimentos). Tais medidas dificultariam o aproveitamento do produto

¹⁰⁷ A Crystal potencializa a análise e o monitoramento de transações de criptomoedas no blockchain, trazendo as melhores soluções de conformidade AML (anti money laundering) e gerenciamento de risco para exchanges, bancos e FIs.

¹⁰⁸ A Elliptic fornece análise de blockchain para conformidade de ativos criptográficos.

¹⁰⁹ virtual asset service provider.

¹¹⁰ Dinheiro corrente.

do crime e potencialmente poderiam levar à investigação que acabaria por impedir que novos crimes se materializassem.

Contudo, conforme descrito, a não regulamentação e fiscalização do mercado de ativos digitais proporcionam ao empreendedor criminal o caminho do sucesso. Várias operações já foram deflagradas pela Polícia Federal, Ministério Público e Autoridade Judicial com intuito de desmantelar organizações criminosas que utilizam deste meio para a prática de crimes. A Operação Lamanai, deflagrada em outubro de 2019, apurou que R\$ 12 bilhões¹¹¹ de reais foram desviados de clientes através de um esquema piramidal que envolveu organização criminosa, lavagem de capital e outros crimes financeiros. A Operação KryptosAgentes, da Polícia Federal, deflagrada em 2021, bloqueou R\$ 38 bilhões¹¹² de reais das contas da empresa alvo por suspeita de crimes financeiros, lavagem de capital e pirâmide financeira.

Logo, a tecnologia está avançando em um ritmo vertiginoso. Isso traz um perigo significativo, pois essas mudanças têm o potencial de tornar a tecnologia, incluindo blockchain, meios empregados na prática criminal. Dada a rápida taxa de mudança tecnológica, são necessários infraestrutura de informações e modelos de investigações criminais em criptomoedas. Dessa forma, a sociedade pode entender os riscos tecnológicos dos criptoativos e tomar decisões informadas.

Por fim, constata-se que qualquer sistema não regulamentado tem a capacidade de financiar atos criminosos. Como resultado, é necessário um processo de *due diligence* semelhante ao de um banco. Isso pode ajudar a acompanhar as identidades reais dos investidores e verificar suas localizações quando estão comprando ou vendendo criptomoedas. Em tese, qualquer violação de tais normas devem ser punida com severas sanções.

¹¹¹ CLICRBS, Gaucha Zh. **Caso Unick: Polícia Federal conclui inquérito sobre esquema que teria lesado clientes da empresa em R\$ 12 bilhões.** Disponível em: <<https://gauchazh.clicrbs.com.br/seguranca/noticia/2021/05/caso-unick-policia-federal-conclui-inquerito-sobre-esquema-que-teria-lesado-clientes-da-empresa-em-r-12-bilhoes-ckoltpoya006w01807t4pcr26.html>> acesso em 22/06/2022.

¹¹² TECNOBLOG. **GAS Consultoria Bitcoin tem R\$ 38 bilhões bloqueados e deixa de pagar clientes.** Disponível em <<https://tecnoblog.net/noticias/2021/09/16/gas-consultoria-bitcoin-tem-r-38-bilhoes-bloqueados-e-deixa-de-pagar-clientes/>>, acesso em 22/06/2022.

Consequentemente, este subcapítulo identificou a publicidade de atividades ilícitas praticadas pelo meio de criptoativos, registrados na blockchain. É do estudo que crimes utilizando criptomoedas estão se tornando mais comuns, pois atores criminais que empregam da atividade ilícita buscam novas técnicas para ofuscar seus rastros. As investigações geralmente envolvem o rastreamento de fundos à medida que são transferidos por vários tokens ou cadeias. Tornar obrigatório a necessidade de relatar descobertas estranhas, atos distintos da prática usual, suspeitas de fraude, lavagem de dinheiro ou outras condutas pelas exchanges e players do mercado digital é o centro de combate ao crime organizado e necessário para a contenção da crescente criminosa.

Desse modo, o próximo subcapítulo tem por finalidade identificar a correlação da popularização dos criptoativos com a atividade criminal.

2.2 O AUMENTO DA POPULARIZAÇÃO DOS CRIPTOATIVOS E A CORRELAÇÃO COM A ATIVIDADE CRIMINAL

Os criptoativos estão alimentando um novo tipo de onda de crimes. Computadores conectados através de redes interligadas são continentes sem lei no qual criminosos navegam para onde querem, entrando em indústrias, comércios e residências, furtando dados¹¹³ em grandes quantidades para vender e permitir a prática de outros crimes concatenados. Essas novas condutas estão em ascendência. O Bitcoin, meio de pagamento construído para operar através de computadores e redes, adicionou elemento disruptivo através de pagamentos anônimos para e entre criminosos. Criminosos de todo o mundo foram inspirados por essa maneira quase instantânea e sigilosa de pagar e aceitar dinheiro, para modernizar crimes existentes e elaborar novas fases do *iter criminis*.¹¹⁴

¹¹³ A JBS pagou US\$ 11 milhões em criptomoeda para resolver ataque de hackers que paralisou operações nos Estados Unidos e na Austrália. A informação é do The Wall Street Journal, revelada em 09/06/2021. Disponível em: <<https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781>>, acesso em 31/07/2022

¹¹⁴ LUI, Alison; RYDER, Nicholar. **Fintech, Artificial intelligence and the law**. Published in 2021: by Routledge, New York.

De acordo com um relatório emitido pela Chainalysis¹¹⁵ (The Chainalysis 2022 Crypto Crime) baleias¹¹⁶ criminosas detêm em carteiras digitais (on-line e offline) mais de US\$ 25 bilhões em criptoativos de diversas origens ilícitas. No geral, a Chainalysis identificou 4.068 baleias criminosas com mais de US\$ 25 bilhões de criptomoeda. Baleias criminosas representam 3,7% de todos os maiores investidores em criptomoedas – ou seja, carteiras privadas com mais de US\$ 1 milhão em criptomoedas.

Contudo, o crescimento criminal tem chamado atenção das autoridades policiais, o relatório¹¹⁷ descreve que:

One positive development in the last year has been law enforcement's growing ability to seize cryptocurrency from criminals. We saw several examples of this in 2021, including: • The U.S. Department of Justice (DOJ) seizing \$2.3 million worth of cryptocurrency from the DarkSide ransomware operators responsible for the attack on Colonial Pipeline, as we cover in-depth in our ransomware section. • IRS-CI's cumulative seizures of over \$3.5 billion worth of cryptocurrency over the course of 2021. London's Metropolitan Police Service (MPS) made the UK's largest ever seizure of cryptocurrency, taking £180 million worth from a suspected money launderer.

As condutas criminais identificadas pelo meio de pagamento digital foram: *Malware*¹¹⁸, tipificado no art. 154-A do Código Penal; financiamento ao terrorismo, tipificado no art. 6 da lei 13.326 de 2016; furto digital (qualificado), tipificado no art. 155, § 4º-B, do Código Penal; estelionato eletrônico, tipificado no art. 171, § 2º-A, do Código Penal; *rasomware* que possui a mesma tipificação que o crime de *Malware*; venda de pornografia infantil, previsto no art. 241-A lei 8.069

¹¹⁵ CHAINANLYSIS. **The 2022 Crypto Crime Report.** disponível em: < <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>>, acesso em 31/07/2022.

¹¹⁶ meaning criminals holding \$1 million or more in cryptocurrency.

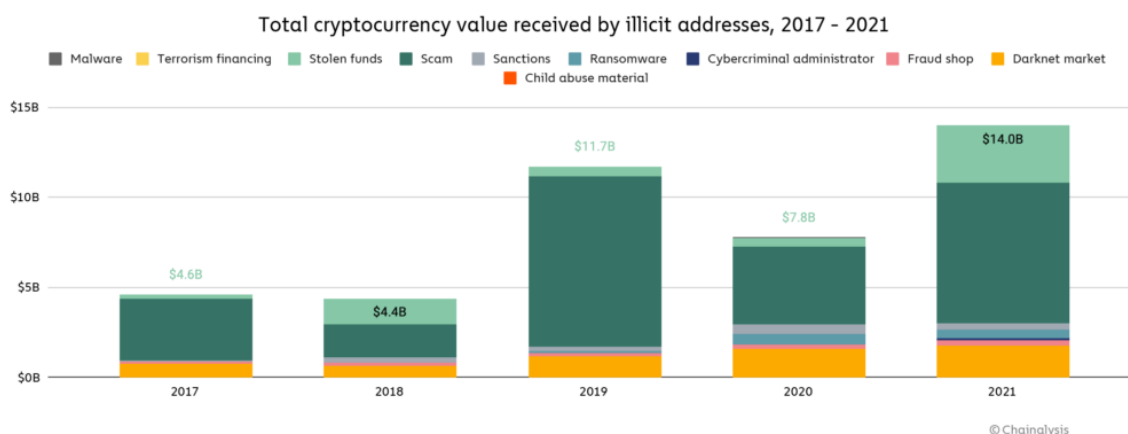
¹¹⁷ CHAINANLYSIS. **The 2022 Crypto Crime Report.** disponível em: < <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>>, acesso em 31/07/2022 p. 23.

¹¹⁸ Software projetado especificamente para interromper, danificar ou obter acesso não autorizado a um sistema de computador.

de 1990; venda de objeto ilícitos na *darknet*; venda de mercadoria em sites fakes (cópia fiel de um site conhecido) que caracteriza, em tese, estelionato;

Os delitos praticados pelo criptoativo atingiu recorde histórico em 2021, com endereços ilícitos recebendo US\$ 14 bilhões ao longo do ano, acima dos US\$ 7,8 bilhões em 2020 (Figura 1).

Figura 1 – Total de moeda digitais recebidas por endereços ilícitos



Fonte: CHAINANLYSIS, p. 3.

Logo, o uso de criptoativos como facilitador de esquemas criminosos aumentou vertiginosamente e a aceitação deste meio de pagamento foi acelerada pelo mercado descentralizado. No entanto, o número geral e o valor de transações de criptomoeda relacionadas a atividades criminosas ainda representam apenas uma parcela pequena, quando comparada a crimes praticados com Fiat (moeda corrente) e outras formas de transações. Algumas justificativas são lógicas, como a alta volatilidade do ativo digital que impõe um fator importante e os riscos digitais.¹¹⁹

Infere-se, portanto, que o uso criminoso de criptoativos não está mais confinado a atividades voltadas ao crime cibernético, pelo contrário, o estudo demonstra a relação de uma gama e tipos de crime que exigem transmissão de

¹¹⁹ EUROPOL. **Cryptocurrencies tracing the evolution of criminal finances.** Disponível em: <<https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf>>, acesso em 31/07/2022.

valor monetário. No entanto, a escala e a participação do uso ilícito de criptoativos como parte de atividades criminosas é difícil de se estimar. A própria característica do ativo, que foi ventilada no capítulo 1, dificulta a identificação da cadeia criminosa.

Adentrando especificadamente no tema central, estima-se, pela quantidade de criptomoedas enviadas de endereços ilícitos para endereços hospedados por serviços, que cibercriminosos lavaram aproximadamente US\$ 8,6 bilhões em criptomoedas em 2021¹²⁰. Com fito comparativo, o escritório de drogas e Crime da ONU estima que a quantidade de dinheiro lavado globalmente em um ano é de 2 a 5% do PIB global, ou US\$ 800 bilhões a US\$ 2 trilhões de dólares. No geral, foi lavado mais de US\$ 33 bilhões de dólares em criptomoedas desde 2017, com a maior parte do total passando ao longo do tempo para exchanges centralizadas. Assim, a lavagem de dinheiro representou apenas 0,05% de todo o volume de transações de criptomoedas em 2021.

Os criminosos que lidam com criptomoedas compartilham um objetivo comum: transferir seus fundos ilícitos para um serviço onde possam ser mantidos a salvo das autoridades e eventualmente convertidos em dinheiro. É por isso que a lavagem de dinheiro sustenta todas as outras formas de crimes baseados em criptomoedas. Se não houver como acessar os fundos, não há incentivo para cometer crimes envolvendo criptomoedas.

A maior diferença entre a lavagem de dinheiro baseada em moeda fiduciária e criptomoeda é que, devido à transparência inerente das blockchains, é possível rastrear mais facilmente como os criminosos movem criptomoedas entre carteiras e serviços em seus esforços para converter seus fundos em dinheiro.

Conforme supramencionado, o uso ilícito de criptomoedas está predominantemente associado ao fim de lavagem de dinheiro, comércio (online) de bens e serviços ilícitos e fraude.

¹²⁰ OCCPR. **Report: Money Laundering via Cryptocurrencies up 30% in 2021**. Disponível em: <https://www.occrp.org/en/daily/15898-report-money-laundering-via-cryptocurrencies-up-30-in-2021#:~:text=Money%20laundering%20via%20cryptocurrencies%20increased,by%20blockchain%20analysis%20firm%20Chainalysis>. Acesso em 31/07/2022.

A lavagem é facilitada pelo uso do sistema DeFi¹²¹, no qual é adstrito a um mercado sem intervenção estatal, conforme identificado pela EUROPOL¹²²:

Criminals now increasingly add steps to their laundering processes and rely on unlicensed exchanges. These exchanges often impose loose KYC requirements and allow illicit cryptocurrency trades by exchanging funds across various markets. Some exchanges have been accused of facilitating money laundering activities and illicit transactions using fake and stolen identities.

Não obstante a blockchain seja imutável e o rastro de negociabilidade seja fixado permanentemente nela, o anonimato¹²³, gerado pela chave digital, sem identificação de quem está por trás daquela carteira e a descentralização proporcionam um ambiente favorável para os criminosos. Conforme mencionado no capítulo 1, é importante lembrar que as criptomoedas não são anônimas. Cada transação é registrada na blockchain, que é um registro de todas as transações distribuídas a todos os usuários da rede. A maioria das blockchains estão disponíveis publicamente, tornando as transações rastreáveis. No entanto, vários serviços e técnicas podem aumentar o anonimato e dificultar as investigações policiais. As *privacy coins*¹²⁴ também podem ocultar (partes) de sua

¹²¹ Decentralized Finance: Decentralized finance (DeFi) is an emerging financial technology based on secure distributed ledgers similar to those used by cryptocurrencies. The system removes the control banks and institutions have on money, financial products, and financial services.

¹²² EUROPOL. **Cryptocurrencies tracing the evolution of criminal finances.** Disponível em: <<https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf>>, acesso em 31/07/2022, p. 8.

¹²³ Para ARRABAL, ENGELMANN e MELO o anonimato é: Em certo sentido, o anonimato cibernético pode ser visto como uma categoria paradoxal, pois permite a integração na rede sem revelar a identidade. Essa concepção está fundamentada na lógica do controle, uma vez que o indivíduo anônimo busca ter o poder de escolher os efeitos de suas ações e comunicações na rede. A ideia de liberdade como autonomia sugere que a ação individual é governada pela vontade do agente, e atribui-se ao indivíduo a responsabilidade pela tomada de decisões relacionadas à sua própria existência. Sob essa perspectiva, surge o anonimato cibernético, que muitas vezes é confundido equivocadamente com a noção de privacidade e proteção de direitos individuais. ARRABAL, Alejandro Knaesel. ENGELMANN, Wilson. MELO, Milena Petters. **Liberdade e anonimato no contexto da cibercultura.** Revista De Direitos E Garantias Fundamentais, 18(2): 2018.

¹²⁴ Moedas de privacidade são criptomoedas que obscurecem transações em seu blockchain para manter o anonimato de seus usuários e suas atividades. Os participantes de uma transação saberão o valor transacionado e as partes envolvidas. No entanto, a mesma informação será inalcançável para qualquer observador externo.

blockchain. A descentralização deste sistema financeiro oferece oportunidades adicionais porque contorna o papel de verificação de uma autoridade central tradicional, bem como as restrições geográficas. Isso não apenas permite transações internacionais extremamente rápidas, mas também oferece a possibilidade de explorar lacunas regulatórias entre jurisdições

Portanto, com o criptoativo, tudo o que é necessário para mover e transferir fundos de um país para outro é uma conexão com a internet. Como não há uma autoridade central regulando as transações, os fundos podem ser facilmente movidos entre países dentro da rede estabelecida pela criptomoeda. Nesse diapasão, PIFFER, CRUZ e TEIXEIRA¹²⁵ afirmam que:

E eis a constatação: fixou-se um novo paradigma monetário, de caráter transnacional, dentro de um ilimitado e desterritorializado universo virtual, por meio de um sistema de fluência transfronteiriço que poderia ser regulado pelo estabelecimento de diretrizes a partir de um Direito Transnacional, “aplicado por instituições com órgãos e organismos de governança, regulação, intervenção [...]”, tornando-se factível quando do efetivo estabelecimento de “espaços públicos transnacionais”, quiçá, em um ambiente virtual.

E complementam¹²⁶:

[...] o advento da evolução tecnológica do Século XX, com a manutenção de um sistema econômico transnacional com informações instantâneas por meio da internet, se mostrou controlável pelos Estados até a utilização de cartões ou “dinheiro plástico”. Mas as transformações advindas a partir desse ponto mudaram esta perspectiva. Deste modo, abordar o assunto sob a ótica soberana estatal não se apresenta mais como meio adequado, para não dizer impraticável. Isso corrobora com a afirmação de que a partir da criação das moedas digitais e criptomoedas se instaurou um novo paradigma monetário, ou seja, a transnacionalidade das moedas digitais como um novo modelo descentralizado, virtual, independente dos poderes e controle

¹²⁵ PIFFER, C.; CRUZ, P. M.; TEIXEIRA, A. V. **Da transnacionalidade financeira de Bretton Woods às moedas digitais**. Revista Justiça do Direito, v. 34, n. 1, p. 6-28, 30 abr. 2020. p. 23.

¹²⁶ PIFFER, C.; CRUZ, P. M.; TEIXEIRA, A. V. **Da transnacionalidade financeira de Bretton Woods às moedas digitais**. Revista Justiça do Direito, v. 34, n. 1, p. 6-28, 30 abr. 2020. p. 24.

estatais, criado a partir da transnacionalização do capital e em concomitância com a evolução tecnológica.

À vista disso, como o blockchain é compilado por pares, cada nó teria que ser desconectado para causar um colapso do sistema. Esse design permite que a rede seja resiliente a distúrbios externos, facilitando maior portabilidade na transferência de fundos ilícitos.

A lavagem de dinheiro pelo ativo digital não é exatamente praticada de apenas uma única maneira. O GAFI, o GAO e outras entidades competentes no combate à lavagem listam que as modalidades mais conhecidas são: *Tumblers*, *OTC Trading*, *Privacy Coins*, *Dexs*, aquisição direta de bens e mineração como fachada.

Tumblers são uma das ferramentas proeminentes para lavagem de criptoativos para moeda corrente e se concentram predominantemente nas principais moedas, como Bitcoin, Litecoin ou Ethereum. Também conhecidos como serviços de mixagem, eles operam a partir de sites na *clearnet* (Smartmixer, Bitcoin Mixer, JoinMarket, entre outros.) Os *mixers* efetivamente interrompem o vínculo transacional entre as carteiras, literalmente misturando transferências legítimas de Bitcoin com ganhos ilícitos e enviando os fundos virtuais resultantes para um novo endereço. Após a remoção das taxas de serviço, as moedas lavadas são sacadas através do Paypal ou Western Union. As limitações de tamanho associadas ao limite fiduciário limitam a eficácia das instalações da descoberta do crime, mas, uma vez que as moedas estejam limpas, outras vias de saque se abrem, pois, as transações não estão mais sob suspeita. Além disso, nenhum limite de tamanho se aplica a negociações criptográficas.¹²⁷¹²⁸¹²⁹

¹²⁷ FATF. **Virtual assets and virtual asset service providers**. Disponível em: <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>>, acesso em 02/08/2022. p. 82.

¹²⁸ MOSLAVAC. **Cryptocurrency tumbler: legality, legalization, criminalization**. Disponível em: <<http://www.mpce.mp.br/wp-content/uploads/2019/12/ARTIGO-12.pdf>>, acesso em 02/08/2022.

¹²⁹ GAO, U.S. Government Accountability Office. **Trafficking: Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking**. Disponível em: <<https://www.gao.gov/products/gao-22-105101>>, acesso em 01/06/2022.

MOSLAVAC¹³⁰ leciona que a utilização de Tumblers deve ser criminalizada e que o único propósito para utilização de tal de serviço é a lavagem de dinheiro:

CRIMINALIZATION OF TUMBLERS

Mere prohibitions shouldn't be the only content of a legal order. Through-out regulations and in every single case included, legislator must provide positive measures to preserve and/or reinstate determined law institute. Criminal law itself, considering its primary punishment nature, must not be limited to prohibitions and punishments. Tumblers should be criminalized due to their potential use in illegal activities. On the other side, every technology could be potentially used for unlawful activity. Criminalization must depend about real danger of abuse and potential harm or damage to the society itself. One must ask himself isn't using cryptocurrency tumbler in fact money laundry. Also, every act of making some activity illegal, necessary means that same activity was previously legal. Drug abuse is illegal on a count of the fact that taking drugs is health hazard. But that's not the case with prostitution, because sex isn't illegal mater. Although, prostitution is the misdemeanor offense for the reason of public morality. That's not the case with cryptocurrency tumbler, because we stated before in text, it isn't legal or legalized yet. If criminalization of tumblers at the end takes part, legislators are to instruct jurisdiction- focused principles over punishments. Governments could decide for partial prohibition of a blockchain and tumblers in that context aren't exception, due to possible use for money-laundry.

Assim sendo, esta modalidade de lavagem de dinheiro através de *mixers* é usualmente conhecida pelas autoridades, mas que apresenta complexidade investigatória dada as circunstâncias da tecnologia empregada.

Já, Over-The-Counter ou OTC Trading no contexto de Bitcoin e criptomoedas, são negócios privados para compra ou venda dos ativos digitais. Essas transações não são realizadas em exchanges regulares, não há livro de ofertas públicas. Isso fornece maior privacidade para compradores e vendedores.

¹³⁰ MOSLAVAC. **Cryptocurrency tumbler: legality, legalization, criminalization**. Disponível em: <<http://www.mpce.mp.br/wp-content/uploads/2019/12/ARTIGO-12.pdf>>, acesso em 02/08/2022. p. 221.

OTC é por natureza um serviço íntimo e personalizado. Os OTC Traders conservam uma rede de investidores e vendedores de criptomoedas. Além disso, as maiores organizações de OTC mantêm inventário de várias criptomoedas para atender a demanda projetada a qualquer momento. Para negociações de criptomoedas para dinheiro corrente e vice-versa, o mercado OTC é implacável. O volume de transações de balcão é estimado em três ou quatro vezes o tamanho dos mercados oficiais. Existem duas maneiras principais para negociações OTC; através de um corretor (Kraken, Bitstocks, Genesis Trading, entre outros) ou fundos especializados. A rampa de saída (cripto para fiduciário) para essas transações ainda exige um relacionamento bancário, de modo que são de menor interesse para os lavadores de dinheiro, a menos que as moedas tenham sido lavadas antes de chegar ao corretor. Como as transações de criptografia não exigem uma troca organizada, duas pessoas podem simplesmente trocar chaves públicas [ou digitalizar um código de resposta rápida (QR)] para concluir uma negociação de criptografia para criptografia.

As conversões da Fiat exigem uma reunião presencial com dinheiro na mesa e os provedores de serviços OTC geralmente cobram uma taxa de 3% a 8% por seus serviços.

Desse modo, OTC é uma ferramenta originária do mercado de ações tradicional. Significando, em síntese, que esse tipo de transação não se reflete no mercado, pois é feita diretamente entre o vendedor e o comprador, contornando todo o mercado.

Por sua vez, *privacy coins* são moedas privadas, negociadas diretamente entre comprador e vendedor. Em resposta à crise de 2008, Nakamoto (2008) apresentou, através do conhecido artigo¹³¹ (Bitcoin: A Peer-to-Peer Electronic Cash System) uma moeda transparente desprovida de controle externo. Até agora, esse empreendimento revolucionário é relativamente bem-sucedido, mas a rastreabilidade da bitcoin deixou nos empreendedores criminais a sensação de vulnerabilidade. Assim, desenvolvedores logo formularam uma solução

¹³¹ Disponível em: <https://bitcoin.org/bitcoin.pdf>.

alternativa e, de 2014 a 2016, moedas como Monero, Dash e Zcash foram criadas com um único fito: anonimato. Essas moedas implementam ativamente um livro-razão público ofuscado, onde qualquer adquirente pode transmitir, mas a fonte, o valor e o destino estão ocultos. Zcash e Dash são *hard forks*¹³² do blockchain do Bitcoin, então eles compartilham vulnerabilidades semelhantes. A credibilidade é que o sigilo associado a essas criptomoedas é rígido.

O GAFI¹³³ descreve que a negociação de *privacy coins* é uma *red flag*, a qual indica a prática criminosa:

This set of indicators draws from the inherent characteristics and vulnerabilities associated with the underlying technology of VAs. The various technological features below increase anonymity and add hurdles to the detection of criminal activity by LEAs. These factors make VAs attractive to criminals looking to disguise or store their funds. Nevertheless, the mere presence of these features in an activity does not automatically suggest an illicit transaction. For example, the use of a hardware or paper wallet may be legitimate as a way to secure VAs against thefts. Again, the presence of these indicators should be considered in the context of other characteristics about the customer and relationship, or a logical business explanation.

[...] Transactions by a customer involving more than one type of VA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins.

De acordo com o site INVESTOPEDIA¹³⁴, especializado em finanças, mercados digitais e títulos e valores mobiliários, os criptoativos com maior

¹³² Um hard fork (ou hardfork), no que se refere à tecnologia blockchain, é uma mudança radical no protocolo de uma rede que torna válidos blocos e transações anteriormente inválidos, ou vice-versa. Um hard fork requer que todos os nós ou usuários atualizem para a versão mais recente do software de protocolo.

¹³³ FATF. **Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing**. Disponível em: <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>>, acesso em 03/08/2022. p. 9.

¹³⁴ INVESTOPEDIA. **The 6 Most Private Cryptocurrencies**. Disponível em: <<https://www.investopedia.com/tech/five-most-private-cryptocurrencies/>>, acesso em 03/08/2022.

privacidade são: Monero, Zcash, Dash, Horizen Verge e Beam. O canal informativo destaca ainda:

Although Bitcoin remains the most popular choice, it is by government agencies. They have become quite good at tracing Bitcoin transactions, creating a strong incentive to switch to more private cryptocurrencies. Bitcoin has been a popular choice to protect a user's identity and as a result, transactions are constantly being targeted and monitored by government agencies. They have become quite good at tracing Bitcoin transactions, creating a strong incentive for users to switch to more private cryptocurrencies like those listed here.

Logo, em síntese, *privacy coins* são criptomoedas exclusivas que permitem ao usuário o anonimato total nas transações na blockchain, assim, tanto a identidade dos usuários, quanto as origens de suas transações são totalmente protegidas. Essas moedas permitem que remetentes e destinatários permaneçam anônimos com diferentes níveis de privacidade, como endereços de carteira ocultos e saldos de transações. Com as *privacy coins*, os pagamentos permanecem privados. Nesse sentido, a rastreabilidade, característica notória do registro na blockchain da moeda comum (bitcoin), é completamente ofuscada pela negociação destes criptoativos, proporcionando ao ator criminal o exaurimento da lavagem de capital sem deixar vestígios no livro registral.

Em contrapartida, Decentralized exchanges (DEXs) são distintos dos mercados organizados (centralized exchanges) que operam sob a vigilância de um custodiante, pessoa jurídica, que é, em última instância, responsável pelo cumprimento das normas emitidas por órgãos reguladores. As negociações realizadas pelo mercado organizado têm uma desvantagem notável; os usuários não têm acesso às suas chaves privadas, pois estas são mantidas em um depósito consolidado controlado pelo custodiante. No meio financeiro existe, inclusive, um ditado popular que exemplifica essa prática “não são suas chaves, não são suas moedas!”. Além disso, as exchanges centralizadas estão constantemente sob ataque de hackers e alguns são bem-sucedidos. Por exemplo, a plataforma de

negociação japonesa Coincheck¹³⁵ teve sua carteira furtada (avaliada em um valor de mercado de US\$ 530 milhões) em 2018. Em razão desta deficiência uma nova geração de trocas surgiu recentemente, conhecidas como DeFi (Decentralized Finance Exchanges), LIN¹³⁶ define DEX como:

The term “decentralized exchange” generally refers to distributed ledger protocols and applications that enable users to transact cryptocurrencies without the need to trust a centralized entity to be an intermediary for the trade or a custodian for their cryptocurrencies.

Esses mercados operam on-line anonimamente, usando contratos inteligentes *on-chain* e não exigem um endereço de e-mail para concluir uma transação. Nesse sentido, LIN¹³⁷, afirma que:

The term “decentralized exchange” is used colloquially to describe both blockchain-based exchange protocols, as well as applications that leverage the protocols. A decentralized exchange protocol generally describes a software program, hosted on or integrated into one or more distributed ledgers (e.g., Ethereum), that enables peer-to-peer transactions that are automatically settled on the distributed ledger. Users retain sole custody of their private keys throughout the transaction process.

As DEXs permitem que usuários controlem suas chaves privadas, elas são distribuídas para que não sofram de um único ponto de falha potencial (tempo de inatividade do servidor), não envolvem terceiros, não há risco de contraparte e não podem ser encerradas por governos. Por outro lado, LIN¹³⁸ destaca que há riscos na utilização de tal serviço, pois o usuário deverá confiar no operador da DEX:

¹³⁵ FORTUNE. **How to Steal \$500 Million in Cryptocurrency.** Disponível em: <<https://fortune.com/2018/01/31/coincheck-hack-how/>>, acesso em 03/08/2022.

¹³⁶ LIN, Lindsay X. **Deconstructing decentralized exchanges.** <<https://assets.pubpub.org/ob89i66u/61573938834913.pdf>>, acesso em 03/08/2022. p. 58.

¹³⁷ LIN, Lindsay X. **Deconstructing decentralized exchanges.** <<https://assets.pubpub.org/ob89i66u/61573938834913.pdf>>, acesso em 03/08/2022. p. 59.

¹³⁸ LIN, Lindsay X. **Deconstructing decentralized exchanges.** <<https://assets.pubpub.org/ob89i66u/61573938834913.pdf>>, acesso em 03/08/2022. p. 76.

Different decentralized exchange applications require different levels of user trust. Users may need to trust: (1) the decentralized exchange application creator and operator to perform activities such as hosting and publishing order books or performing order matching, (2) the underlying decentralized exchange protocol, including relevant smart contracts, and (3) the security, miners, and validators of the underlying distributed ledger. Users must trust each part of the exchange application stack to perform its job fairly, reliably, and securely. If any part of the stack fails, users may be unable to reliably and securely submit and fill orders, match with orders that meet their specified criteria, and confirm the settlement of trades. Moreover, users may find that trusted parties could censor some of their transactions or act in a self-interested manner to the users' detriment.

Portanto, depreende-se que no que tange DEXs não há regras de *know your customer* (KYC). Em essência, os usuários de criptomoedas se tornam seus próprios bancos, proporcionando acesso livre a toda e qualquer fase da lavagem de dinheiro oriunda de ilícitos penais.

Em prosseguimento, a aquisição diretamente de bens através de criptoativos é um dos meios mais protegido na lavagem de criptoativos, pois é o processo *off-ramp* (offline); a troca de moeda digital por moeda fiduciária, como dólares, euros ou ienes. Na maioria dos casos, o grande volume financeiro oriundo da atividade criminal torna o processo complexo e os depósitos bancários diretos deixam um rastro a ser seguido (*follow the money*). Por isto, prática usual, replicada em filmes e seriados, é a aquisição de grandes ativos (imóveis, carros, joias, artes, vinhos, entre outros produtos de valor agregado) com os rendimentos ilícitos, em dinheiro, e depois revender o ativo no mercado aberto. Ocorre que, nos dias atuais, trazer uma mala cheia de dinheiro para comprar uma casa causaria espanto – embora a prática ainda exista em alguns mercados. DUPUIS e GLEASON¹³⁹ afirmam que a prática é a mesma com criptoativos:

The same process applies to crypto purchases, minus the negative stigma. While the fad lasts, it is actually considered innovative and

¹³⁹ DUPUIS, D. GLEASON, K. **Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic.** Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3681297>, acesso em 03/08/2022.

remarkable, in a positive way, to purchase real estate with Bitcoin. The practice is gaining such popularity that Bitcoin RealEstate is presently developing a website, Dubai property developers now accept cryptocurrency¹⁴⁰.

Não obstante a troca de criptoativos por bens móveis e imóveis seja visto com uma prática lícita, a aquisição de mercadorias conforme supramencionado com o criptoativo ofusca, de certo modo, a rastreabilidade do capital ilícito inserido no mercado. A ANOREG¹⁴¹ retrata que foi:

Apresentado no Senado Federal, um projeto de lei quer criar orientações sobre a compra de casa, apartamentos e outros imóveis com criptomoedas. No Brasil, não é proibido negociar e adquirir bens com essas moedas digitais, que apesar de não serem reconhecidas como dinheiro pelo Governo Federal, tem valor entre as pessoas.

E são vários os casos de negociações de criptomoedas já realizados no país. Inclusive, grandes empresas listadas na bolsa de valores já buscam oferecer essa solução de pagamentos para seus clientes, como a Even, por exemplo, que foi a primeira empresa listada na B3 a aceitar pagamentos em Bitcoin.

Nessa modalidade o criptoativo é visto como a porta de entrada para aquisição de um mercado que terá como objetivo a lavagem e exaurimento do crime.

Ao fim, a mineração como fachada (*mining as a front*) é outro método identificado pelas autoridades competente é a mineração como fachada (*mining as a front*). A modalidade é uma conhecida tática usada em todo o mundo; canalizar os fundos ilícitos para um negócio intensivo em dinheiro, pagar os impostos resultantes e reintegrar à vontade o dinheiro limpo. O contra-ataque mais comum a essa forma de lavagem consiste na análise de fluxos de caixa para negócios

¹⁴⁰ HGTV. **How to buy real estate with bitcoin**. Disponível em: <www.hgtv.com/lifestyle/real-estate/how-to-buy-real-estate-with-bitcoin>, acesso em 03/08/2022.

¹⁴¹ ANOREG. **Comprou imóvel com criptomoedas? Senado Federal analisa projeto de lei sobre questão**. Disponível em: <<https://www.anoregpr.org.br/comprou-imovel-com-criptomoedas-senado-federal-analisa-projeto-de-lei-sobre-questao/>>, acesso em 03/08/2022.

suspeitos, mas, para ser eficaz, esse método depende de dados estatísticos, que provavelmente são incompletos para um campo relativamente novo, como mineração de moeda virtual. Essas operações são adequadas para ocultar a receita, pois é relativamente difícil para entidades externas avaliar a produção que depende da eficiência, do *hashrate* e das condições de mercado. As moedas ilegais são facilmente misturadas com os rendimentos regulares da mineração e tornam-se indistinguíveis, completando assim o ciclo de lavagem.

Dessarte, considerando que o crime de lavagem de dinheiro necessariamente sucede uma conduta ilícita antecedente, o proveito criminoso do fato penal se dará através da colocação, ocultação e posterior integração, no mercado corrente, pelos criptoativos.

De modo consequente, o próximo subcapítulo irá penetrar o tema relacionado aos crimes praticados, especialmente a narco traficância. Será detalhado o endereço digital *Silk Road* que objetiva a intermediação de negócios ilícitos através do criptoativo.

2.3 O FINANCIAMENTO DE NARCÓTICOS NA DEEP WEB ATRAVÉS DA CRIPTOMOEDA

Conforme menção anterior, a alavanca criminal com alta representatividade na prática delituosa através de ativos digitais é a propagação na *deepweb*¹⁴², especificadamente em marketplaces hospedados, não indexados, fora dos limites da surface web¹⁴³.

Os traficantes de drogas e de pessoas estão utilizando cada vez mais mercados online e moedas virtuais para se conectarem com compradores e ocultarem pagamentos. Os *marketplaces* online permitem o anonimato, conectam compradores e vendedores e oferecerem várias opções de pagamento, incluindo moedas virtuais. Esses mercados geralmente usam uma parte oculta da Internet, que os usuários acessam por meio de um software especial com pouco risco de

¹⁴² A *deep web*, a web invisível ou a web oculta são partes da World Wide Web cujos conteúdos não são indexados pelos mecanismos de pesquisa padrão da web.

¹⁴³ A internet que conhecemos e utilizamos no dia a dia.

detecção. Os traficantes também usam serviços de pagamento móvel ponto a ponto para transferir fundos entre usuários e quiosques – em lojas de conveniência e outros lugares – para converter dinheiro em moedas virtuais. Essas transações, normalmente, podem ser difíceis de rastrear pelas agências de fiscalização e pelas autoridades.¹⁴⁴

Os críticos¹⁴⁵¹⁴⁶¹⁴⁷ de criptoativos há muito afirmam que seu uso generalizado capacitaria hackers e outros criminosos. Suposto anonimato, facilidade de transporte transfronteiriço, falta de regulamentação transnacional e facilidade de liquidação são características que seduzem aqueles que desejam contornar a lei. Desde o início da bitcoin, vários casos de conduta criminal de alta complexidade foram desmantelados. Entre eles está a criação do primeiro bazar de drogas on-line do mundo e um hack maciço na bolsa de bitcoins Mt. Gox¹⁴⁸, que desencadeou um mercado negativo no preço da bitcoin.

Em fevereiro de 2011, Ross William Ulbricht¹⁴⁹, que atendia pelo nome de “Dread Pirate Roberts”, fundou o site Silk Road. ORMSBY¹⁵⁰ afirma que o Silk Road:

¹⁴⁴ GAO, U.S. Government Accountability Office. **Trafficking: Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking.** Disponível em: <<https://www.gao.gov/products/gao-22-105101>>, acesso em 01/06/2022.

¹⁴⁵ FORTUNE. **What the media gets wrong in its persistent crypto criticism.** Disponível em: <<https://fortune.com/2022/07/06/media-crypto-criticism-downturn-bear-markets-tech-defi-miller-whitehouse-levine/>>, acesso em 03/08/2022.

¹⁴⁶ WASHINGTON POST. **First she documented the alt-right. Now she’s coming for crypto.** Disponível em: <<https://www.washingtonpost.com/technology/2022/05/29/molly-white-crypto/>>, acesso em 03/08/2022.

¹⁴⁷ FORBES. **The False Narrative of Bitcoin’s Role in Illicit Activity.** Disponível em: <<https://www.forbes.com/sites/haileylennon/2021/01/19/the-false-narrative-of-bitcoins-role-in-illicit-activity/?sh=4c682ef93432>>, acesso em 03/08/2022.

¹⁴⁸ Mt. Gox foi uma exchange de criptomoedas com sede em Tóquio que operou entre 2010 e 2014. Foi responsável por mais de 70% das transações de Bitcoin em seu pico. Embora seja mais comumente conhecido como Mt. Gox, a bolsa às vezes é chamada de MtGox ou Mt Gox. A exchange declarou falência em 2014, mas continuou sendo objeto de ações judiciais e especulações por anos.

¹⁴⁹ FORDHAM. **Silk Road: The Dark Side of Cryptocurrency.** Disponível em: <<https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/>>, acesso em 20/07/2022.

¹⁵⁰ ORMSBY, Eileen. **Silk Road.** Macmillan: Pan Macmillian Australia. published in 2014. p. 7.

[...] was the 'eBay of drugs'. SILK ROAD lay at the heart of the 'Dark Web' – a parallel internet of porn, guns, assassins and drugs. Lots of drugs. With the click of a button LSD, heroin, meth, coke, any illegal drug imaginable, would wing its way by regular post from any dealer to any user in the world.

Autonomeado anarquista, sonhava com um mercado online onde as pessoas lograssem êxito em comprar e vender narcóticos e outros itens ilícitos, sem interferência governamental. Embora os usuários de um site da Darknet possam usar o Tor¹⁵¹ e as redes privadas virtuais para obscurecer e ocultar suas identidades, eles não tinham como trocar pagamentos anônimos entre si, a não ser enviar envelopes cheios de dinheiro pelo serviço postal, um procedimento obviamente impraticável. A solução foi idealizada por Ulbricht que contornou esse enigma usando a bitcoin como método de pagamento. Os endereços Bitcoin não exigem uma conta bancária, ID, número de segurança social (sinônimo de CPF) ou nome e são gratuitos para abrir e manter. No entanto, assim como o mercado comum, pessoas que comercializam no meio ilícito necessitam de segurança, por tal razão o livro-razão descentralizado do Bitcoin – o blockchain – forneceu uma maneira de verificar se os pagamentos foram recebidos ou enviados. Ao usar bitcoin, a única informação de identificação para uma transação de narcóticos seria o endereço do destinatário, um problema resolvido usando um P.O anônimo¹⁵². Nesse sentido, Ulbricht atuaria como um serviço de custódia entre comprador e vendedor e lucraria com as comissões retiradas de cada transação.¹⁵³¹⁵⁴

CHRISTIN¹⁵⁵ descreve que:

¹⁵¹ Tor é um software desenvolvido (browser) para rede digital com intuito de anonimizar as comunicações na internet. A abordagem tecnológica do Tor é baseada no "roteamento cebola", no qual as comunicações na internet são ofuscadas por rotas diferentes e variáveis.

¹⁵² An anonymous mail drop is a business-mail receiving service that will accept mail in your name but doesn't use your real mailing address.

¹⁵³ BILTON, Nick. American Kingpin: Catching the Billion-Dollar Baron of the Dark Web. Ebury Publishing; 2ª edição, 2018.

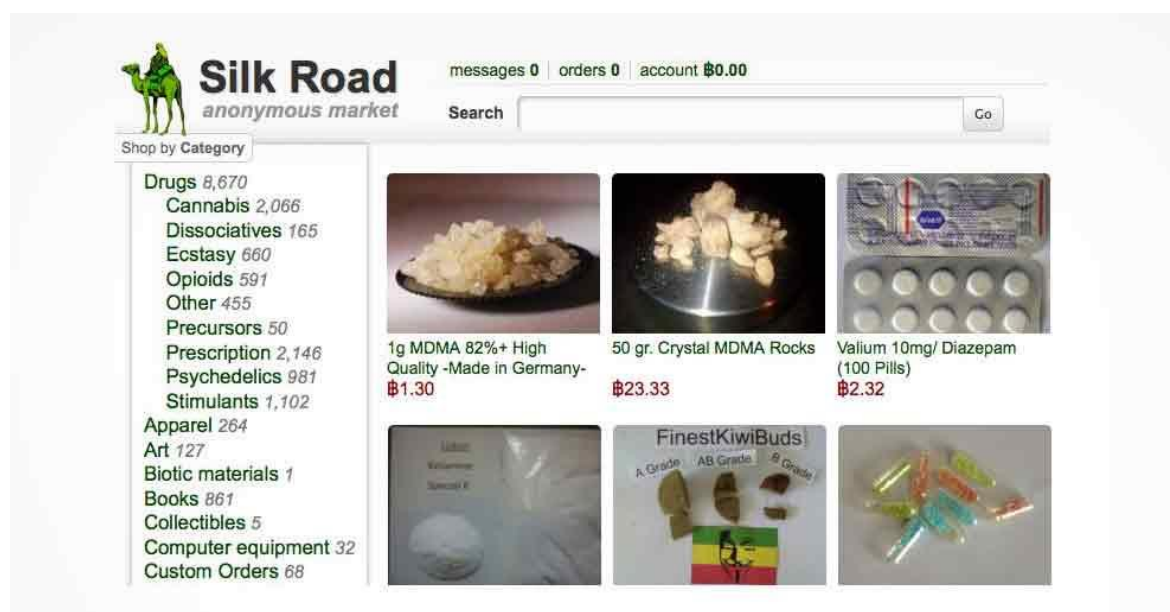
¹⁵⁴ CHRISTIN, Nicolas. **Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace.** Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/2488388.2488408>>, publicado em 2013, acesso em 05/03/2023.

¹⁵⁵ CHRISTIN, Nicolas. **Traveling the Silk Road: A Measurement Analysis of a Large**

Silk Road is an online anonymous marketplace that started its operations in February 2011. Silk Road is not, itself, a shop. Instead, it provides infrastructure for sellers and buyers to conduct transactions in an online environment. In this respect, Silk Road is more similar to the Amazon Marketplace, Craigslist, or eBay than to Amazon.com. The major difference between Silk Road and these other marketplaces is that Silk Road focuses on ensuring, as much as possible, anonymity of both sellers and buyers. In this section, we summarize the major features of Silk Road through a description of the steps involved in a typical transaction: accessing Silk Road, making a purchase, and getting the goods delivered.

O website Silk Road (FIGURA 2) começou de forma modesta, com cogumelos psicodélicos cultivados pelo próprio Ross, listados como os primeiros itens à venda.¹⁵⁶

Figura 2: página inicial do website Silk Road



Fonte: ROBINSON¹⁵⁷, 2020.

Anonymous Online Marketplace. Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/2488388.2488408>>, acesso em 05/03/2022.

¹⁵⁶ BILTON, Nick. **American Kingpin: Catching the Billion-Dollar Baron of the Dark Web.** Ebury Publishing; 2ª edição, 2018.

¹⁵⁷ ROBINSON, Tom. **\$1 Billion of Silk Road Bitcoins Are On The Move.** Elliptic, 4. Nov. 2020. Disponível em: <https://www.elliptic.co/blog/1-billion-silk-road-bitcoins-are-on-the-move> Acesso em: 20 abr. 2023.

Porém, com o intuito de alavancar as vendas, Ross promoveu seu site em um famoso fórum digital, ato que atraiu alguns compradores para seus cogumelos, mas acabou levando a sua queda. Até o final de fevereiro, no primeiro ano de vida, vinte e oito transações de narcóticos variando de LSD à mescalina foram realizadas no site. Porém, em dois meses, mais de mil pessoas se inscreveram. Os servidores do Silk Road não conseguiram lidar com o influxo, e uma combinação de hackers e aumento do tráfego do site forçou Ross a deixar o Silk Road temporariamente offline, para reequipá-lo e atualizá-lo. O verdadeiro fluxo de usuários, no entanto, ocorreu depois que o Gawker¹⁵⁸, uma coluna digital, publicou a história detalhada do Silk Road. Em poucos meses, Ulbricht recuperou seu investimento inicial e conseguiu criar um mercado virtualmente anônimo e próspero para a venda de narcóticos, completo com uma função de revisão de fornecedores, semelhante à Amazon ou eBay. Naquela época, o preço de uma única bitcoin disparou de cerca de um dólar para mais de trinta dólares, um aumento atribuível em grande parte ao acréscimo da atenção que a bitcoin recebeu por causa do Silk Road.¹⁵⁹

No verão de 2013, o Silk Road estava se aproximando de sua milionésima conta, com comissões diárias que ultrapassava dez mil dólares.¹⁶⁰ Todavia, POPPER¹⁶¹ leciona que os problemas continuaram a atormentar Ross e Silk Road. Hacks adicionais custavam a Ross aproximadamente US\$ 350.000 (trezentos e cinquenta mil dólares) ao ano. Ainda, quando um usuário teria, em tese, chantageado Ulbricht, ele teria contratado um suposto assassino para eliminá-lo.¹⁶² Foi noticiado que ele realizou o mesmo ato depois que um indivíduo e três associados furtaram usuários do Silk Road. Com o passar do tempo o

¹⁵⁸ GAWKER. **The Underground Website Where You Can Buy Any Drug Imaginable**. Disponível em: <<https://www.gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160>>, acesso em 31/07/2022.

¹⁵⁹ BILTON, Nick. *American Kingpin: Catching the Billion-Dollar Baron of the Dark Web*. Ebury Publishing; 2ª edição, 2018.

¹⁶⁰ POPPER. Nathaniel. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. Editora: Harper Paperbacks; Reprint edição, 2016.

¹⁶¹ POPPER. Nathaniel. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. Editora: Harper Paperbacks; Reprint edição, 2016.

¹⁶² SOLON, Olivia. **Police crackdown on Silk Road following first drug dealer**. Disponível em: <<https://www.wired.co.uk/article/silk-road-crackdown>>, acesso em 20/06/2022.

empreendedor criminal ficou cada vez mais paranoico, pois o FBI começou a fazer prisões mensais de compradores e vendedores do Silk Road.¹⁶³ Ulbricht tomou mais precauções para esconder sua identidade, mas temia que seu IP real ou endereço de servidor eventualmente vazasse. Em determinado momento, agentes da Patrulha Broder interceptaram um pacote contendo nove carteiras de motorista falsificadas com destino a residência de Ross.¹⁶⁴ Quando confrontado em sua porta, ele mostrou aos agentes sua licença real com seu nome verdadeiro, mas se recusou a responder a quaisquer outras perguntas sobre a origem dos documentos. Embora Ross fosse suspeito neste momento, a força-tarefa não havia divulgado amplamente seu nome e os agentes saíram sem fazer uma prisão. Ulbricht decidiu mudar de apartamento, mas não deixou o mercado ilícito digital.

Em 1º de outubro de 2013, Ross foi até uma biblioteca pública na cidade de São Francisco, com seu laptop em mãos. Sem que ele soubesse, agentes federais rastreavam cada movimento seu. Assim que Ross fez login em seu laptop criptografado, ele recebeu uma mensagem de “cirrus”, um novo moderador cuja conta foi apropriada pelo FBI¹⁶⁵. Cirrus pediu a Ross que verificasse certos posts sinalizados, pois isso exigiria que Ross fizesse login na parte interna fortemente criptografada do Silk Road. Ross finalmente respondeu, perguntando quais postagens sinalizadas o usuário estava se referindo, sinalizando aos agentes que ele havia logado. Quando Ulbricht se virou, um agente entrou e pegou seu laptop aberto, enquanto outros o prenderam rapidamente. Ross Ulbricht foi preso em flagrante, indiciado por acusações de conspiração de narcóticos, lavagem de dinheiro e solicitação de assassinato por aluguel. Após o empreendo estar em custódia, usuários do Silk Road que visitaram o site encontraram um emblema do FBI sobre o anúncio: “*THIS HIDDEN SITE HAS BEEN SEIZED.*”¹⁶⁶

163 SOLON, Olivia. **Police crackdown on Silk Road following first drug dealer.** Disponível em: <<https://www.wired.co.uk/article/silk-road-crackdown>>, acesso em 20/06/2022.

164 WIRED. **The Untold Story of Silk Road, Part 1.** Disponível em: <<https://www.wired.com/2015/04/silk-road-1/>>, acesso em 31/07/2022.

165 SOLON, Olivia. **Police crackdown on Silk Road following first drug dealer.** Disponível em: <<https://www.wired.co.uk/article/silk-road-crackdown>>, acesso em 20/06/2022.

166 O GLOBO. **FBI fecha Silk Road, site secreto para comércio de drogas ilícitas.** <<https://g1.globo.com/tecnologia/noticia/2013/10/fbi-fecha-silk-road-site-secreto-para-comercio-de-drogas-ilicitas.html>>, acesso em 31/07/2022.

No decurso da investigação foi identificado que o Silk Road processou US\$ 9 bilhões de dólares¹⁶⁷ em transações, sendo que com cada uma dessas transações uma pequena fatia de Bitcoin havia sido reservada para Ross Ulbricht.

Ironicamente, um erro antiquado levou à queda do Dread Pirate Roberts. Gary Alford, um agente do IRS designado para trabalhar no Silk Road, vasculhou a web em seu tempo livre procurando por menções de Silk Road e Dread Pirate Roberts. Foi revelado na fase investigativa que o agente do IRS encontrou uma postagem no fórum Bitcoin, descrevendo um mercado de drogas anônimo, com a última postagem de um usuário listando a um endereço de e-mail, rossulbricht@gmail.com. Enquanto seus superiores estavam inicialmente céticos, Alford continuou cavando e encontrou vários links entre o Silk Road e Ross Ulbricht, incluindo um endereço IP em San Francisco que estava ligado aos servidores do Silk Road. Eventualmente, a força-tarefa Marco Polo foi capaz de capitalizar as descobertas de Alford. Em última análise, Ross Ulbricht foi condenado à prisão perpétua sem possibilidade de liberdade condicional. A sentença foi anunciada por Preet Bharara, procurador do Distrito Sul de Nova York. Ulbricht foi considerado culpado em cada uma das sete acusações que enfrentou, após um julgamento de júri de quatro semanas. A juíza distrital dos EUA Katherine B. Forrest impôs a sentença em 29 de maio.¹⁶⁸

Logo, o Silk Road surgiu como o mercado criminoso mais sofisticado e extenso da Internet, servindo como um amplo mercado negro onde bens e serviços ilegais, incluindo drogas ilegais de praticamente todas as variedades, eram comprados e vendidos regularmente pelos usuários do site. Enquanto em operação, o Silk Road foi usado por milhares de traficantes e outros vendedores ilegais para distribuir centenas de quilos de drogas ilegais e outros bens e serviços

¹⁶⁷ Fonte: **Sealed Complaint 13 MAG 2328: United States of America v. Ross William Ulbricht.** Disponível em: <<https://web.archive.org/web/20140220003018/https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf>>, acesso em 03/08/2022.

¹⁶⁸ ICE. **Ross Ulbricht, aka Dread Pirate Roberts, sentenced to life in federal prison for creating, operating 'Silk Road' website.** Disponível em: <<https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating>>, acesso em 31/07/2022.

ilegais para mais de 100.000 compradores e, ainda, para lavar centenas de milhões de dólares decorrentes dessas transações ilegais.

Ao impor a sentença, o juiz FORREST¹⁶⁹ disse:

There must be no doubt that lawlessness will not be tolerated. There must be no doubt that no one is above the law - no matter one's education or privileges. All stand equal before the law. There must be no doubt that you cannot run a massive criminal enterprise and because it occurred over the Internet minimize the crime committed on that basis.

Ulbricht, com 31 anos de idade à época de sua condenação, natural de São Francisco, Califórnia, foi condenado pelos seguintes crimes: distribuição de entorpecentes, distribuição de entorpecentes por meio da Internet, conspiração para distribuir entorpecentes, envolvimento em um empreendimento criminoso contínuo, conspiração para cometer *hacking* de computador, conspirar para traficar documentos de identidade falsos e conspirar para cometer lavagem de dinheiro.

Por oportuno, no Brasil, em 2021¹⁷⁰, o Ministério Público do Estado do Rio de Janeiro (MPRJ), por meio do Grupo de Atuação Especial de Combate ao Crime Organizado (GAECO/RJ) em conjunto com a Polícia Civil deflagrou uma operação em que uma organização criminosa comercializava drogas, através do aplicativo Whatsapp, em troca de criptomoedas.

Não obstante haja informações do envolvimento do tráfico de drogas, lavagem de capitais e os criptoativos no Brasil, é nos Estados Unidos que o combate estatal se mostra páreo à ascendência criminosa. Agências federais americanas têm a tarefa de investigar e processar casos de tráfico que envolvem mercados online e moeda virtual. Isso abarca entidades policiais federais dentro do Departamento de Justiça (DOJ), como a *Drug Enforcement Administration* (DEA) e

¹⁶⁹ SUPREMECOURT. **ROSS WILLIAM ULBRICHT, PETITIONER v. UNITED STATES OF AMERICA.** Disponível em: <https://www.supremecourt.gov/DocketPDF/17/17-950/24860/20171222095855755_Ulbricht%20cert%20petition.pdf>, acesso em 31/07/2022.

¹⁷⁰ SEU DINHEIRO. **Aceita bitcoin: Tráfico de drogas no Rio de Janeiro aceitava criptomoedas por WhatsApp; envolvidos são presos.** Disponível em: <<https://www.seudinheiro.com/2021/bitcoin/trafico-de-drogas-bitcoin-criptomoedas-whatsapp/>>, acesso em 02/08/2022.

o *Federal Bureau of Investigations* (FBI), bem como o Departamento de Segurança Interna (DHS). Outras agências, incluindo o Departamento do Tesouro (Treasury), apoiam as investigações de casos de tráfico. Algumas de suas ações e investigações recentes incluem¹⁷¹:

In 2016, DHS's Immigration and Customs Enforcement's Homeland Security Investigations and the Secret Service identified and seized \$1.2 million from a trafficker's virtual currency wallet.

In 2020, an investigation by Treasury's Internal Revenue Service Cyber Crime Unit helped shut down Helix, a dark web platform that laundered money for drug traffickers.

Treasury's Financial Crimes Enforcement Network (FinCEN) issued guidance to help financial institutions detect trafficking activity that involved virtual currencies.

Federal banking, securities, and derivatives regulators oversee financial institutions' compliance with Bank Secrecy Act/Anti-Money Laundering (AML) requirements, including their reporting of suspicious activities, such as potential trafficking. Law enforcement agencies use these data to investigate potential criminal activity.

Ainda, no Reino Unido, uma organização de criminosos¹⁷² que lucrou milhões de libras em criptomoedas fornecendo drogas pela *dark web* foi descoberta e sentenciada. O esquema era simples: o grupo fornecia drogas em todo o norte da Inglaterra e as distribuía para traficantes de rua, que então as vendiam por dinheiro que depois era devolvido ao grupo criminoso. Um mensageiro então coletaria o dinheiro e o entregaria a um corretor que providenciaria para que os fundos fossem convertidos em bitcoin. O corretor então enviaria a bitcoin para um endereço especificado pelo grupo criminoso, cobrando uma pequena taxa de 4%. A rede Bitcoin é essencialmente usada como um sistema de transferência de valor,

¹⁷¹ GAO. **As Virtual Currency Use in Human and Drug Trafficking Increases, So Do the Challenges for Federal Law Enforcement.** Disponível em: <<https://www.gao.gov/blog/virtual-currency-use-human-and-drug-trafficking-increases-so-do-challenges-federal-law-enforcement>>, acesso em 02/08/2022.

¹⁷² BBC. **Dark web drug dealer jailed over cryptocurrency millions.** Disponível em: <<https://www.bbc.com/news/uk-england-leeds-61809398>>, acesso em 02/08/2022.

e análises posteriores mostraram que os fundos foram finalmente enviados para um serviço OTC aninhado em uma popular exchange de criptomoedas.

Por fim, na Rússia existe um fórum digital chamado de RAMP, que é um website russo para membros cibercriminosos, anteriormente conhecido como Payload.bin. Este fórum comercializava FortiNet VPN e ferramentas de hacking compartilhadas usadas em operações de infiltração. O site, que foi lançado em 2012 e está disponível exclusivamente na Rússia, tinha a reputação de ser o melhor lugar para comprar drogas e que poderiam ser entregues dentro das fronteiras do país. No entanto, em 2017, a polícia russa anunciou que havia retirado este fórum do ar. Porém, em 2021, um novo fórum com o nome RAMP 2.0 surgiu na Dark Web, possuindo identidade visual idêntica ao portal mais antigo. Especula-se que o site está em pleno funcionamento e oferece diariamente produtos ilícitos em troca de pagamentos em criptoativos.¹⁷³

Dito isto, o subcapítulo teve como enfoque a abordagem do submundo comercial, realizado através da *deep web*, com estudos práticos, desmantelados por autoridades americana, brasileiras, ingleses e russas. O objetivo foi demonstrar o avanço análogo do criptoativo no emprego de atos criminosos na *deep web*. Identificou-se a facilidade negocial e a complexidade investigativa no que se refere ao ativo digital. É cediço que a transferência de recursos através de criptoativos é uma das características peculiares. Não há intermédio, tampouco compensação por uma entidade terceira. A negociação é gerada somente através do *peer-to-peer* (p2p), ou seja, diretamente entre o comprovador e o vendedor. Já, na *deep web*, onde o anonimato é apregoado, para dar legitimidade e garantir a entre do bem, plataformas de *market place* intermediam negócios (*middle man*) ilícitos com intuito de auxiliar a realização negocial entre as partes.

O próximo subcapítulo busca elucidar a transferência P2P através da explanação da definição e a correlação com o rompimento das barreiras financeiras entre os Estados.

¹⁷³ BLEEPINGCOMPUTER. **Russian Authorities Announce Takedown of RAMP Dark Web Marketplace.** Disponível em: <<https://www.bleepingcomputer.com/news/security/russian-authorities-announce-takedown-of-ramp-dark-web-marketplace/>>, acesso em 03/08/2022.

2.4 A MODALIDADE DE TRANSFERÊNCIA DE BITCOIN P2P E O DESAPARECIMENTO DE BARREIRAS FINANCEIRAS GOVERNAMENTAIS

A transferência de recursos entre instituições financeira, pessoas, empresas e Estados é fundamental para a manutenção da economia global. Diariamente bancos realizam compensações do expediente entre si, conhecidos usualmente como CDI. O portal de informações INFOMONEY¹⁷⁴ destaca que,

O CDI (Certificado de Depósito Interbancário) é um título de curtíssimo prazo emitido pelos bancos. Em algum grau, ele se assemelha ao CDB. Isso porque o CDI também é usado pelas instituições para captar recursos.

Mas há uma diferença fundamental entre eles: o certificado interbancário não é oferecido diretamente aos investidores individuais. Como o próprio nome indica, ele serve para que os bancos emprestem e tomem recursos entre si de um dia para o outro. O CDI tem prazo de vencimento de um dia útil.

É notório que o procedimento de compensação interbancária, entre pessoas físicas e jurídicas, possui regulamentação, fiscalização e normatização pelo Banco Central (Bacen). Não é diferente em outras jurisdições, citando caso análogo, nos Estados Unidos o FED é detentor de tal competência. Mas, o criptoativo, com suas características únicas, conforme supramencionado, não é regulamentado, fiscalizado ou normatizado.

Logo, a transferência *peer-to-peer* ou rede ponto a ponto (p2p) é uma arquitetura de aplicativo distribuída que particiona tarefas ou cargas de trabalho entre pares. Os pares são participantes igualmente privilegiados e equipotentes na rede. Eles formam uma rede ponto a ponto de nós. MELCHIORI¹⁷⁵ destaca:

E é justamente por essa característica peculiar que as autoridades administrativas brasileiras, como Receita Federal, Banco Central e

¹⁷⁴ INFOMONEY. **CDI: O que é, como funciona e como se relaciona com seus investimentos.** Disponível em: <<https://www.infomoney.com.br/guias/cdi/>>, acesso em 02/08/2022.

¹⁷⁵ MELCHIORI, Juliano Callegari. **As criptomoedas e o crime de evasão de divisas.** Disponível em: <<https://www.conjur.com.br/2021-nov-20/juliano-melchiori-criptomoedas-crime-evasao-divisas>>, acesso em 02/08/2022.

Comissão de Valores Mobiliários, já definiram que as criptomoedas não constituem moeda de curso legal (vide Instrução Normativa 1.888/19 da RFB), não possuem garantia de conversão para moedas soberanas, tampouco lastreadas em ativo real de qualquer espécie (vide Comunicado 31.379/17 do BCB), e que não podem ser qualificadas como ativos financeiros e, por isso, não podem ser adquiridas por fundos de investimento (vide Ofício Circular 1/2018 da CVM).

Por esse motivo, as criptomoedas estão alheias ao sistema financeiro brasileiro, de modo que não podem, afinal de contas, serem objeto dos crimes definidos na Lei nº 7.492/86 (que define os crimes contra o sistema financeiro nacional), como, por exemplo, o crime de evasão de divisas, estabelecido no artigo 22 da referida lei, conforme reconhecido pelo Superior Tribunal de Justiça por ocasião do julgamento do conflito de competência nº 161123/SP.

Na ocasião, o STJ reconheceu que como a criptomoeda, até o momento, não é tida como moeda, valor mobiliário ou ativo financeiro, não estando nem sujeita ao controle do Banco Central, é inapta a ensejar crimes contra o sistema financeiro.

Ainda, mesmo que seja regulamentado, vide projeto de lei PL 4.401/2021¹⁷⁶, não seria comparado a uma transferência comum. Em uma relação financeira ordinária toda compensação passará por uma câmara de compensação ou instituição financeira. Essas instituições possuem obrigações legais em reportar anomalias ou inconsistências. No entanto, o criptoativo é uma modalidade de pagamento que não necessita de um terceiro interventor no ato negocial. O negócio, transação ou pagamento será gerado entre duas pessoas: o comprador e o vendedor. Além disso, a negociação pode ser física, em carteiras usb¹⁷⁷, ou digital. Considerando que o criptoativo é um *digital asset* e que a custódia é por conta do possuidor, a barreira estatal criada para dificultar que divisas (dinheiro)

¹⁷⁶ Dispõe sobre a prestadora de serviços de ativos virtuais; e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 7.492, de 16 de junho de 1986, e 9.613, de 3 de março de 1998, para incluir a prestadora de serviços de ativos virtuais no rol de instituições sujeitas às suas disposições. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/151264>>.

¹⁷⁷ As carteiras de hardware armazenam as chaves privadas que dão acesso às suas criptomoedas de forma física.

sejam transferidas para fora do Estado sem conhecimento do governo deixa de existir.

A importância do controle de fluxo de capitais é estudada por economistas e representa, em suma, risco sistêmico para o mercado de capitais e risco-país, para MUNHOZ¹⁷⁸:

No que diz respeito ao elevado peso de capitais financeiros no balanço de pagamentos do Brasil e seus impactos sobre a taxa de câmbio, o apontamento mais frequente no debate econômico atual para sua diminuição é que o país deve continuar utilizando medidas de controles de capitais. Não só o FMI já os aceita e os recomenda, ainda que com algumas restrições, como já foram divulgados manifestos de economistas de vários países defendendo os controles. Assim, não só os economistas, mas também os policymakers têm sido favoráveis aos controles de capitais, especialmente aqueles que incidem sobre os seus influxos, capazes de limitar a sobrevalorização cambial e reduzir a fragilidade financeira resultante dos fluxos de capitais voláteis (Forbes et al., 2011).

O controle de transferência de recursos não é apenas uma maneira do Estado controlar as reservas de seus cidadãos ou de ter conhecimento sobre o patrimônio auferido por cada um deles, mas, tem como princípio fundamental apurar o fluxo financeiro disponível em reservas. O tipo penal previsto no art. 22 da Lei 7.492, qual seja evadir divisas, objetiva impedir que recursos sejam evadidos ao exterior sem autorização legal.

O GAFI no recente relatório¹⁷⁹ de recomendações - *virtual assets and virtual asset service providers* destacou na recomendação 16 que:

Recommendation 16. As noted in Section III, providers in this space must comply with the requirements of Recommendation 16 (i.e. the

¹⁷⁸ MUNHOZ, Vanessa da Costa. Vulnerabilidade externa e controle de capitais no Brasil: uma análise das inter-relações entre câmbio, fluxos de capitais, IOF, juros e risco-país. *Nova Economia* [online]. 2013, v. 23, n. 2 [Acessado 2 Agosto 2022], pp. 371-402. Disponível em: <https://doi.org/10.1590/S0103-63512013000200005>, acesso em 05/03/2023.

¹⁷⁹ FATF. **Virtual assets and virtual asset service providers**. Disponível em: <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>>, acesso em 02/08/2022. p. 82.

'travel rule'). This includes the obligation to obtain, hold, and submit required originator and beneficiary information associated with VA transfers in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities. The requirements apply to both VASPs and other obliged entities such as FIs when they send or receive VA transfers on behalf of a customer.

Porém, a recomendação apenas enfatiza a necessidade de *virtual asset service provider* (VASPs) e outras entidades que participam do mercado negocial a submissão de informações pertinentes e é omissa quanto a transferência de recursos entre *peers*, sem a intermediação desses terceiros interessados.

O GAFI¹⁸⁰ define peer-to-peer como:

The FATF defines peer-to-peer' (P2P) transactions as VA transfers conducted without the use or involvement of a VASP or other obliged entity (e.g., VA transfers between two unhosted wallets whose users are acting on their own behalf).¹⁰ P2P transactions are not explicitly subject to AML/CFT controls under the FATF Standards. This is because the Standards generally place obligations on intermediaries, rather than on individuals themselves (with some exceptions, such as requirements related to implementing targeted financial sanctions).

O GAFI reconhece que as transações P2P podem representar riscos específicos de lavagem de dinheiro e financiamento ao terrorismo, pois podem ser usadas para evitar controles de *anti money laundering* e countering the financing of terrorism nos padrões especificados por ele. Quando as transferências de criptoativos ocorrem numa base P2P, não existem entidades obrigadas envolvidas na prevenção ou mitigação dos riscos supramencionados. Embora as transações P2P também sejam usadas para atividades lícitas, os atores ilícitos podem explorar a falta de intermediários obrigados nas transações P2P para ocultar os proventos do crime, porque não há nenhuma entidade obrigada que desempenhe as funções recomendadas pela entidade intergovernamental.) Por outro lado, a visibilidade de

¹⁸⁰ FATF. **Virtual assets and virtual asset service providers**. Disponível em: <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>>, acesso em 02/08/2022. p. 18.

transações P2P na blockchain pode apoiar análises financeiras e investigações de criminais, especialmente quando combinada com outras fontes de informação, a menos que haja protocolos e tecnologias de aprimoramento do anonimato associados ao criptoativo utilizado na lavagem. Ainda, o GAFI¹⁸¹, destaca que o setor P2P de criptoativos é muito maior do que aquele intermediado por exchanges e que é praticamente impossível de mensurar o tamanho exato do risco gerado:

The FATF's Second 12-Month Review report provides an overview of the extent to which VAs are used on a P2P basis, based on data provided by seven blockchain analytic companies. 11 This report indicated that a potentially significant amount of certain VAs is transferred on a P2P basis, and the share of identified illicit transactions appears higher for P2P transactions compared with direct transactions with VASPs. However, the high level of variation in the data provided by the blockchain analytic companies means that there is no consensus on the size of the P2P sector and its associated ML/TF risk. It also reveals the challenges and limitations inherent in this kind of research with blockchain analytics, in terms of coverage, timeliness, accuracy and reliability, even if P2P transactions are recorded on public ledgers.

Por fim, realça que os países e as VASPs devem procurar entender quais tipos de transações P2P representam maior ou menor risco, a origem das transações P2P e seus diferentes perfis de risco. Fatores relevantes que podem, dependendo do tipo do criptoativo, impactar potencialmente a extensão em que os usuários se envolvem em transações P2P, incluem a acessibilidade e liquidez do criptoativo e os protocolos que controlam a privacidade, transparência, segurança e taxas de transação associadas. Vários fatores devem ser levados em consideração e, especialmente, como eles se manifestam em cada país para avaliar riscos sistêmicos e aplicar controles de mitigação consistentes com um *Risk-Based Approach*¹⁸². A rápida evolução deste setor significa que as mudanças no

¹⁸¹ FATF. **Virtual assets and virtual asset service providers**. Disponível em: <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>>, acesso em 02/08/2022. p. 18.

¹⁸² A risk-based approach means that countries, competent authorities, and banks identify, assess, and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk. Source: <https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>

nível e na natureza do risco provavelmente ocorrerão rapidamente e merecerão uma atenção de supervisão concertada.

Nesse sentido, o controle do Estado, através do *risk-based approach*, com celeridade legislativa e implementação de serviços de inteligência nesse setor é medida que se impõe.

Por derradeiro, o terceiro capítulo abordará, em essência, intervenções legais no ativo digital, a relação da aplicabilidade da lei nacional e jurisdições estrangeiras e a prevenção necessária para o combate à lavagem de dinheiro.

Capítulo 3

INTERVENÇÕES LEGAIS NO AVANÇO DO MERCADO ILÍCITO DE CRIPTOATIVOS

3.1 O ENTENDIMENTO DOS TRIBUNAIS SUPERIORES SOBRE OS TIPOS PENAIS QUE ENVOLVEM CRIPTOATIVOS

A introdução de novas tecnologias que atualizam as conexões sociais econômicas está intimamente ligada ao campo do Direito Penal Econômico, que estuda os delitos econômicos, financeiros e tributários. A influência de novas manifestações de valores ou formas de transações comerciais, como os criptoativos, exige uma compreensão da extensão em que o direito penal abarca esses fenômenos econômicos. Isso ocorre com o advento dos ativos virtuais nas transações privadas, que transforma o paradigma das interações econômicas definidas pelo Direito Penal Econômico como dependentes de moedas e de supervisão governamental.

Por operarem sem intermediários centralizados e por serem ativos que não estão sob a soberania do Estado, os criptoativos foram desenvolvidos com o intuito de diminuir os custos de transação, facilitar a troca de valores e aumentar a discricionariedade dos negócios. Por esses motivos, a utilização de criptoativos de forma ilícita e inapropriada cresce ano após ano¹⁸³.

Contudo, antes de adentrar no estudo de casos concretos é necessário destacar que, em 11 de outubro de 2022, a Comissão de Valores Mobiliários entabulou ao mercado o parecer de orientação nº 40, que define conceitos e delimita limites sobre os criptoativos e o mercado de títulos e valores mobiliários. Dessarte, ao alterar entendimento anterior, o qual afirmava que criptoativos não eram títulos e valores mobiliários, portanto não regulamentados

¹⁸³ WSJ. **Cryptocurrency-Based Crime Hit a Record \$14 Billion in 2021**. Disponível em: <<https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073>>, acesso em 03/12/2022.

pelo órgão, criou-se revés que será levado ao judiciário com difícil mensuração do deslinde final.

A CVM destaca no parecer que:

Embora ainda não haja legislação específica sobre o tema, este Parecer tem o objetivo de garantir maior previsibilidade e segurança, bem como de fomentar ambiente favorável ao desenvolvimento dos criptoativos, com integridade e com aderência a princípios constitucionais e legais relevantes. Desta forma, a CVM está contribuindo para (i) a proteção do investidor e da poupança popular; (ii) a prevenção e o combate à lavagem de dinheiro, (iii) prevenção e combate à corrupção; (iv) controle à evasão fiscal; e (v) prevenção e combate ao financiamento do terrorismo e/ou proliferação de armas de destruição em massa.

A Instrução Normativa 1.888/2019 da Receita Federal já havia mostrado indícios de categorizar o criptoativo como uma “*representação digital de valor denominado em sua própria unidade de conta*”¹⁸⁴, estabelecendo certos requisitos de coleta de informações para trocas de criptoativos. Isso demonstra o desenvolvimento, ainda que em estágio inicial, de um microssistema regulatório que direciona o controle das transações e a possibilidade de persecução penal, ou seja, o reconhecimento dos criptoativos como objeto do crime de lavagem de dinheiro e a troca como bem jurídico que obrigada aos deveres de transparência e informação.

No concernente às principais propriedades dos ativos criptográficos, desenvolve-se um cenário que contraria leis anti-lavagem, ao exigirem a restrição do anonimato e o registro das transações. Apesar da transcrição das transações comerciais na blockchain, a rastreabilidade do próprio usuário detentor das chaves criptografadas permanece instável, dada a possibilidade de um único indivíduo

¹⁸⁴ RECEITA FEDERAL. **Instrução Normativa RFB Nº 1888, de 03 de Maio de 2019**. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Publicado(a) no DOU de 07/05/2019, seção 1, página 14. Disponível em: <<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592>> Acesso em 15.08.2022.

manter várias contas e utilizar-se de recursos como *mixers*¹⁸⁵. Assim, infere-se que a aplicação da Lei de Lavagem esgota a base fundamental desse sistema comercial virtual.

É controvertível argumentar que a Lei nº 9.613/1998 é inaplicável por contrariar as propriedades essenciais dos criptoativos, haja vista que persiste comportamento ilícito neste sistema. Diante disso, é necessário o efetivo controle da situação, definindo condutas lícitas e ilícitas, pois a dificuldade de compreensão das transações virtuais não é desculpa para descumprir a aplicação da lei.

É tendência regulamentária mundial que leis anti-lavagem de dinheiro sejam compatíveis com a nova tecnologia das criptomoedas, por outro lado, são necessárias investigações aprofundadas sobre o mecanismo de funcionamento desses sistemas, idealmente quanto sua característica transnacional devido à natureza circular e digital dos criptoativos.

A regulamentação interna brasileira sobre exchange, que permite que os detentores de ativos sejam identificados por meio de seus clientes, parece estar progredindo. Adicionalmente, o Grupo de Ação Financeira contra a Lavagem de Dinheiro e Financiamento do Terrorismo (GAFI) divulga recomendações que direcionam a regulamentação voltada para desenvolvedores de software para que sejam criadas aberturas para vigilância estatal e desincentivos de transações diretas por usuários. No entanto, não é possível basear-se no pressuposto de que a necessidade de anonimato e de proteção dos dados pessoais resulte invariavelmente de uma conduta ilícita. Todas essas tentativas regulatórias permeiam a discussão crítica sobre o monitoramento governamental dos indivíduos. Para evitar que as atividades regulatórias tenham o efeito inverso – a construção de sistemas ainda mais anônimos e a transferência de usuários para

¹⁸⁵ Um serviço que combina vários fluxos de criptomoedas possivelmente reconhecíveis é conhecido como *mixer* ou *tumbler*. Como resultado, as transações são mais anônimas, pois o criptoativo é mais difícil de rastrear. Não há vínculo entre a transação original e o endereço inicial, pois o proprietário do criptoativo envia os fundos para o serviço de mixagem, que os combina com os fundos de outros usuários e envia os fundos combinados para o endereço solicitado. Para que a transação seja composta por vários pequenos pagamentos parciais distribuídos por um período mais longo, os valores das transações podem ser escolhidos aleatoriamente. A taxa típica para o serviço de mistura é de 0,25% a 3% da quantidade a ser misturada.

eles – a regulação direta de pessoas é sempre um processo difícil que exige especialização das entidades envolvidas.

Portanto, infere-se que a intervenção estatal, pelo parecer nº 40 da CVM, trata-se de um efeito consequencial de crimes que são praticados contra possíveis investidores e o mercado financeiro que obrigatoriamente exige celeridade legislativa. Outrora, a CVM afirma que a ideia de segurança tem um aspecto instrumental e objetivo na medida em que serve para restringir o regime de valores mobiliários e, conseqüentemente, a competência da CVM. Assim, caso um criptoativo seja classificado como valor mobiliário, os emissores e eventuais agentes contratados devem seguir a regulamentação estabelecida para o mercado de valores mobiliários e podem estar sujeitos à regulamentação da CVM. Nesse diapasão, é possível afirmar que, ao equiparar a oferta de criptoativos a títulos e valores mobiliários, a CVM faz com que a lei 7.492/1986, que define os crimes contra o sistema financeiro nacional, e dá outras providências, seja aplicável a casos que envolvam criptoativos. Conseqüentemente haverá, em futuras investigações/ações penais, penas mais severas, pois é possível interpretar em julgados como em casos paradigmas Unick e GAS, duas empresas que foram denunciadas pela prática de crimes com criptoativos, a possibilidade de aplicação da lei contra o sistema financeiro nacional e tipos penais como gestão fraudulenta, operar instituição financeira sem a devida autorização e apropriação indébita especial.

Entrementes, apesar dos criptoativos não serem considerados valor monetário ou valores mobiliários – na via judicial, conforme decisão do Conflito de Competência nº 161.123/SP, não sendo de competência do Banco Central (Bacen) ou da Comissão de Valores Mobiliários (CVM), essa nova regulamentação, parecer de orientação nº 40 da CVM, altera por vez a perspectiva jurisprudencial. No conflito de competência supracitado entendeu-se que quem opera com tais ativos não é instituição financeira para fins penais. Isso porque esse conceito pressupõe “(...) a captação, intermediação ou aplicação de recursos financeiros de terceiros, em moeda nacional ou estrangeira, ou a custódia, emissão, distribuição, negociação, intermediação ou administração de valores mobiliários” (art. 1º da Lei nº 7.492/86).

Nesse sentido, no Habeas Corpus RHC 161.635¹⁸⁶, julgado pela Quinta Turma do STJ, impetrado pela defesa de um grupo organizado que praticava, em tese, crimes envolvendo criptoativos questionou-se a capitulação dos delitos, entendendo-se, na opinião da defesa, ser impossível a imputação de dois crimes a um único fato. A organização acusada, segundo o processo, utilizava uma plataforma eletrônica para aliciar investidores com a promessa de ganhos acima da média por meio da compra e venda de criptomoedas. A organização primeiro disponibilizou alguns resgates, mas as vítimas gradualmente deixaram de receber o dinheiro depositado. Também foi modelada uma operação de marketing multinível, que vinculou o envolvimento do negócio à captação de novos investidores. O Ministério Público acusou a organização de crimes contra a economia pública (art. 2º, IX, da Lei 1.521/1951) e estelionato (art. 171, caput, do Código Penal), por haver vítimas reconhecidas, cada uma com seus prejuízos, contatados por recrutadores. Por seu turno, a defesa impetrou habeas corpus para trancar o processo criminal em relação a todas as acusações de estelionato, alegando a ocorrência de *bis in idem*, mas o pedido foi negado. A defesa argumentou no recurso ao STJ que a dupla acusação decorreu do mesmo fato.

Na decisão o STJ afastou a imputação de estelionato pelo dano geral causado a um número indeterminado de vítimas cooptadas pela internet, dando provimento parcial ao recurso de um dos arguidos, decisão que foi alargada aos corréus.

Por outro lado, além da discussão acerca do conceito jurídico e da tipicidade das condutas praticadas, a territorialidade do crime de lavagem de dinheiro utilizando criptoativos também é fundamento para questionamento recorrente nas cortes superiores. Dada a transnacionalidade das transações neste contexto, o conflito de competências positivo e negativo é altamente provável. O CC n. 161.123/SP fulminou discussões acirradas sobre o tema, pois decidiu que a lavagem de dinheiro, oriunda da prática de crimes com criptoativos, apenas será de competência da Justiça Federal se houver crime antecedente que seja de

¹⁸⁶ BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus n. 161.635/DF**. Relator Ministro Ribeiro Dantas, Quinta Turma, julgado em 23/8/2022, publicado no DJe em 30/8/2022.

competência deste. Outrora, declarou, no que tange ao crime de evasão de divisa, ser teoricamente possível a utilização do comércio de criptoativos como meio para a prática desse delito, desde que o agente adquira a moeda virtual para a realização de operação cambial ilícita (conversão de reais em estrangeiros moeda) a fim de promover a evasão de moeda, *in verbis*¹⁸⁷:

CONFLITO NEGATIVO DE COMPETÊNCIA. INQUÉRITO POLICIAL. JUSTIÇA ESTADUAL E JUSTIÇA FEDERAL. INVESTIGADO QUE ATUAVA COMO TRADER DE CRIPTOMOEDA (BITCOIN), OFERECENDO RENTABILIDADE FIXA AOS INVESTIDORES. INVESTIGAÇÃO INICIADA PARA APURAR OS CRIMES TIPIFICADOS NOS ARTS. 7º, II, DA LEI N. 7.492/1986, 1º DA LEI N. 9.613/1998 E 27-E DA LEI N. 6.385/1976. MINISTÉRIO PÚBLICO ESTADUAL QUE CONCLUIU PELA EXISTÊNCIA DE INDÍCIOS DE OUTROS CRIMES FEDERAIS (EVASÃO DE DIVISAS, SONEGAÇÃO FISCAL E MOVIMENTAÇÃO DE RECURSO OU VALOR PARALELAMENTE À CONTABILIDADE EXIGIDA PELA LEGISLAÇÃO). INEXISTÊNCIA. OPERAÇÃO QUE NÃO ESTÁ REGULADA PELO ORDENAMENTO JURÍDICO PÁTRIO. BITCOIN QUE NÃO TEM NATUREZA DE MOEDA NEM VALOR MOBILIÁRIO. INFORMAÇÃO DO BANCO CENTRAL DO BRASIL (BCB) E DA COMISSÃO DE VALORES MOBILIÁRIOS (CVM). INVESTIGAÇÃO QUE DEVE PROSSEGUIR, POR ORA, NA JUSTIÇA ESTADUAL, PARA APURAÇÃO DE OUTROS CRIMES, INCLUSIVE DE ESTELIONATO E CONTRA A ECONOMIA POPULAR.

1. A operação envolvendo compra ou venda de criptomoedas não encontra regulação no ordenamento jurídico pátrio, pois as moedas virtuais não são tidas pelo Banco Central do Brasil (BCB) como moeda, nem são consideradas como valor mobiliário pela Comissão de Valores Mobiliários (CVM), não caracterizando sua negociação, por si só, os crimes tipificados nos arts. 7º, II, e 11, ambos da Lei n. 7.492/1986, nem mesmo o delito previsto no art. 27-E da Lei n. 6.385/1976.

¹⁸⁷ BRASIL. Superior Tribunal de Justiça. **Conflito negativo de competência nº 161.123/SP**. Relator Ministro Sebastião Reis Júnior, Terceira Seção, julgado em 28/11/2018, publicado no DJe em 5/12/2018.

2. Não há falar em competência federal decorrente da prática de crime de sonegação de tributo federal se, nos autos, não consta evidência de constituição definitiva do crédito tributário.

3. Em relação ao crime de evasão, é possível, em tese, que a negociação de criptomoeda seja utilizada como meio para a prática desse ilícito, desde que o agente adquira a moeda virtual como forma de efetivar operação de câmbio (conversão de real em moeda estrangeira), não autorizada, com o fim de promover a evasão de divisas do país. No caso, os elementos dos autos, por ora, não indicam tal circunstância, sendo inviável concluir pela prática desse crime apenas com base em uma suposta inclusão de pessoa jurídica estrangeira no quadro societário da empresa investigada.

4. Quanto ao crime de lavagem de dinheiro (art. 1º da Lei n. 9.613/1998), a competência federal dependeria da prática de crime federal antecedente ou mesmo da conclusão de que a referida conduta teria atentado contra o sistema financeiro e a ordem econômico-financeira, ou em detrimento de bens, serviços ou interesses da União, ou de suas entidades autárquicas ou empresas públicas (art. 2º, III, a e b, da Lei n. 9.613/1998), circunstâncias não verificadas no caso.

5. Inexistindo indícios, por ora, da prática de crime de competência federal, o procedimento inquisitivo deve prosseguir na Justiça estadual, a fim de que se investigue a prática de outros ilícitos, inclusive estelionato e crime contra a economia popular.

6. Conflito conhecido para declarar a competência do Juízo de Direito da 1ª Vara de Embu das Artes/SP, o suscitado.

Já, no TRF4, a Operação Daemon¹⁸⁸ deflagrada pela Polícia Federal em conjunto com o Ministério Público Federal, apurou a prática de estelionato, pirâmide financeira, lavagem de dinheiro, organização criminosa e crimes contra o sistema financeiro nacional. No julgado analisado o Ministério Público apontou as

¹⁸⁸ BRASIL. Tribunal Regional Federal (4. Região). **Habeas Corpus nº 5044182-02.2021.4.04.0000**. Impetrante: Marcelo Almeida e Adrielle Santos em favor de Claudio Jose de Oliveira. Impetrado: Juízo da 23ª Vara Federal de Curitiba. Oitava Turma, Relator: Carlos Eduardo Thompson Flores Lenz. Porto Alegre, 24 novembro de 2021.

condutas supracitadas porque ficou constatado que a organização fornecia opções ostensivas de investimento enquanto, na verdade, fraudava os consumidores, usando uma complexa operação criminosa de longo prazo irrigada por um vasto volume monetário, reunido ao longo dos anos por meio de investimentos em criptomoeda, nestas palavras:

EMENTA: ORGANIZAÇÃO CRIMINOSA. PRISÃO PREVENTIVA. MANUTENÇÃO. GARANTIA DA ORDEM PÚBLICA, DA APLICAÇÃO DA LEI PENAL E PARA RESGUARDAR A CONVENIÊNCIA DA INSTRUÇÃO CRIMINAL. RISCO CONCRETO DE REITERAÇÃO DELITIVA.

1. Cláudio José de Oliveira teve sua prisão preventiva decretada no âmbito da "Operação Daemon", que apura de crimes previstos nos artigos 171 do Código Penal (estelionato), art. 1º, IX, da Lei nº 1.521/1951 (crime contra a economia popular), arts. 7º, II, e 22, parágrafo único, da Lei nº 7.492/1986 (crimes contra o sistema financeiro nacional), art. 1º da Lei nº 9.613/1998 (lavagem de capitais) e art. 2º, caput, da Lei nº 12.850/2013 (organização criminosa).
2. O vasto acervo probatório angariado dá conta de que Cláudio era o líder da organização criminosa, o qual oferecia supostas oportunidades de investimentos, enquanto, na verdade, dava desfalques nos clientes, por meio de um "sofisticado esquema criminoso de longo tempo de duração, irrigado por grande volume de dinheiro obtido ao longo dos anos a partir de investimentos realizados em criptomoedas".
3. Estão presentes os elementos de materialidade, os indícios de autoria, restando comprovado, ainda, que o réu tentou incessantemente transferir, ocultar e desfazer-se de seus bens, o que caracteriza o risco à garantia da ordem pública, da ordem econômica e da aplicação da lei penal.
4. Não se mostra adequada a substituição da prisão preventiva por uma das medidas elencadas no art. 319 do CPP, pois não constituem meios hábeis a resguardar eficazmente a ordem pública de novas práticas delituosas ou para garantir o atendimento pelo paciente ao chamado do Poder Judiciário.

5. O STF firmou entendimento no sentido de que a falta da reavaliação da preventiva, a cada 90 dias, nos termos do artigo 316, parágrafo único, do CPP, não gera direito à revogação automática da prisão preventiva. Ademais, a decisão que recebeu a denúncia, em agosto de 2021, reafirmou a necessidade de manutenção da segregação cautelar.

6. Denegação da ordem.

Sob outra perspectiva, ainda no TRF4, na ação penal oriunda da Operação Egypto, aventou-se pela defesa atipicidade da conduta por falta de legislação vigente, através de um Habeas Corpus. Contudo, a corte esclareceu que o assunto é relativamente novo no campo do direito, não havendo uma orientação abrangente sobre o status legal das criptomoedas, e que não havia, naquela caso, um pretexto para discutir prematuramente uma questão tão complicada e importante, inferida em um único documento submetido à Corte, e no restrito espaço de conhecimento inerente à ação constitucional, *in verbis*¹⁸⁹:

EMENTA: HABEAS CORPUS. OPERAÇÃO EGYPTO. TRANCAMENTO DA AÇÃO PENAL. HIPÓTESE EXCEPCIONALÍSSIMA. CRIMES CONTRA O SISTEMA FINANCEIRO NACIONAL. ATIPICIDADE. CONSTATAÇÃO DE PLANO. INOCORRÊNCIA. TESES DEFENSIVAS RELATIVAS AO CONCEITO, NATUREZA E DEFINIÇÃO JURÍDICA DE CRIPTOATIVOS. MATÉRIA A SER LEVANTADA E AMPLAMENTE DISCUTIDA NO CURSO DA INSTRUÇÃO CRIMINAL. INCABÍVEL O EXAME NA VIA ESTREITA DO HABEAS CORPUS PARA O PREMATURO TRANCAMENTO DA AÇÃO PENAL.

1. Os Tribunais Superiores já firmaram entendimento no sentido de ser imperiosa a necessidade de racionalização do writ, devendo ser observada sua função constitucional de sanar ilegalidade ou abuso de poder que resulte coação ou ameaça à liberdade de locomoção.

¹⁸⁹ BRASIL. Tribunal Regional Federal (4. Região). **Habeas Corpus nº 5017581-56.2021.4.04.0000**. Impetrante: Alexandre Collares, Pedro Machado de Almeida Castro, Octavio Orzari, Vinícius André de Sousa e Bruno Henrique de Moura em favor de Angelo Ventura da Silva. Impetrado: Juízo Federal da 7ª Vara Federal de Porto/Alegre/RS. Sétima Turma, Relatora Bianca Georgia Cruz Arenhart. Porto Alegre, 17 de agosto de 2021.

2. A utilização de habeas corpus para suspensão ou trancamento de ação penal, por ausência de justa causa ou inépcia da denúncia é medida excepcionalíssima, cabível apenas quando o fato narrado na denúncia não configurar, nem mesmo em tese, conduta delitiva, quando restar evidenciada a ilegitimidade ativa ou passiva das partes, quando incidir qualquer causa extintiva da punibilidade do agente, ou quando eventual deficiência da inicial acusatória impedir a compreensão da acusação, comprometendo o direito de defesa, hipóteses a serem constatadas de plano, por prova pré-constituída, pois inviável o exame probatório em sede de habeas corpus.

3. A aferição sobre a natureza das atividades efetivamente exercidas pela empresa, a definição jurídica de criptoativos, e eventual readequação típica nos termos do art. 383 do CPP demanda dilação probatória e envolve matéria complexa a ser examinada e discutida no curso da ação penal e decidida em sentença, não cabendo a pretendida incursão sobre o tema pela via estreita do habeas corpus, nem a postulada emendatio libelli antecipada, com a "desclassificação para crime contra a economia popular ou mesmo para estelionato, que, pelas mesmas razões, se for o caso, ocorrerá no momento processual oportuno.

4. Tratando-se de discussão relativa à definição jurídica de criptoativos - "matéria a ser levantada e amplamente discutida no curso da instrução criminal" -, que ainda não foi decidida nem mesmo pelo Superior Tribunal de Justiça, não se tem comprovação de plano da atipicidade sustentada pela defesa a autorizar o trancamento da ação penal.

5. O tema ainda é novo na jurisprudência, não há orientação consolidada acerca da natureza jurídica das criptomonedas, e não se revela adequada a pretensão de discutir questão tão complexa e relevante de forma prematura, deduzida em única peça apresentada ao Tribunal, e no restrito espaço de conhecimento inerente à ação constitucional.

(TRF4, HC 5017581-56.2021.4.04.0000, SÉTIMA TURMA, Relatora BIANCA GEORGIA CRUZ ARENHART, juntado aos autos em 17/08/2021)

No Habeas Corpus nº 2216677-24.2022.2022.8.26.0000¹⁹⁰, da Comarca de São Paulo, a 7ª Câmara de Direito Criminal indeferiu o pleito defensivo sob argumento de que havia, naquele momento processual, prova suficiente de materialidade quanto ao crime de lavagem de dinheiro e que a soltura do réu seria incabível, por se tratar de ação penal da qual o meio empregado (criptoativos) possibilita transacionar de qualquer lugar do mundo, proferindo da seguinte forma:

Pelo que consta o paciente está respondendo por estelionato, pichadíssimo, organização criminosa e lavagem de dinheiro Inicialmente a r. decisão menciona pedido do Delegado de Polícia e da anuência do Ministério Público, fazendo menção expressa a eles, que podem ser considerados como fundamentação aliunde. Além disto, destaca o risco concreto de fuga em face do alto valor das transações financeiras, que estão em criptomoedas e podem ser acessadas de qualquer lugar do mundo. Também destaca a existência de testemunhas e mídias onde se demonstra que o paciente, juntamente com terceiros, montou uma organização criminosa que teria movimentado mais de mais de quatorze milhões de reais em cinco meses para captar vítimas, as enganando em sistemas de pirâmide e estelionato com venda fictícia de criptomoedas Também presente indícios de autoria e materialidade da lavagem de dinheiro no fato de serem apreendidos vários objetos de alto valor, adquiridos em dinheiro em espécie, bem como o uso de terceira pessoa, conhecida nos meios policiais como "laranja profissional", que costuma prestar serviços ao PCC, para por meio dela adquirir carros de luxo. Ressalta-se, finalmente, o uso de empresas pelo paciente para tais condutas. Desta forma, demonstrados indícios suficientes de autoria dos Crimes. Visto a grande quantidade de dinheiro em espécie, estando ele em criptomoedas, que podem ser transacionadas em qualquer lugar do mundo, indispensável a manutenção do paciente no país para se evite sua fuga.

Nessa mesma toada o STJ fundamentou o Habeas Corpus nº 699416-MG (2021/0325254-5)¹⁹¹. O resumo das alegações do membro ministerial é que o

¹⁹⁰ BRASIL. Tribunal de Justiça do Estado de São Paulo. **Habeas Corpus nº 2216677-24.2022.2022.8.26.0000**, Relator: Mens de Mello, julgado em 26/09/2022 pela 7ª Câmara de Direito Criminal.

¹⁹¹ BRASIL. Superior Tribunal de Justiça. **Habeas Corpus n. 699.416**. Relator Ministro Antonio Saldanha Palheiro, Publicado no DJe em 02/12/2021.

investigado, juntamente com terceiros, se uniu sob a forma de organização criminosa com o objetivo de praticar o crime conhecido como pirâmide, bem como crimes contra relações de consumo, estelionato e lavagem de dinheiro e que após a concessão das medidas judiciais, foram realizados atos para ouvir as potenciais vítimas da fraude. É dos autos que as sociedades dos réus foram utilizadas pelos arguidos para atividades ilícitas conducentes à posterior aquisição de bens móveis e imóveis, por si próprios ou através de laranjas. A empresa teria faturado milhões em diversas movimentações financeiras, utilizando laranjas para a lavagem do capital com criptoativos. O relator, monocraticamente, decidiu que:

Nesse sentido, v.g., o levantamento preliminar realizado à folha 68, indicando a existência de 15 possíveis vítimas (que investiram valores entre 72 e 500 mil reais), extratos bancários de folhas 199/265, informando movimentação financeira através de TED, documentos/transferências bancárias entregues pelas possíveis vítimas às folhas 275/288, 334/342, interceptações telefônicas envolvendo todos os investigados (f. 643/669, 665/668, 675/674, 716/728, tudo levando os indícios a crer que todos os investigados operavam em conjunto e que permanecendo os investigados que se requer os acautelamentos em liberdade, possibilitará a continuidade da organização criminosa atraindo investidores através de sites na internet, os ludibriando através de remunerações de valores iniciais com valores oriundos de outros investidores iniciais, transformando os recursos em criptomoedas, e os pulverizando em nomes de terceiros, os quais, indicam os indícios, que se tratam dos demais investigados agindo em conluio. Portanto, como já salientado quando da análise do pedido liminar, a prisão teve como fundamento o fato de "a organização criminosa da qual o paciente supostamente faz parte tem atuação em cinco Estados da Federação, com vítimas em todo o país e prejuízos que ultrapassam 50 milhões de reais" (e-STJ fl. 32). Tal circunstância autoriza a decretação da prisão preventiva pois, conforme magistério jurisprudencial do Pretório Excelso, "a necessidade de se interromper ou diminuir a atuação de integrantes de organização criminosa enquadra-se no conceito de garantia da ordem pública, constituindo fundamentação cautelar idônea e suficiente para a prisão preventiva" (STF, HC n. 95.024/SP, relatora Ministra Cármen Lúcia, Primeira Turma, DJe 20/2/2009).

Com isso, deduz-se dos julgados a dificuldade do juiz em subsumir a tipicidade penal praticada, o risco empregado pela conduta perpetrada e a dificuldade do juízo, mesmo após o réu se encontrar cautelarmente preso, em cessar a lavagem de dinheiro. O tema das pirâmides financeiras, evasão de divisas e estelionato é apenas o começo do novo imbróglio que o parecer 40 da CVM trará. No entanto, aparentemente, os tribunais concordam que a lavagem de dinheiro usando criptoativos é aplicável, devido à dissimulação e ocultação que podem fornecer e especialmente pela transnacionalidade do ativo digital.

Formalmente, a venda pública de investimentos no mercado de criptoativos é legislada. Afinal, por se tratar de um acordo coletivo de investimento, a conduta enquadra-se nas categorias previstas nos artigos 7º e 16 da Lei nº 4.595/64. Portanto, dado as circunstâncias perscrutadas, a lavagem de capitais através da compra de criptoativos por corretoras descentralizadas e/ou *peer-to-peer*, inserindo em moedas anônimas, reintegrando ao mercado nacional caracteriza crime nos termos da Lei 9.613/98. É nesse sentido que as autoridades nacionais intentam dismantelar grupos especializados no branqueamento de capital.

Recentemente, a Polícia Federal e a Receita Federal, iniciaram (setembro de 2022) a Operação Colosso, objetivando combater uma organização envolvida com lavagem de dinheiro. A Receita Federal alega que a organização explorou um sistema sofisticado de transferência de recursos criminosos para o exterior por meio da aquisição e venda de criptoativos.¹⁹² Segundo a PF, as operações cambiais suspeitas movimentaram mais de R\$ 2 bilhões. Tais recursos entravam e fluíam através do sistema financeiro formal, através de empresas de fachada com pouca capacidade econômica ou financeira, além de contas transitórias até serem convertidos em criptoativos que pudessem ser utilizados no exterior.

¹⁹² LABOISSIÈRE, Paula. **Operação combate lavagem de dinheiro no mercado de criptomoedas.** AgênciaBrasil. Disponível em: <<https://agenciabrasil.ebc.com.br/geral/noticia/2022-09/operacao-combate-lavagem-de-dinheiro-no-mercado-de-criptomoedas>>, acesso em 22/10/2022.

Em que pese a lavagem de dinheiro por criptoativos seja recente no Brasil e que a regulamentação, conceito jurídico e marco legislativo permeiam embaraço e dissenso, verifica-se que tal conduta é imputável pelos tribunais brasileiro e ultimamente atraiu espaço adicional nas investigações policiais, pois conforme demonstrado a característica do ativo digital facilita com que as fases da lavagem de dinheiro sejam, teoricamente, não rastreáveis, possibilitando a ocultação de proveitos criminosos. Contudo, cumpre destacar que os julgados encontrados sequer são ações penais transitadas em julgado e que toda e qualquer informação criminal acerca da lavagem de dinheiro através desse novo meio de troca se deu, até o momento, em face do descobrimento de outros crimes, como por exemplo as pirâmides financeiras. Ante o exposto, depreende-se que os crimes entremeiam os criptoativos são: pirâmide financeira, estelionato, organização criminosa, lavagem de dinheiro, evasão de divisas, crimes contra o sistema financeiro nacional e crimes contra a ordem econômica. É possível argumentar que não há exaurimento tipificado retro, pois conforme acentuado, a conduta praticada é ligada a vários fatores, cujos possibilitam práticas ilícitas.

Por fim, diferentemente do noticiado pela mídia nacional, a jurisdição americana avança no combate da lavagem de dinheiro pelo criptoativo. É ordinário que megaoperações oriundas do departamento de justiça americano sejam manchetes de jornais. Logo, o próximo subcapítulo tem por enfoque analisar como a jurisdição americana se dissemelha da brasileira e de que modo os precedentes jurídicos, na esfera penal, são sobrepostos.

3.2 A RELAÇÃO ENTRE OS JULGADOS NACIONAIS E A JURISDIÇÃO AMERICANA

A lavagem de dinheiro é crime nos Estados Unidos desde 1986, tornando o país um dos primeiros países a criminalizar sua prática. Existem duas disposições criminais de lavagem de dinheiro, 18 Código dos Estados Unidos, Seções 1956 e 1957 (18 U.S.C. §§ 1956 e 1957).

Há ampla jurisdição extraterritorial sob as disposições penais de lavagem de dinheiro. De acordo com a Seção 1956, existe jurisdição extraterritorial sobre a conduta de lavagem de dinheiro por um cidadão dos EUA em qualquer

lugar do mundo, ou sobre um cidadão não americano, se a conduta ocorrer parcialmente nos Estados Unidos. Parcialmente pode ser considerada uma transferência de fundos para um banco dos EUA.

De acordo com a Seção 1957, existe jurisdição sobre crimes ocorridos fora dos Estados Unidos por pessoas dos EUA (cidadãos, residentes e pessoas jurídicas) e indivíduos de fora dos EUA, desde que a transação ocorra total ou parcialmente em solo americano.

SULLIVAN¹⁹³ afirma que o Departamento de Justiça dos EUA é responsável por processar qualquer pessoa considerada culpada por crimes de lavagem de dinheiro. A Divisão Criminal do Departamento de Justiça tem uma divisão especializada, chamada Seção de Lavagem de Dinheiro e Recuperação de Ativos ("MLARS"), a qual é responsável por processar casos de lavagem de dinheiro e tomar as medidas de confisco correspondentes. As 94 Procuradorias dos EUA localizadas no país e seus territórios, podem processar casos de lavagem de dinheiro por conta própria ou em conjunto com o MLARS. Qualquer processo de uma instituição financeira por um Ministério Público dos EUA requer a aprovação do MLARS.

O Secretário do Tesouro, o Secretário de Segurança Interna, o Procurador-Geral e o Serviço Postal têm um memorando de entendimento (não público), delineando as funções e responsabilidades das várias agências federais de aplicação da lei com jurisdição investigativa sobre as Seções 1956 e 1957, conforme exigido pela Seção 1956(e)¹⁹⁴. A definição ampla de jurisdição é a autoridade para conduzir uma investigação sobre o comportamento criminoso declarado subjacente. Em circunstâncias onde suas jurisdições se sobrepõem, os diferentes órgãos federais colaboram regularmente com as autoridades estaduais e municipais.

¹⁹³ SULLIVAN, Kevin. (2015). *Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business*. Editora Apress: 2015, California/USA.

¹⁹⁴ CORNELL. **18 U.S. Code § 1956 - Laundering of monetary instruments**. Disponível em: <<https://www.law.cornell.edu/uscode/text/18/1956>>, acesso 10/10/2022.

As investigações de lavagem de dinheiro são realizadas rotineiramente pelo Federal Bureau of Investigation, Drug Enforcement Administration, U.S. Secret Service, U.S. Immigration and Customs Enforcement, Internal Revenue Service Criminal Division e Postal Inspection Service. Os delitos de lavagem de dinheiro ligados a crimes ambientais podem ser investigados por uma unidade de investigação da Agência de Proteção Ambiental.

As penalidades potenciais, para lavagem de dinheiro, são prisão individual de até 20 anos e multas de até \$ 500.000 ou o dobro do valor da propriedade em questão, o que for maior.

Desde 2002, cerca de 39 instituições financeiras sujeitas aos requisitos regulatórios de AML entraram em acordos de delação premiada ou chegaram a acordos com o Departamento de Justiça. Conforme declarado, esses acordos são baseados em supostas violações dos requisitos regulatórios anti-lavagem de dinheiro ("AML") da BSA (como falha em manter um Programa AML eficaz e/ou falha em enviar relatórios de atividades suspeitas ("SARs" obrigatórios).

Além das violações da BSA, alguns desses acordos com bancos estrangeiros supostamente envolviam violações de sanções. Como parte desses acordos, penalidades significativas ou confiscos foram pagos. Dois processos adicionais da BSA contra bancos por não relatarem transações em moeda ocorreram no final dos anos 1980 e, em 1990, o Banco de Crédito e Comércio Internacional (BCCI) admitiu a lavagem de dinheiro.

Nesse diapasão, conforme breve introdução, os Estado Unidos combatem ativamente o crime de lavagem de dinheiro há décadas. Contudo, recentemente iniciou um novo conflito, enraizado pela diversidade digital e discricionariedade do criptoativo. Em resposta à ascensão criminal, pelo emprego de criptoativos nas fases da lavagem de dinheiro, em setembro de 2022, o Departamento de Justiça Americano anunciou um relatório¹⁹⁵ dissertando como

¹⁹⁵ JUSTICE. **The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets.** Disponível em: <<https://www.justice.gov/ag/page/file/1535236/download>>, acesso em 22/10/2022.

assegurar que ativos digitais sejam desenvolvidos com responsabilidade, e os meios utilizados pelo governo para prevenir a prática criminosa com os criptoativos. Outrora, destaca que *“This Report is a companion to the International Law Enforcement Cooperation Report and serves as an update to the Cryptocurrency Enforcement Framework.”*¹⁹⁶

O relatório do departamento descreve as diversas maneiras pelas quais os criminosos usaram ativos digitais no início de sua seção sobre o papel da aplicação da lei em detectar, investigar e processar atividades criminosas usando-os. Distingue três tipos principais de usos ilegais: 1) usar criptomoedas para financiar ou facilitar atividades criminosas; 2) usar ativos digitais para ocultar atividades financeiras ilícitas; e 3) crimes que envolvam ou prejudiquem o ecossistema de ativos digitais. O departamento reafirma os riscos inerentes dos criptoativos e a necessidade de integração jurisdicional, ainda afirma que:

As your Executive Order recognizes, the growing use of digital assets in the global financial system demands strong steps to reduce the risk that digital assets are used for illicit finance or other criminal purposes - such as money laundering, cybercrime, ransomware, narcotics, theft and fraud, and human trafficking - or to undermine our national security by enabling terrorism and proliferation financing. The Department of Justice and our law enforcement and regulatory partners are committed to protecting the public from criminal actors in the digital assets ecosystem and to meeting the unique challenges posed by developments in digital asset technologies.¹⁹⁷

O relatório também discute como a nova tecnologia, particularmente no campo das finanças descentralizadas, ou DeFi, apresenta novas dificuldades para a aplicação da lei; fornece exemplos de esforços bem-sucedidos de aplicação da lei para investigar, processar e impedir crimes envolvendo ativos digitais, apesar

¹⁹⁶ JUSTICE. **The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role of Law Enforcement in Detecting, Investigating, And Prosecuting Criminal Activity Related to Digital Assets.** Disponível em: <<https://www.justice.gov/ag/page/file/1535236/download>>, acesso em 22/10/2022. p. 6.

¹⁹⁷ JUSTICE. **The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role of Law Enforcement in Detecting, Investigating, And Prosecuting Criminal Activity Related to Digital Assets.** Disponível em: <<https://www.justice.gov/ag/page/file/1535236/download>>, acesso em 22/10/2022. p. 2.

dessas dificuldades; e descreve os programas que o departamento e outras agências de aplicação da lei estabeleceram, como o lançamento da DAC Network pelo departamento. Contudo, é salientado pelo parecer que:

Criminals continue to use cryptocurrency and other digital assets for money laundering, facilitating tax evasion, and evading sanctions. Criminals have developed increasingly sophisticated obfuscation techniques— complex and rapid transactions, “chainhopping” by converting funds from one cryptocurrency into another, use of AECs, and other measures—designed to make tracing difficult and to place stolen funds beyond recovery. Criminals can also use mixers and tumblers, including automated services that employ smart contracts to combine multiple users’ coins together before sending out unrelated coins to each user’s designated recipient, to obfuscate their transactions.¹⁹⁸

Ao fim, o Departamento de Justiça Americano avulta que os mercados emergentes e tecnologia trazidos pelo crescimento de ativos digitais deram aos criminosos novas maneiras de ferir vítimas específicas, contornar leis, contornar sanções econômicas, financiar o terrorismo e lavar dinheiro ilícito. Em que pese a Autoridade Americana esteja comprometida em combater atividades criminosas tecnologicamente sofisticadas e seja hábil para fazê-lo, serão necessários esforços orçamentários, legislativos e regulatórios significativos para acompanhar e proteger as vítimas do uso indevido da tecnologia em rápida evolução no espaço de ativos digitais. Independentemente disso, é necessário que os órgão competentes e seus parceiros se adaptem à medida que os mercados e aplicativos para ativos digitais mudam, implantando efetivamente o conhecimento adquirido recentemente e fazendo uso dos recursos já existentes para educar novas gerações de agentes, analistas, promotores e outros advogados que, em tese, serão capazes de usar todos os recursos à sua disposição para mitigar riscos nesta área e levar malfeitores à justiça.

¹⁹⁸ JUSTICE. **The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role of Law Enforcement in Detecting, Investigating, And Prosecuting Criminal Activity Related to Digital Assets.** Disponível em: <<https://www.justice.gov/ag/page/file/1535236/download>>, acesso em 22/10/2022. p. 12.

A regulamentação de criptomoedas nos Estados Unidos é um campo jurídico complexo e em constante evolução, envolvendo várias agências federais e locais. A *Securities and Exchange Commission (SEC)*, a *Commodity Futures Trading Commission (CFTC)* e o *Internal Revenue Service (IRS)* são as principais agências reguladoras governamentais envolvidas em criptomoedas.

A SEC destaca que algumas criptomoedas, como as oferecidas em ofertas iniciais de moedas (ICOs), podem ser consideradas valores mobiliários e sujeitas às regras federais de valores mobiliários. A CFTC tem autoridade sobre transações de derivativos, incluindo aquelas baseadas em criptomoedas, e tomou medidas contra fraudes envolvendo moedas digitais.

Para fins fiscais, o IRS considera a criptomoeda como propriedade, o que significa que os ganhos de negociação de criptomoedas estão sujeitos ao imposto sobre ganhos de capital. A regulamentação estadual varia, com alguns estados aprovando legislação para supervisionar as trocas de criptomoedas e outros adotando uma abordagem mais permissiva. Nova York tem sido especialmente ativa na regulamentação de criptomoedas por meio de seu programa BitLicense, que exige que as empresas que desejam operar no mercado de criptomoedas do estado adquiram uma licença.

A regulamentação de criptomoedas nos Estados Unidos está em constante evolução, e há um debate em curso sobre o grau adequado de regulamentação necessário para proteger os investidores e evitar atividades ilícitas sem sufocar a inovação.

Ante o exposto, os julgados com maior repercussão, que envolvem criptoativos e o efetivo combate através das autoridades retro citadas, são: Liberty, Eastern Metal Securities, Lichtenstein e Morgan, Polybius Bank.

Liberty Reserve

O Departamento de Justiça dos EUA acusou a Liberty Reserve, um transmissor de dinheiro com sede na Costa Rica, e sete de seus diretores e funcionários de operar um negócio intermediador de dinheiro não registrado e

lavagem de dinheiro por facilitar a movimentação de mais de 6 bilhões de dólares em receitas ilícitas em maio de 2013, no que é atualmente o maior caso de lavagem de dinheiro online da história¹⁹⁹. O Departamento do Tesouro essencialmente desligou o Liberty Reserve do sistema financeiro dos EUA, designando-o como uma instituição financeira de principal preocupação com lavagem de dinheiro sob a Seção 311 do USA PATRIOT Act.

A fim de escapar da atenção regulatória e da aplicação da lei e para ajudar os criminosos na distribuição, armazenamento e lavagem de receitas de fraude de cartão de crédito, roubo de identidade, fraude de investimento, hacking de computador, tráfico de narcóticos e pornografia infantil, o Liberty Reserve foi criado em 2006. Operando em grande escala, realizou mais de 55 milhões de transações, praticamente todas ilegais, e teve mais de um milhão de membros em todo o mundo, incluindo mais de 200.000 nos Estados Unidos. Embora tivesse sua própria moeda virtual, Liberty Dollars (LR), as transações eram feitas e armazenadas usando moeda fiduciária nas duas pontas (dólares americanos).

O GAFI²⁰⁰ declarou que:

To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names (“Russia Hackers,” “Hacker Account,” “Joe Bogus”) and blatantly false addresses (“123 Fake Main Street, Completely Made Up City, New York”).

Arthur Budovsky, 42 anos, foi condenado a 20 anos²⁰¹ de prisão em 2016, por um juiz federal em Manhattan por operar um vasto esquema de lavagem de dinheiro utilizando sua empresa, Liberty Reserve, que antes era usada por

¹⁹⁹ DINORO, Rinatis. **The Truth About Liberty Reserve**. Epub Kindle Edition.

²⁰⁰ FATF. **Guidance for a risk-based approach: virtual currencies**. Disponível em <<https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>>, acesso em 10/07/2022.

²⁰¹ JUSTICE. Liberty Reserve Founder Arthur Budovsky Sentenced In Manhattan Federal Court To 20 Years For Laundering Hundreds Of Millions Of Dollars Through His Global Digital Currency Business. Disponível em <<https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years>>, acesso em 20/10/2022.

cibercriminosos em todo o mundo para ocultar os lucros de seus negócios ilícitos. Em outubro de 2014, BUDOVSKY foi extraditado para os Estados Unidos após ser detido na Espanha em maio de 2013. Em 29 de janeiro de 2016, BUDOVSKY se declarou culpado de uma acusação de conspiração para lavagem de dinheiro, três dias antes do início de seu julgamento. A sentença foi proferida pela juíza distrital dos EUA Denise L. Cote, a qual observou que o réu não demonstrou arrependimento real e que suas ofensas resultaram em danos significativos e criaram inúmeras vítimas de fraude em todo o mundo.

Eastern Metal Securities

Roger Nils-Jonas Karlsson, um cidadão sueco, foi condenado a 15 anos de prisão (United States vs. Roger Karlsson and Eastern Metal Securities) por fraude de valores mobiliários, fraude eletrônica e crimes de lavagem de dinheiro com criptoativos envolvendo milhares de vítimas. O tribunal também ordenou que o réu entregasse várias propriedades tailandesas, incluindo um resort, bem como um prêmio em dinheiro de confisco superior a US\$ 16 milhões de dólares. O Tribunal apresentou uma ordem de julgamento alterada em 22 de agosto de 2022, que incluía o cronograma de restituição do governo totalizando US\$ 8.532.068,77 de dólares.²⁰²

Em 4 de março de 2022, Roger Nils-Jonas Karlsson, 47, se declarou culpado. Karlsson liderou uma operação de fraude de investimento de 2011 até sua prisão na Tailândia em junho de 2019. Karlsson persuadiu as vítimas a investir na fraude *Eastern Metal Securities*, utilizando criptomoedas como Bitcoin e outros sistemas de pagamento online. Karlsson ofereceu às vítimas grandes recompensas com base nos preços do ouro. Em vez disso, o dinheiro das vítimas foi transferido para as contas bancárias pessoais de Karlsson e os ganhos foram usados para comprar residências luxuosas, um cavalo de corrida e um resort tailandês.

²⁰² JUSTICE. **Cryptocurrency Fraudster Sentenced for Money Laundering and Securities Fraud in Multi-Million Dollar Investment Scheme.** Disponível em: <<https://www.justice.gov/opa/pr/cryptocurrency-fraudster-sentenced-money-laundering-and-securities-fraud-multi-million-dollar>> acesso em 20/10/2022.

United States of America vs Ilya Lichtenstein and Heather Morgan at the U. S. District Court for the District of Columbia

Em outra megaoperação, o Governo Americano apreendeu US\$ 3,6 bilhões em criptomoedas, furtadas diretamente ligada a invasão hacker²⁰³ e furto digital da carteira Exchange Bitfinex, em 2016.

De acordo com os autos do tribunal²⁰⁴, Lichtenstein e Morgan planejavam lavar os ganhos de 119.754 bitcoins furtados da plataforma Bitfinex depois que um hacker se infiltrou nos servidores da empresa e lançou mais de 2.000 transações ilegais. Essas transações ilegais enviaram o bitcoin furtado para uma carteira digital controlada por Lichtenstein. Aproximadamente 25.000 desses bitcoins furtados foram retirados da carteira de Lichtenstein durante os cinco anos anteriores por meio de um método complicado de lavagem de dinheiro, que resultou em parte do dinheiro subtraído sendo colocado em contas financeiras controladas por Lichtenstein e Morgan. O restante, totalizando mais de 94.000 bitcoins, permaneceu na carteira usada para receber e guardar os ganhos ilícitos da invasão. Agentes especiais obtiveram acesso a arquivos em uma conta na Internet mantida por Lichtenstein após a execução de mandados de busca autorizados pelo tribunal em contas controladas por Lichtenstein e Morgan. Esses arquivos forneciam as chaves privadas necessárias para acessar a carteira digital que recebia o dinheiro retirado da Bitfinex diretamente, permitindo que agentes especiais apreendessem e recuperassem adequadamente mais de 94.000 bitcoins furtados da empresa Bitfinex. No momento da apreensão, os criptoativos apreendidos valiam mais de US\$ 3,6 bilhões.

O procurador dos EUA Matthew M. Graves do Distrito de Columbia afirmou que a criptomoeda e trocas de moeda virtual estão se tornando uma parte cada vez mais importante do sistema financeiro dos EUA, mas furtos de moeda

²⁰³ A exchange de criptomoedas Bitfinex foi hackeada em agosto de 2016. 119.754 bitcoins, no valor de cerca de US\$ 72 milhões na época, foram furtados.

²⁰⁴ JUSTICE. **Government Seized \$3.6 Billion in Stolen Cryptocurrency Directly Linked to 2016 Hack of Virtual Currency Exchange.** Disponível em <<https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launders-45-billion-stolen-cryptocurrency>>, acesso em 15/09/2022.

digital realizados por meio de esquemas complexos de lavagem de dinheiro podem minar a confiança na criptomoeda.

A denúncia criminal afirmou que Lichtenstein e Morgan usaram uma variedade de métodos sofisticados de lavagem de dinheiro, incluindo a criação de contas online com nomes falsos; automatização de transações com programas de computador; transferiram o dinheiro furtado em contas de várias bolsas de valores virtuais e mercados na *darknet*, reintegrado o dinheiro, o que permitiu que inúmeras transações ocorressem rapidamente. Ainda, foi identificado a utilização de um sistema complexo de mixagem de moedas.

Os réus foram acusados de lavar e disfarçar sua enorme renda em uma estratégia deliberada e calculada, de acordo com o chefe de investigação criminal do IRS, Jim Lee (IRS-CI)²⁰⁵. Contudo, agentes especiais da Unidade de Crimes Cibernéticos do IRS-CI descobriram o esquema sofisticado de lavagem de dinheiro, permitindo-lhes rastrear, acessar e coletar o dinheiro furtado, totalizando a maior apreensão de criptomoedas de todos os tempos, avaliada em mais de US\$ 3,6 bilhão.

As acusações contra Lichtenstein e Morgan incluem conspiração para fraudar os Estados Unidos e conluio para cometer lavagem de dinheiro, cada uma das quais acarreta uma possível sentença de 20 anos de prisão. Depois de levar em consideração as Diretrizes de Sentença dos EUA e outras considerações legais, um juiz do tribunal distrital federal decidirá sobre qualquer punição.²⁰⁶

Polybius Bank

Em outra investigação²⁰⁷, uma conspiração para fraude de bitcoin e lavagem de dinheiro de US\$ 575 milhões é objeto de uma ação penal de 18

²⁰⁵ BLOOMBERG. **'Hundreds' of Crypto Cases Coming, IRS Criminal Chief Says.** Disponível em: <<https://news.bloombergtax.com/crypto/hundreds-of-crypto-cases-coming-irs-criminal-chief-says>>, acesso em 03/12/2022.

²⁰⁶ JUSTICE. **Two Arrested for Alleged Conspiracy to Launder \$4.5 Billion in Stolen Cryptocurrency.** Disponível em: <<https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency>>, acesso em 05/10/2022.

²⁰⁷ JUSTICE. **Two Estonian Citizens Arrested in \$575 Million Cryptocurrency Fraud and Money**

acusações, resultante na prisão de dois indivíduos estonianos em Tallinn, na Estônia, em 20 de novembro de 2022.

Em 27 de outubro, um grande júri no Distrito Oeste de Washington produziu a acusação, a qual foi revelada em 21 de novembro de 2022.

De acordo com os autos do tribunal, Ivan Turgin e Sergei Potapenko, ambos com 37 anos, são acusados de fraudar centenas de milhares de pessoas por meio de um sistema complexo. Eles persuadiram as vítimas a se inscreverem nos falsos contratos de aluguel de equipamentos do serviço de mineração de bitcoin HashFlare dos réus. Além disso, eles convenceram as vítimas a investir no Polybius Bank, um banco de moeda virtual. Na verdade, Políbio nunca foi um banco e nunca fez os pagamentos de dividendos prometidos. Mais de \$ 575 milhões em compensação foram pagos pelas vítimas aos negócios de Potapenko e Turgin. Os fundos do golpe foram posteriormente utilizados por Potapenko e Turgin para comprar casas e automóveis de luxo enquanto eram lavados por empresas de fachada.

O departamento, que alegou estar o caso sob investigação do FBI, afirmou que o esquema de lavagem de dinheiro incluía pelo menos 75 propriedades imobiliárias, seis automóveis de luxo, carteiras de criptomoedas e milhares de equipamentos de mineração de criptomoedas.

Assim sendo, de acordo com o líder da divisão, Jim Lee, a divisão de Investigação Criminal do IRS está desenvolvendo centenas de casos criptográficos, muitos dos quais serão tornados públicos em breve²⁰⁸. Lee afirmou, em uma coletiva de imprensa²⁰⁹, que os casos envolvem fatos como transações off-

Laundering Scheme. Disponível em: <<https://www.justice.gov/opa/pr/two-estonian-citizens-arrested-575-million-cryptocurrency-fraud-and-money-laundering-scheme>>, acesso em 25/11/2022.

²⁰⁸ IRS. **2022 Annual Report.** Disponível em: <<https://www.irs.gov/pub/irs-pdf/p3583.pdf>>, acesso em 03/12/2022.

²⁰⁹ BLOOMBERG. **'Hundreds' of Crypto Cases Coming, IRS Criminal Chief Says.** Disponível em: <<https://news.bloombergtax.com/crypto/hundreds-of-crypto-cases-coming-irs-criminal-chief-says>>, acesso em 03/12/2022.

ramping²¹⁰, nas quais ativos digitais são convertidos em dinheiro fiduciário e pessoas recebem pagamentos em criptomoedas sem declará-los.

A fim de consolidar seus esforços para auxiliar na investigação de ativos digitais, investigação de crimes cibernéticos, perícia digital e perícia forense física, a agência americana estabeleceu o Escritório de Serviços Cibernéticos e Forenses em 2021. O intuito do órgão foi combater de forma efetiva a nova modalidade empregada na lavagem de capital.

Portanto, perfaz-se que nos Estados Unidos da América a investigação criminal, o combate cibernético, a prevenção e a implementação de regulamentações obrigatórias a corretoras de criptomoedas está em nível elevado se comparado ao Brasil. Observa-se que as operações americanas são oriundas de diversos crimes antecedentes, diferentemente do Brasil, que persegue a lavagem de dinheiro especificadamente em fraudes revestidas por pirâmide financeira e/ou esquema de ponzi. Deste modo, depreende-se que a lavagem de dinheiro, pelo meio criptoativo, está tipificada no ordenamento americano e é combatida nas diversas fases. Foi assinalado que o criptoativo por ter peculiaridades inerentes a sua criação pode criar risco sistêmico ao mercado financeiro como um todo, uma vez que a lavagem de dinheiro pelo ativo digital é transnacional e evade jurisdições distintas. O próximo subcapítulo tem como escopo analisar estratégias preventivas para o combate de lavagem de dinheiro. Para tanto, serão considerados os estudos supracitados e as orientações publicadas pelo GAFI, FinCen e autoridades americanas.

3.3 PREVENÇÃO E COMBATE A LAVAGEM DE CAPITAL ATRAVÉS DO CRIPTOATIVO

O uso de criptoativos no processo de lavagem de dinheiro potencializa efeitos significativos nas economias de todo o mundo. A lavagem de dinheiro ininterruptamente é um obstáculo crítico para os governos ao longo da história. O combate ao crime está ligeiramente correlacionado com as regulamentações

²¹⁰ Uma rampa de saída na tradução literal é um serviço que permite a troca de criptomoedas por moeda fiduciária. A disponibilidade de uma rampa de saída garante aos usuários que eles não estão presos a uma criptomoeda e podem “sair” (vender criptomoeda por moeda fiduciária) a qualquer momento.

financeiras, pois as fases da lavagem - colocação, ocultação e integração - são atos realizados desde a invenção do sistema bancário central. Devido ao sigilo que oferece, o criptoativo está veemente associado à lavagem de dinheiro. Grupos criminosos transferem capital com facilidade crescente e evitam o escrutínio do governo graças ao uso de criptoativos no processo de lavagem de dinheiro.

Os preços do Bitcoin e de outros criptoativos variam consideravelmente, mas demonstraram se tornar mais confiáveis e geralmente reconhecidos com o tempo. O uso indevido de criptoativos pode ser empregado para ameaçar a estabilidade da economia global - pois a fuga de capital é instantânea, acaso o processo de lavagem de dinheiro não for esmiuçado e combatido. A resposta para o problema do uso ilegal de criptoativos é a regulamentação e repressão da lavagem de dinheiro onde quer que seja encontrada, bem como a instituição de regramentos estritos de 'conheça seu cliente' (KYC) das próprias exchanges que intermediam criptoativos, incluindo controles comuns de combate à lavagem de dinheiro e outras medidas preventivas já empregadas no sistema bancário.

Especificadamente, o combate ao crime deve ser direcionado a cada fase da lavagem de dinheiro, pois diferente de práticas usuais a lavagem com criptoativos pode ser complexa e distinta de outros modelos já conhecidos. Para GRZYWOTZ²¹¹ a etapa de colocação, na lavagem de dinheiro, ocorre na coleta de criptoativos com valores obtidos da conduta de um crime anterior ou quando é infundido valores patrimoniais no sistema de criptoativos. Isso pode ser feito adquirindo criptoativos em bolsas, usando caixas eletrônicos para comprá-lo com dinheiro, valendo-se de plataformas que vinculam usuários para transações diretas, vendendo bens obtidos por meio de atividades criminosas e sendo pagos em ativo digital, comprando criptoativo diretamente com o produto de atividades criminosas, como por exemplo ao vender drogas e ser pago em Bitcoin e, ainda, transferir criptoativos de uma Exchange para outra.

²¹¹ GRZYWOTZ, Johanna. **Virtuelle Kryptowährungen und Geldwäsche**. Berlin: Duncker & Humblot.

A dissimulação, por outro lado, pode ser dividida em formas básicas e complexas. ESTELLITA²¹² afirma que a mais simples se caracteriza através de um único indivíduo produzir um número ilimitado de chaves públicas, alterando o endereço dos criptoativos sem perder o controle sobre elas. Também é possível usar os endereços de criptoativos fornecidos por terceiros, como consultores financeiros. No entanto, em cada um desses cenários, a abertura do blockchain simplificará o rastreamento do curso e do histórico das transações. No entanto, os dados do sistema não podem revelar as identidades dos usuários, ou seja, os proprietários dos endereços dos criptoativos. Como o titular do endereço não pode ser identificado e há grande rastreabilidade, é permitido referir-se ao pseudo-anonimato em vez de anonimato. Já, a forma complexa abrange a utilização de *coin mixers*, negociações na *Dark Web*²¹³, *Privacy Coins*²¹⁴, *OTC Market*²¹⁵ e *Decentralized exchanges*.

Na fase da integração, a lavagem ocorre pela troca de criptoativos por dinheiro fiduciário por meio de exchanges ou pela compra direta de bens e serviços. Cumpre destacar somente ser possível encontrar informações sobre uma transação se ela ocorre em um país que tenha jurisdição sobre as exchanges. No entanto, dada a natureza transnacional dos ativos digitais, é concebível escolher uma nação com medidas regulatórias menos rigorosas para a realização das operações.

Nesse sentido, uma das ferramentas mais utilizadas por organizações criminosas, de acordo com o Chainalysis²¹⁶, para burlar o sistema de pseudo-

²¹² ESTELLITA, Heloisa. **Criptomoedas e lavagem de dinheiro**. Revista Direito GV [online]. 2020, v. 16, n. 1 [Acessado 1 Dezembro 2022], e1955. Disponível em: <<https://doi.org/10.1590/2317-6172201955>>. Epub 27 Abr 2020. ISSN 2317-6172. <https://doi.org/10.1590/2317-6172201955>.

²¹³ A dark web é a parte invisível da internet que você só pode visitar usando um navegador especial, como o Tor. Tor é uma abreviação de The Onion Router.

²¹⁴ Moedas de privacidade são criptomoedas projetadas para proteger a privacidade do usuário e suas transações.

²¹⁵ Over-The-Counter Trading, ou OTC Trading, é uma estrutura de tecnologia financeira que permite negociar mercados fora de uma bolsa regular. Especificamente, dentro do mercado de criptomoedas e bitcoin, é um mercado comercial privado para compra ou venda de criptomoedas.

²¹⁶ CHAINANALYSIS. **The 2022 Crypto Crime Report**. disponível em: <<https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>>, acesso em 31/07/2022.

anonimato, é a troca através de Exchanges Descentralizadas. Os mercados (Exchanges Centralizadas) estruturados padrões são monitorados por um custodiante, uma pessoa jurídica que é responsável, em última instância, pelo cumprimento das exigências das autoridades reguladoras. Os usuários dessas trocas não têm acesso às suas chaves privadas, pois são mantidas em um depósito centralizado sob a autoridade do custodiante, o que é uma desvantagem significativa. Nem suas chaves, nem suas moedas, são teoricamente do usuário. Além disso, as trocas centralizadas são frequentemente alvo de hackers, alguns dos quais são bem-sucedidos. Por exemplo, o site comercial japonês *Coincheck*, que tinha um valor de mercado de US\$ 530 milhões, foi saqueado em 230 milhões de dólares em 2018. Já, por outro lado, DEXs (exchanges descentralizadas), são um novo modelo de troca, que surgiu recentemente. Segundo LIN²¹⁷ DEXs (Decentralized exchanges) são:

[...] protocolos de ledger distribuído e aplicativos que permitem aos usuários realizar transações com criptomoedas sem a necessidade de confiar em uma instituição centralizada para funcionar como intermediário da transação ou custodiante de sua criptomoeda.

Esses mercados usam contratos inteligentes *on-chain*²¹⁸ para realizar transações anonimamente pela Internet e não precisam, inclusive, de uma conta de e-mail. Os usuários podem gerenciar suas chaves privadas, os DEXs são dispersos para evitar um único ponto de falha (tempo de inatividade do servidor), não há terceiros ou risco de contraparte e os governos não podem censurar ou desligar os DEXs. Obviamente, não há regulamentos de política *Know Your Customer*. Nesse contexto, os usuários de criptoativos se tornam essencialmente seus próprios bancos.²¹⁹

²¹⁷ LIN. X. L., Legal Counsel at Interstellar and Stellar Development. (2019). **Deconstructing Decentralized Exchanges**. Stanford Journal of Blockchain Law & Policy. Disponível em <<https://stanford-jblp.pubpub.org/pub/deconstructing-dex>>, acesso em 01/12/2022.

²¹⁸ As transações que ocorrem em um blockchain e são registradas no livro-razão público distribuído são chamadas de transações "on-chain". As transações que atualizam a rede blockchain mais ampla são conhecidas como transações on-chain, pois foram verificadas ou autenticadas.

²¹⁹ GURREA-MARTINEZ, Aurelio; REMOLINA, Nydia. **The Law and Finance of Initial Coin Offerings**. Ibero-American Institute for Law and Finance, Working Paper Series, n. 4, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182261>, acesso em

Entretanto, definições recentes pela Força-Tarefa de Ação Financeira (GAFI) quanto a provedores de serviços de ativos virtuais incluem exchanges de criptomoedas, emissores de moedas estáveis, protocolos DeFi e mercados de tokens não fungíveis (NFT) como operadores financeiros e fiscalizáveis. Dessarte, os criptoativos podem ser utilizadas como ferramenta para prática de lavagem de dinheiro, bem como auxiliam na condução de ações ilícitas, necessitando de medidas de controle (regulação preventiva). É importante observar que nem a regulamentação, nem a criminalização do uso de criptoativos, devem impedir o desenvolvimento desse novo recurso. O cenário mundial regulamentário de criptoativos é positivo e está evoluindo como resultado.

Nos EUA e no Reino Unido a criação do marco legal para gerenciar e fiscalizar a negociação com criptomoedas é a resposta estatal. De acordo com o HM Treasury do Reino Unido²²⁰, todas as carteiras e emissores estarão sujeitos a regulamentos de crimes financeiros, incluindo requisitos anti-lavagem de dinheiro, e todos serão obrigados a se registrar sob o registro anti-lavagem de dinheiro para suas operações em relação a todas as variedades de criptoativos.

Nos Estados Unidos, os criptoativos são atualmente considerados legais e estão sob a autoridade da Lei de Sigilo Bancário (BSA). Com efeito, as exchanges de criptomoedas devem se registrar no FinCEN e seguir os requisitos de Anti-money laundering (AML) e financiamento contra o terrorismo (CFT).

O Conselho de Estabilidade Financeira (FSB)²²¹, um conselho composto por reguladores, funcionários do tesouro e banqueiros centrais do Grupo das 20 nações (G20), estabeleceu diretrizes mundiais para criptoativos em outubro de 2022. O FSB emitiu uma proposta para a regulamentação mundial das operações de criptoativos. Os principais componentes desta estrutura são ideias

10/11/2022.

²²⁰ GOV.UK. **Government sets out plan to make UK a global cryptoasset technology hub.** Disponível em: <<https://www.gov.uk/government/news/government-sets-out-plan-to-make-uk-a-global-cryptoasset-technology-hub>>, acesso em 03/12/2022.

²²¹ FSB. **FSB proposes framework for the international regulation of crypto-asset activities.** Disponível em <<https://www.fsb.org/2022/10/fsb-proposes-framework-for-the-international-regulation-of-crypto-asset-activities/>>, acesso em 07/11/2022.

para melhorar a consistência e amplitude das abordagens regulatórias, de supervisão e aplicação das atividades e mercados de criptoativos, bem como para aumentar a colaboração internacional, coordenação e compartilhamento de informações. Outrora, destacou que para lidar com os problemas associados à estabilidade financeira de forma eficaz, com sugestões de alto nível para a regulamentação, alterou o monitoramento e supervisão dos acordos de *stablecoin* globais.

O FSB consignou²²² que uma estrutura regulatória eficaz deve garantir que as operações de criptoativos estejam sujeitas a uma normatização abrangente e proporcional aos perigos que representam, ao mesmo tempo em que capitaliza as vantagens potenciais da tecnologia que as sustenta. Nos casos em que criptoativos e intermediários cumprem um papel econômico semelhante ao dos instrumentos e intermediários tradicionais do sistema financeiro, eles devem estar sujeitos a leis baseadas na premissa de mesma atividade, mesmo risco e mesma regulamentação. Ainda, destacou²²³ que:

High regulatory standards are required in particular for crypto-assets – such as stablecoins – that could be widely used as a means of payments and/or store of value, as they could pose significant risks to financial stability.

[...]

The high-level Recommendations seek to promote consistent and effective regulation, supervision and oversight of GSCs across jurisdictions to address the potential financial stability risks posed by GSCs, both at the domestic and international level, while supporting responsible innovation and providing sufficient flexibility for jurisdictions to implement domestic approaches.

²²² FSB. **Crypto-assets and Global “Stablecoins”**. Disponível em <<https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/crypto-assets-and-global-stablecoins/>>, acesso em 07/11/2022.

²²³ FSB. Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements: Consultative report. Disponível em <<https://www.fsb.org/wp-content/uploads/P111022-4.pdf>>, acesso em 03/12/2022.

Assim, infere-se que um dos fatores predominantes para reprimir a propagação da lavagem de capitais em criptoativos advém de fontes de informações, as quais buscam identificar manualmente ou automatizado o uso indevido de criptoativos, ou seja identificar as camadas transacionais e equiparar ao sistema de controle institucional de clientes bancários.

Das informações e operações coletadas, colige-se que as informações utilizadas no curso de investigações sobre o uso ilícito de moeda digital originam das mesmas fontes de investigações financeiras convencionais. No entanto, a força policial deve implementar novas habilidades e abordagens para usar e interpretar o livro chave do criptoativo, pois devido à sua tecnologia e ecossistema criptográfico modelos comuns tornam-se inoperáveis. A exemplo disso são medidas assecuratórias²²⁴ disponíveis no Código de Processo Penal (art. 125 ao 144 do CPP), se um criptoativo é custodiado por uma Exchange que não tem obrigatoriedade de cumprir leis brasileiras é improvável que um pedido de sequestro de bens seja efetivo.

Dessarte, existem seis categorias de informações convencionais que as Autoridades devem levar em conta, de acordo com o Relatório do GAFI: Questões Operacionais - Orientação para Investigações Financeira²²⁵. As categorias listadas pelo GAFI são:

Criminal records and intelligence: This is law enforcement information related to the subject and/or criminal activity. Information such as previous arrests, indictments, convictions, but also reports of links with known criminals. Criminal information is typically gathered from surveillance, informants, interviews/interrogation and data research, or may be just picked up “on the street” by individual police officers.

²²⁴ É o conjunto de medidas cautelares que visam assegurar os direitos do ofendido e a responsabilização pecuniária do criminoso. São elas o sequestro, o arresto e a hipoteca legal dos bens do indiciado ou do responsável civil.

²²⁵ FATF. **Operational Issues Financial Investigations Guidance**. Disponível em: <https://www.fatf-gafi.org/media/fatf/documents/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf>, acesso em 10/09/2022.

AML/CFT Disclosures: In addition to suspicious transaction reports (STRs), this includes other information as required by national legislation such as cash transaction reports, wire transfer reports and other threshold-based declarations or disclosures.

Financial Information: This is information about the financial affairs of entities of interest that helps to understand their nature, resources, structure and capabilities, and it also helps predict future activity and locate assets. This goes beyond the information contained in AML/CFT disclosures and is normally maintained by private third parties. This includes bank accounts, financial accounts, other records of personal or business financial transactions and information collected in the context of meeting customer due diligence (CDD) obligations.

Classified information: Information that is gathered and maintained for national security purposes to include terrorism financing information. Access is typically restricted by law or regulation to particular groups of persons.

Regulatory information: Information that is maintained by regulatory agencies; access is typically restricted to official use only. This category of information could be held by central banks, tax authorities, other revenue collecting agencies, etc.

Sendo assim, regulamentar o criptoativo através de legislação anti-lavagem de dinheiro (AML) refere-se às regras, políticas e procedimentos implementados para impedir que criminosos transformem o ativo digital adquirido ilicitamente em dinheiro fiduciário. A legislação AML internacional é padronizada pela Força-Tarefa de Ação Financeira (GAFI). Os formuladores de políticas nos estados membros do GAFI agiram rapidamente quando a orientação da organização sobre criptomoeda AML foi publicada em 2014. Nos dias atuais, o FinCEN, a Comissão Europeia e várias outras organizações reguladoras ratificaram a maioria das sugestões que lhes foram sugeridas.

Apesar de sua arquitetura transparente e rastreável, o criptoativo permanece atraente para os criminosos devido aos seus pseudônimos e à simplicidade com que os usuários podem transferir dinheiro para qualquer lugar. A quantia que foi lavada por meio de trocas de criptoativos em 2020 foi de US\$ 2,3

bilhões²²⁶. Políticas eficazes de AML têm dois efeitos significativos: primeiro, aumentam o perigo e diminuem a lucratividade da lavagem de dinheiro e, segundo, abrem novas portas investigativas e legais para crimes financeiros.

A legislação focada em AML conhecida como regra de viagem criptográfica exige que os VASPs²²⁷ enviem, recebam e revisem informações pessoais e da empresa sempre que auxiliarem em transações de criptoativos acima de um limite específico de valor. Essa barreira é de US\$ 3.000 dólares nos Estados Unidos, mas na União Europeia é de € 0 euros conforme decidido pelos formuladores de políticas²²⁸. Em outras palavras, independentemente do valor de uma transação, as empresas de criptoativos que operam sob uma licença da UE são obrigadas a coletar informações sobre o remetente e o destinatário de cada transação.

Portanto, no que tange criptoativos, a frase conheça seu cliente (KYC) deve ser aplicada, pois refere-se a um conjunto de medidas de verificação de identificação exigidas por lei para fornecedores de serviços de ativos virtuais (VASPs). No caso de endereços de criptoativos pseudônimos ou até anônimos (Dash, Zcash, and Monero²²⁹) estarem vinculados ao crime, os processos KYC são cruciais porque permitem que os investigadores criminais vinculem os endereços a pessoas e lugares reais.

Os padrões KYC são menos uniformes no setor de criptoativos. A maioria das exchanges de ativos digitais exige que os novos usuários forneçam seus nomes completos, documento de identidade emitido pelo seu país e endereço,

²²⁶ REUTERS. **Cryptocurrency and anti-money laundering enforcement.** Disponível em: <<https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26>> acesso em 01/12/2022.

²²⁷ Virtual asset service providers. Um VASP é uma empresa que se envolve em uma ou mais das seguintes atividades, conforme definido pelo GAFI: troca de ativos virtuais (VAs) e moeda fiduciária; trocas de um ou mais tipos de ativos virtuais (VAs);

²²⁸ CONSILIUM. **Digital finance: agreement reached on European crypto-assets regulation (MiCA).** Disponível em: <<https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>>, acesso em 03/12/2022.

²²⁹ Existem mais de 70 tokens de criptomoeda anônimos, mas esses três estão no topo da lista das maiores criptomoedas de privacidade.

mas isso varia dependendo da localização da exchange e dos serviços que ela oferece.

Em junho de 2022, o GAFI²³⁰ reafirmou que, dependendo das atividades em que se envolvem, os mercados NFT, protocolos DeFi e fornecedores de *stablecoin* devem ser obrigados a realizar processos de KYC. Destacando²³¹:

In FATF consultations to date, several jurisdictions indicated they are addressing this issue by requiring VASPs to use blockchain analytic services to mitigate some of the ML/TF risks of unhosted wallets. Nevertheless, such jurisdictions recognise limitations in this approach. Given the ability to use unhosted wallets for financial activity, including to conduct peer-to-peer transactions, FATF will continue to monitor and discuss how countries are approaching transactions with unhosted wallets, as well as other key elements of the FATF Standards.

[...]

The FATF Standards outline the types of information that VASPs are required to send/receive for the Travel Rule. Beyond these requirements, around one fifth of jurisdictions (around 20 out of 98) indicated that they plan to require additional information to assist in VASPs detecting relevant ML/TF risks, and to meet broader AML/CFT requirements such as targeted financial sanctions. Most frequently, this includes: the purpose of the VA transfer, source of VA funds, and residential addresses of the beneficiary.

Devido ao crescimento exponencial do uso de criptoativos, as empresas que mercantilizam esses recursos precisam implementar procedimentos de conformidade KYC para evitar comportamentos ilegais. Os métodos mais

²³⁰ FATF. **Targeted update on Implementation of the Fatf standards on virtual Assets and virtual asset Service providers.** Disponível em: <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf>>, acesso em 03/12/2022.

²³¹ FATF. **Targeted update on Implementation of the Fatf standards on virtual Assets and virtual asset Service providers.** Disponível em: <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf>>, acesso em 03/12/2022. pp. 15-16.

eficazes para atingir esse objetivo são verificação de identidade, avaliação de risco e monitoramento contínuo.

Além disso, as empresas intermediadoras podem aumentar sua credibilidade com clientes e autoridades sem prejudicar seus resultados ao implementar novos requisitos de KYC. Nessa toada, uma *exchange* de criptoativos chamada Binance descobriu que a maioria dos indivíduos²³² - 96%, 97% dos usuários – aceitaria passar pelo sistema de verificação interno da corretora. Essa ligeira diminuição nos registros de cliente (3-4% que não aceitariam tal conduta) é um pequeno preço a pagar pela capacidade de funcionar em centenas de ambientes regulatórios, fornecer serviços a milhões de clientes e impedir todo tipo de atividade ilegal.

A devida diligência do cliente ou Customer due diligence, é reconhecida como uma das principais estratégias de combate à lavagem de dinheiro no espaço dos criptoativos. A empresa que medeia operações deve verificar a informação fornecida pelo potencial cliente ao longo do processo de identificação para avaliar o indivíduo que se faz passar por potencial cliente ou seja, conhecer a identidade e documentos comprobativos e principalmente a origem dos fundos.

As organizações financeiras e regulatórias estão cientes dessas preocupações e tentam implementar políticas que reduzirão o risco e promoverão a conformidade no mercado de criptoativos em constante expansão. As instituições financeiras, por exemplo, podem seguir as recomendações do Grupo de Ação Financeira (GAFI) e continuar a cumprir as regras mais recentes sem necessidade de aguardar o marco legislativo.

Repisa-se que a fim de identificar possíveis riscos que possam resultar em violações de lavagem de dinheiro e implementar penalidades conforme

²³² BLOOMBERG. **Binance CEO Advocates for Fundamental Crypto Rights**. Disponível em: <<https://www.bloomberg.com/news/articles/2021-11-16/binance-ceo-cz-zhao-advocates-for-fundamental-crypto-rights>>, acesso em 01/12/2022.

necessário, os governos nacionais estão colaborando com os reguladores como por exemplo o projeto de lei 4.401/21²³³, aprovado pelo plenário.

Muito embora a tecnologia Blockchain sustente as transações de ativos de criptomoeda, o status do Blockchain como um livro-razão imutável - um registro que não pode ser alterado - é um dos principais fatores que influenciam a segurança nas transações de criptoativos. Cada bloco contém registros de cadeias de transações completas que podem ser comparadas com os registros de outros blocos para encontrar anormalidades. Isso, teoricamente, indica que todos os dados no blockchain são confiáveis e corretos.

Este livro-razão imutável acompanha os nomes das carteiras de criptomoedas que são a fonte de cada transação. Se uma transação ilegal puder ser vinculada a uma carteira, o proprietário dessa carteira poderá ser encontrado e a conduta ilegal poderá ser evitada por meio de ação legal.

Diferentes tecnologias de blockchain fornecem detecção automática de fraude AML, permitindo o desenvolvimento de regras que impediriam a implementação de transações questionáveis, bloqueando-as ou sinalizando-as. No futuro, para que existam instituições financeiras e empresas de criptoativos, os governos terão que especificar que esses tipos de restrições são necessários.

Outra forma eficiente de prevenir a lavagem de dinheiro é utilizar provedores de serviços de análise Blockchain. Empresas como a Elliptic, Chainalysis e Ciphertrace podem ajudar empresas de criptoativos, Autoridades Policiais e instituições financeiras a rastrear transações no blockchain, analisá-las, detectar casos de atividades ilegais como lavagem de dinheiro e alertar os usuários sobre quaisquer perigos. É com o uso de análise de transações na blockchain que

²³³ Dispõe sobre a prestadora de serviços de ativos virtuais; e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 7.492, de 16 de junho de 1986, e 9.613, de 3 de março de 1998, para incluir a prestadora de serviços de ativos virtuais no rol de instituições sujeitas às suas disposições. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=9052734&ts=1670001123434&disposition=inline>>, acesso em 03/12/2022.

instituições financeiras e empresas que intermediam operações digitais podem garantir que estão cumprindo as normas e leis AML.

De acordo com FALCÃO e MORAIS²³⁴ como qualquer outro setor econômico, os provedores de serviços de criptoativos exigem regulamentação adequada para promover e proteger os investidores, principalmente os institucionais, que têm medo de assumir riscos maiores. Nesse sentido, é imprescindível uma legislação adequada ao setor, principalmente no concernente à construção de medidas de integridade e proteção ao consumidor, a fim de coibir e prevenir fraudes e lavagem de dinheiro relacionadas a criptomoedas. Nesse sentido, o projeto de lei 4.401/21 no art. 2, assentou ser obrigatório para todas as prestadoras de serviço de ativos virtuais prévia autorização de órgão específico. Por lógica, o órgão que será criado ou delegado atenderá as orientações do GAFI e implementará obrigações aos prestadores de serviços com cruzamento de informações e registros pessoais de cada cliente, como ocorre no sistema bancário.

Além disso, o projeto de lei inova ao criar o art. 171-A do Código Penal, ao tipificar a conduta de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros.

Em pese o projeto de lei supracitado não esteja vigorando, vê-se que o Brasil avança no combate a lavagem de dinheiro e uso ilícito dos criptoativos. A criação do marco legal concomitante com o Parecer nº 40 da CVM atrai responsabilidade ao governo e segurança ao consumidor/investidor.

As políticas de prevenção a lavagem de dinheiro com criptoativos são fundamentais para difundir esse novo mercado e possibilitar a exploração saudável. Contudo, considerando o conceito do criptoativo e que sua criação se originou como fruto de afastamento da intervenção estatal, deve-se levar em consideração que qualquer política anti-lavagem implementada pode ser paliativa e momentânea. A demora estatal em dismantelar novos recursos criminosos acarreta prejuízo

²³⁴ MORAIS, Fábio Luiz de. FALCÃO, Rondinelli Melo Alcântara. **A regulação de criptomoedas como instrumento de prevenção à lavagem de dinheiro.** Cadernos Técnicos da CGU, v. 3 (2022): Coletânea de Artigos Correccionais, novembro de 2022. Disponível em: <https://revista.cgu.gov.br/Cadernos_CGU/article/view/607/337>, acesso em 02/12/2022, p. 20.

social e guia mercados financeiros a ruínas. Nesse sentido, é importante que a regulamentação seja aplicada, porém a fiscalização e investigação será fundamental para barrar novos empreendimentos criminosos. Políticas de compartilhamento de informações transnacionais, análise da cadeia de custódia da blockchain, identificação de carteiras criminosas e implementação de KYC são os meios mais efetivos para prevenir e combater a lavagem de dinheiro com criptoativos.

O compliance é uma faceta essencial na indústria de criptomoedas, porque serve para garantir que as empresas que intermediam negociações funcionem dentro de estruturas legais e governamentais, além de diminuir o risco de atividade fraudulenta ou ilícita. As empresas que intermediam negociações em criptoativo, nos Estados Unidos, estão sujeitas a uma variedade de regras federais e estaduais, incluindo a legislação de lavagem anti-dinheiro (AML) e conhecimento de seu cliente (KYC). Essas regras obrigam as empresas a validar as identidades de seus clientes, assistir às transações para atividades suspeitas e divulgar qualquer atividade suspeita à aplicação da lei.

Para garantir a conformidade com essas leis, as corretoras geralmente implementam programas de conformidade que incluem avaliações de riscos, políticas e procedimentos, treinamento de funcionários e sistemas de rastreamento. Algumas empresas também empregam especialistas em conformidade para supervisionar seus esforços de compliance.

Outros requisitos, como privacidade de dados e regulamentos de proteção ao cliente, devem ser atendidos por empresas de criptografia, além da regulamentação governamental. Para funcionar em determinados estados ou regiões, eles também podem precisar adquirir licenças ou registros.

O compliance do setor de criptomoedas ainda se desenvolvendo e os reguladores estão aprimorando regulamentações. Como resultado, as empresas que negociam ativos digitais devem acompanhar as alterações regulatórias e modificar seus esforços de conformidade adequadamente.

Dito isto, conclui-se o estudo engendrado e passa-se as considerações finais que articulará a instrumentalização dos criptoativos em práticas criminosas, em especial a lavagem de dinheiro e evasão de divisas. Além disso, será ventilado, em inteligência a hipótese levantada, a ocorrência das fases da lavagem de dinheiro e a dissemelhança com moeda fiduciária. Outrora, concluir-se-á se a conduta de evasão de divisas é caracterizada pela aquisição e transmissão de criptoativos em comparação aos julgados nacionais. Por fim, será correlacionado a evolução legislativa nacional e a aplicabilidade da lei anti-lavagem americana, com exemplos de operações e julgados que foram amealhados no estudo.

CONSIDERAÇÕES FINAIS

A lavagem de dinheiro com criptoativos é um problema jurídico relevante, por permitir que transações financeiras sejam realizadas com um certo grau de anonimato e segurança sem precedentes. Identificou-se na pesquisa que há moedas digitais utilizando do anonimato absoluto com serviços de mixagem para ocultar de forma inigualável a fonte e pessoa/instituição que permutou aquele ativo. Com efeito, as autoridades encontram dificuldades em identificar e rastrear a origem e destino dos recursos, facilitando a lavagem de dinheiro e a prática de outras atividades criminosas.

Por outro lado, a evasão de divisas, crime que afeta diretamente os cofres públicos, independe da participação social, pois o delito com criptoativos ocorre quando um indivíduo ou empresa transfere recursos financeiros para o exterior utilizando criptomoedas com o intuito de evitar o pagamento de impostos ou outras obrigações fiscais. Esse tipo de evasão é possível porque as transações de criptoativos são descentralizadas e não estão sujeitas à supervisão dos órgãos reguladores, obstando a identificação e rastreabilidade das operações realizadas. Além disso, as criptomoedas podem ser convertidas em outras moedas estrangeiras com facilidade, favorecendo a transferência de recursos para o exterior. A evasão de divisas, não obstante tenha afeto diretamente na arrecadação fiscal, é, contudo, um risco sistêmico mercadológico, uma vez que a fuga de capital de um país pode diretamente afetar o risco de bancarrota.

Evidenciou-se que, para combater a lavagem de dinheiro e evasão de divisas com criptoativos, é necessário adotar medidas regulatórias rigorosas e tecnologias avançadas de análise de dados e inteligência artificial para detectar atividades suspeitas. Além disso, é crucial conscientizar o público sobre os riscos e obrigações legais relacionadas às criptomoedas e promover uma abordagem colaborativa entre autoridades, empresas de criptoativos e investidores para garantir a integridade do sistema financeiro global e uma economia mais justa e equilibrada.

Conforme disposto no capítulo 1, a lavagem de dinheiro é uma prática antiga, que remonta à Idade Média, intensificada no século XX, com o aumento do crime organizado e a globalização da economia. Com o avanço da tecnologia, a lavagem de dinheiro se tornou mais sofisticada e difícil detecção. O uso de criptoativos converteu-se em uma nova ferramenta para a evasão de divisas e a lavagem de dinheiro, já que essas moedas digitais permitem transações sem a necessidade de intermediários e rastros criptografados não identificáveis. Os referidos crimes são graves, afetando a economia e a sociedade como um todo. Para combatê-los, o direito penal econômico tem evoluído constantemente, adaptando-se aos novos desafios impostos pelo avanço tecnológico e pelas mudanças no cenário econômico. A regulamentação de criptoativos, como ocorreu recentemente no Brasil com a Lei n. 14.478/22, é um exemplo de medida tomada para combater a lavagem de dinheiro e a evasão de divisas.

No capítulo 2 identificou-se que a tecnologia blockchain é uma inovação descentralizada, a qual permite a realização de transações financeiras seguras e transparentes, sem a necessidade de intermediários, como bancos. O surgimento dos criptoativos é uma das principais aplicações da tecnologia blockchain. No entanto, a sua popularização também ocasionou novos desafios para a segurança financeira, principalmente em relação aos crimes virtuais. A utilização de criptoativos em delitos, como a lavagem de dinheiro e o financiamento de atividades ilícitas na *deep web*, vem aumentando significativamente. Ainda, apontou-se, que um total de US\$ 14 bilhões de dólares em atividades ilegais, incluindo *hacking*, lavagem de dinheiro e financiamento terrorista, foram envolvidos em 0,15% das transações conhecidas de criptomoedas em 2021, de acordo com a empresa de pesquisa blockchain Chainalysis.

Em 2022, endereços ilícitos enviaram quase US\$ 23,8 bilhões de dólares²³⁵ em criptoativos; um aumento de 68,0% em relação a 2021. Como de costume, as principais exchanges receberam a maior quantidade de moedas ilegais, respondendo por pouco menos da metade de todos os fundos enviados de

²³⁵ Chainalysis. **Crypto Money Laundering: Four Exchange Deposit Addresses Received Over \$1 Billion in Illicit Funds in 2022**. Disponível em: <<https://blog.chainalysis.com/reports/crypto-money-laundering-2022>>, acesso em 05/03/2023.

endereços ilícitos. Isso é significativo, não apenas porque essas corretoras geralmente têm medidas de conformidade para relatar atividades suspeitas e tomar medidas contra os usuários em questão, mas também porque essas trocas são saídas fiduciárias, onde a criptomoeda ilícita pode ser convertida em dinheiro.

Neste contexto, explorou-se que o monitoramento policial é essencial na garantia da segurança e integridade do mercado de criptoativos, bem como no duelo aos crimes financeiros. Deste modo, o direito penal econômico revela-se importante na prevenção no combate aos crimes virtuais envolvendo criptoativos. Identificou-se que, em que pese a legislação necessite se adaptar às mudanças tecnológicas para garantir a efetividade do combate a esses crimes, o submundo criminal evolui vertiginosamente, implementando novas tecnologias de mixagem e escambo de moedas na *deep web* e *dark net*. Além disso, mostrou-se que o desaparecimento das barreiras estatais com o criptoativo traz novos desafios para a regulação desse mercado, pois é necessário encontrar um equilíbrio entre a inovação tecnológica e a segurança financeira, para que os criptoativos possam ser utilizados de forma legal e segura.

No capítulo 3 verificou-se que a intervenção do governo no mercado de criptoativos tem sido um tema hodiernamente debatido, especialmente no que tange à regulamentação e fiscalização. No Brasil, há ainda pouca clareza sobre o entendimento dos tribunais em relação aos criptoativos, embora algumas decisões recentes tenham indicado que esses ativos podem ser considerados como propriedade, sujeitos às mesmas regras do direito civil. Vislumbrou-se que por dois anos a discussão judicial se tratava de conflito de competência, pois a justiça federal entendia que a prática de crimes com criptoativos não era de afeto à sua responsabilidade. O tema ascendeu até as cortes superiores, fixando precedente de que a competência, em tese, é da justiça comum, acaso não haja crime antecedente de competência federal e/ou tenha incidência de crimes que englobam a esfera federal. Todavia, o Parecer de Orientação CVM 40, publicado pela Comissão de Valores Mobiliários em 2022 e que trata da oferta pública de criptoativos no Brasil, alterou significativamente o entendimento supracitado. O documento esclarece que a oferta de criptoativos pode ser considerada como pública de valores mobiliários, sujeita à regulamentação da CVM. Dessa forma, as

empresas que desejam realizar ofertas de criptoativos precisam se adequar às normas da autarquia, como a apresentação de informações claras, precisas e completas sobre o ativo, seus riscos e potenciais retornos, além de adotar medidas de segurança para proteger os investidores. O descumprimento de tais regulamentações atrai a incidência da Lei nº 7.492/1986, a qual define os crimes contra o sistema financeiro nacional, e dá outras providências, conseqüentemente provocando a atuação da justiça federal.

O Parecer de Orientação também reforça a importância da transparência e da proteção ao investidor no mercado de criptoativos, especialmente diante dos riscos envolvidos nesse tipo de investimento, como a volatilidade do preço, a falta de regulação e a possibilidade de fraudes e manipulação do mercado.

Em relação aos tribunais brasileiros, ainda há poucos precedentes sobre a regulação de criptoativos, mas é possível observar uma tendência de considerar esses ativos como valores mobiliários, sujeitos à regulamentação da CVM. Nos Estados Unidos, por sua vez, há mais jurisprudências sobre o tema, com diversos casos de regulamentação e punição de empresas que desrespeitaram as normas do mercado de criptoativos.

Destarte, a utilização de criptoativos na lavagem de dinheiro é uma preocupação crescente dos órgãos reguladores e das autoridades policiais. Por isso, o combate à lavagem de dinheiro com criptoativos tem se intensificado nos últimos anos, com a adoção de medidas de monitoramento e regulação do mercado de criptoativos, além de investigações e operações policiais para coibir o uso desses ativos em atividades ilícitas. Verificou-se que as orientações do GAFI (FATF) são parâmetros para os mercados nacionais.

Nos Estados Unidos, há um maior entendimento sobre os criptoativos, com diversos precedentes judiciais estabelecendo a sua natureza e o seu enquadramento legal. O combate à lavagem de dinheiro com criptoativos tem sido um dos principais argumentos para a intervenção do governo americano no mercado desses ativos, criando mecanismos de monitoramento e fiscalização com

o intuito de garantir a identificação de transações suspeitas e a prevenção de atividades ilícitas.

Em síntese, o clima regulatório para criptomoedas nos Estados Unidos ainda está evoluindo, e há uma discussão contínua sobre o grau adequado de regulamentação necessária para proteger os investidores e evitar atividades ilícitas sem sufocar a inovação. No entanto, a popularização dos criptoativos tem criado desafios no cumprimento de leis e atuação das autoridades, especialmente quanto ao financiamento de atividades criminosas na *deep web* e ao desaparecimento das barreiras estatais que outrora limitavam o fluxo de capitais. Como resultado, o debate sobre a intervenção do governo no mercado de criptoativos continua evoluindo, com a necessidade de encontrar o equilíbrio entre a inovação tecnológica e a proteção dos interesses públicos.

Assim sendo, resgatando às problemáticas de pesquisa propostas, buscou-se primeiramente identificar as fases que caracterizam a lavagem de dinheiro pelo criptoativo, por conseguinte tentou-se analisar se a conduta prevista no art. 22 da Lei nº 7.492/1986, denominada evasão de divisas, pode ser atribuída ao criptoativo. Por fim, na última problemática investigou-se a dissemelhança entre o ordenamento jurídico brasileiro e o americano, no que tange à prevenção e combate ao crime econômico, especialmente àquele praticado com ativos digitais.

Quanto a primeira problemática, concluiu-se que a lavagem de dinheiro com criptoativos ocorre e geralmente envolve três fases distintas, confirmando a hipótese formada, quais sejam:

A colocação (*placement*): nesta fase, o criminoso transfere o dinheiro ilícito para o mundo cripto através da compra de criptoativos, como Bitcoin, em plataformas de troca ou diretamente de outra pessoa. Essa transação inicial dos criptoativos ajuda a lavar o dinheiro sujo, por serem anônimos e facilmente movidos de um endereço para outro sem deixar um rastro claro.

Ocultação (*layering*): Na lavagem de dinheiro com criptoativos, a ocultação é uma etapa crítica do processo. Após a colocação, onde o dinheiro ilícito

é convertido em criptoativos, a ocultação visa dificultar a rastreabilidade desses recursos, tornando-os aparentemente legítimos.

Uma das maneiras mais comuns de ocultar os criptoativos é através de transações complexas e fragmentadas, conhecidas como *mixing* ou *tumbling*. Nesse processo, os criptoativos são transferidos entre múltiplas carteiras e endereços, misturando-os com outros ativos de origem legítima. Isso torna difícil seguir o rastro do dinheiro e identificar a origem dos criptoativos utilizados na lavagem de dinheiro.

Além disso, os criminosos podem utilizar serviços de anonimização, como redes de acesso à internet anônimas (como a dark web) ou serviços de carteiras de criptomoedas que não exigem identificação dos usuários, para ocultar a origem dos recursos.

Outra técnica utilizada é a criação de empresas de fachada ou contas falsas em plataformas de câmbio de criptoativos. Essas empresas fictícias são usadas para transferir e misturar os criptoativos em transações aparentemente legítimas, tornando mais difícil rastrear a verdadeira origem do dinheiro.

Além disso, a utilização de criptoativos em transações internacionais pode dificultar ainda mais a identificação da origem dos recursos, uma vez que as transações de criptoativos são geralmente rápidas e globais, sem a necessidade de intermediários, o que torna a rastreabilidade mais complexa.

Integração (*integration*): A fase de integração é a última etapa do processo de lavagem de dinheiro com criptoativos. Nessa fase, os criptoativos que foram previamente ocultados são reintroduzidos no sistema financeiro de forma aparentemente legítima, permitindo que os recursos ilícitos sejam utilizados sem levantar suspeitas.

Existem várias maneiras pelas quais os criminosos podem realizar a integração dos criptoativos na lavagem de dinheiro. Uma delas é a venda dos criptoativos em plataformas de troca de criptomoedas, onde eles podem ser convertidos em moedas tradicionais, como dólares ou euros, e transferidos para

contas bancárias ou outros ativos financeiros. Os criptoativos também podem ser utilizados para aquisição de bens e serviços, como imóveis, veículos, joias, entre outros, para dar uma aparência de legalidade aos recursos obtidos ilegalmente.

Outra técnica utilizada é a transferência dos criptoativos para outras contas de criptomoedas em jurisdições com regulamentações menos rigorosas ou para contas de terceiros, dificultando o rastreamento do dinheiro sujo.

Além disso, os criminosos podem utilizar as criptomoedas para investir em projetos legítimos, como startups ou ICOs (Ofertas Iniciais de Moedas), na tentativa de legitimar os recursos ilícitos e obter retornos financeiros aparentemente legítimos.

Essas fases não são necessariamente sequenciais, e podem ser executadas em várias ordens ou de maneiras distintas, dependendo do método escolhido pelo criminoso. Além disso, a característica do ativo virtual por si só permite que a lavagem de dinheiro seja perpetrada através de uma única fase pois, conforme descrito no presente trabalho, a simples mixagem de ativos virtuais esconde a origem, mistura os ativos com diversos outros e reintegra de forma lícita. Identificou-se que, conforme alhures mencionado, o monitoramento cuidadoso das transações de criptoativos e a implementação de regulamentações adequadas são essenciais para combater a lavagem de dinheiro com criptoativos.

A segunda problemática foi parcialmente confirmada, pois é complexa e depende de variáveis do caso concreto, entretanto alcançou-se com a pesquisa que, no âmbito da norma responsável pelo controle das divisas situadas no exterior, qualquer tipo de investimento no sistema financeiro estrangeiro, como ações, fundos ou cotas de fundos de investimentos, incluindo previdência privada, deve ser considerado como um depósito. Essa interpretação é baseada na leitura sistemática e teleológica da lei, visando tutelar o controle das divisas no exterior, abrangendo todas as formas de aplicações financeiras. No que se refere aos crimes como sonegação fiscal, evasão de divisas (na modalidade prevista no caput do art. 22 da Lei nº 7.492/1986) e lavagem de dinheiro, é possível que o uso do criptoativo seja considerado ilícito, desde que haja comprovação dos requisitos da atividade criminosa. Essa análise deve ser criteriosa e realizada caso a caso. Por outro lado,

enquanto não houver regulamentação por parte do Banco Central do Brasil (BACEN) ou da Comissão de Valores Mobiliários (CVM) - a orientação 40 da CVM não faz menção ao crime de evasão de divisas - não é possível enquadrar a evasão de divisas propriamente dita (primeira parte do § único do art. 22 da LSN) ou a modalidade de evasão imprópria ou depósito de evasão (manutenção de depósitos no exterior não declarados ao BACEN, última parte do art. 22 da Lei nº 7.492/1986) quando a transação financeira envolver a compra e/ou manutenção de criptoativos em contas digitais, que estejam em desacordo com as normas estabelecidas pela referida agência governamental.

Por outro lado, em última análise, se o criptoativo for usado como meio para converter o real em moeda estrangeira sem autorização, com o objetivo de promover a evasão de divisas do país, pode, em teoria, constituir o crime de evasão de divisas previsto no artigo 22, caput, da Lei nº 7.492/1986. Ainda, há de se considerar a equiparação, realizada pela orientação 40 da CVM de criptoativos a títulos e valores mobiliários, gerando consequências penais, sem a sanção de lei normatizando a problemática, teorizando possibilidade do encaixe da norma.

A terceira e última problemática explorou as dissemelhanças do ordenamento jurídico brasileiro e norte americano. A hipótese restou confirmada, conforme descrito, no Brasil, foi sancionada em 2022 uma lei que regulamenta o mercado de criptoativos, incluindo a definição de ativos virtuais, prestadoras e o crime de fraude com utilização de criptoativos, além de estabelecer penas para as violações. O texto (Lei n.º 14.478/2022) foi publicado em 22 de dezembro de 2022 e entrará em vigor no prazo de 180 dias.

Essa recente legislação impõe obrigações específicas para transparência e divulgação de informações, almejando prevenir a lavagem de dinheiro e outros crimes relacionados. É importante ressaltar que a lei inclui penalidades para aqueles que descumprirem as suas disposições, tais como multas e sanções penais. Atualmente, o Brasil apresenta uma das maiores taxas de adoção de criptoativos, tanto por pessoas físicas como por empresas, as quais têm aumentado a inclusão destes ativos em suas demonstrações financeiras. A lei atribui competência ao Banco Central, prevendo que as instituições autorizadas a

funcionar pelo Banco Central do Brasil poderão prestar exclusivamente o serviço de ativos virtuais ou cumulá-lo com outras atividades, na forma da regulamentação a ser editada por órgão ou entidade da Administração Pública federal indicada em ato do Poder Executivo federal. Todavia, a referida Lei desacautela-se ao deixar de fixar o competente órgão federal disciplinará o funcionamento e a supervisão da prestadora de serviços de ativos virtuais, concedendo discricionariedade ao Poder Executivo Fiscal. Os precedentes nacionais, até o ano de 2022, debatiam conceitos jurídicos e as propriedades do ativo digital, trazendo incertezas e insegurança jurídica ao mercado de criptoativos. Observa-se, do estudo elaborado, que a maioria dos crimes contra a economia popular poderiam ser evitados se a resposta estatal estivesse em par com a evolução tecnológica. Com efeito, para a lei, 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, excluindo-se moeda eletrônica nos termos da Lei nº 12.865, de 9 de outubro de 2013.

Por outro prisma, diferentemente do Brasil, a legislação e regulamentação norte americana é diretamente atribuída aos órgãos regulamentadores.

Nos Estados Unidos, a regulamentação de criptomoedas é um campo jurídico complicado e em constante evolução, abrangendo inúmeras entidades federais e locais.

A *Securities and Exchange Commission* (SEC), a *Commodity Futures Trading Commission* (CFTC) e o *Internal Revenue Service* (IRS) são as principais agências reguladoras governamentais envolvidas em criptomoedas. A SEC declarou que certas criptomoedas, como aquelas oferecidas em ofertas iniciais de moedas (ICOs), podem ser consideradas valores mobiliários e suscetíveis às regras federais de valores mobiliários.

A *Commodity Futures Trading Commission* (CFTC) tem autoridade sobre transações de derivativos, incluindo aquelas baseadas em criptomoedas, e adotou medidas contragolpes fraudulentos no que diz respeito a estes ativos. Por

razões fiscais, o IRS considera a criptomoeda como propriedade, significando que os ganhos das negociações estão sujeitos ao imposto sobre ganhos de capital.

A regulamentação da criptomoeda no nível estadual difere, com alguns estados aprovando legislação para supervisionar as trocas de criptomoedas e outros tendo uma abordagem mais permissiva. Nova York tem sido especialmente ativa na regulamentação de criptomoedas por meio de seu programa BitLicense, o qual exige a aquisição de licença pelas empresas que desejem operar no mercado de criptomoedas do estado.

Sob outra perspectiva, a evasão de divisas nos Estados Unidos ocorre se as transações envolverem mais de US\$ 10.000 (dez mil dólares), pois o contribuinte é responsável por relatar todas as transferências ao Internal Revenue Service (IRS) que ultrapassem o valor citado. Não fazer isso pode levar a multas e repercussões criminais. A lei que regulamenta determinado comando legal é a Foreign Account Tax Compliance Act (FATCA). De acordo com o IRS, o FATCA, é uma lei tributária que exige que instituições financeiras estrangeiras, bem como entidades financeiras não estrangeiras, reportem todas as contas e ativos estrangeiros de cidadãos americanos. Nesse sentido, instituições financeiras e provedores de transferência de dinheiro são obrigados a relatar transferências internacionais que excedam US\$ 10.000. Outrora, o IRS obriga o contribuinte a relatar renda, ganho ou perda de todas as transações tributáveis envolvendo moeda virtual nas declarações de imposto de renda federal para o ano tributável da transação, independentemente do valor.

Em vista disso, conclui-se que o mercado de criptoativos no Brasil possui grande relevância jurídica, e que, além das intensas discussões acerca da competência, tipificação e normatização, é crucial levar em consideração os danos financeiros e econômicos decorrentes da inação legislativa, acobertada pela Lei n.º 14.478/2022, bem como o impacto sistêmico acometido ao mercado financeiro.

Por fim, é importante salientar que o tema não foi totalmente explorado, sendo possível aperfeiçoar novos estudos sobre o assunto e monitorar as mudanças legislativas que ocorrerão em decorrência da recente legislação. Além disso, é necessário aguardar o posicionamento dos tribunais e órgãos

superiores, concernente à interpretação da Lei n.º 14.478/2022, concomitantemente com o Parecer de Orientação nº 40 da CVM.

REFERÊNCIA DAS FONTES CITADAS

ACADEMY. **What is a Utility Token?** Disponível em: <<https://academy.bit2me.com/en/que-es-utility-token/>>, acesso em 28/05/2023.

FORDHAM. **Silk Road: The Dark Side of Cryptocurrency.** Disponível em: <<https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/>>, acesso em 20/07/2022.

AMARAL, Thiago Bottino. **Direito Penal Econômico.** FGV, 2015. Disponível em: <https://diretorio.fgv.br/sites/diretorio.fgv.br/files/u100/direito_penal_economico_2015-1.pdf>, acesso em 20/12/2021.

ANOREG. **Comprou imóvel com criptomoedas? Senado Federal analisa projeto de lei sobre questão.** Disponível em: <<https://www.anoregpr.org.br/comprou-imovel-com-criptomoedas-senado-federal-analisa-projeto-de-lei-sobre-questao/>>, acesso em 03/08/2022.

ANTONOPOULOS, Andreas. **Mastering Bitcoin - Unlocking Digital Currencies.** Editora: Sebastopol: O'Reilly, 2015.

ARRABAL, Alejandro Knaesel. ENGELMANN, Wilson. MELO, Milena Petters. **Liberdade e anonimato no contexto da cibercultura.** Revista De Direitos E Garantias Fundamentais, 18(2): 2018.

BACH, Fábio André Guarangi; SOBRINHO, Fernando Martins Maria. **Direito penal econômico administrativização do direito penal, criminal compliance e outros temas contemporâneos.** Londrina, PR: Thoth, 2017.

BATLOUNI, Marcelo. **Crime de lavagem de dinheiro.** Editora Atlas: 2018, 4ª edição.

BBC. **Dark web drug dealer jailed over cryptocurrency millions.** Disponível em: <<https://www.bbc.com/news/uk-england-leeds-61809398>>, acesso em 02/08/2022.

BILTON, Nick. **American Kingpin: Catching the Billion-Dollar Baron of the Dark Web.** Ebury Publishing; 2ª edição, 2018.

BLEEPINGCOMPUTER. **Russian Authorities Announce Takedown of RAMP Dark Web Marketplace.** Disponível em: <<https://www.bleepingcomputer.com/news/security/russian-authorities-announce-takedown-of-ramp-dark-web-marketplace/>>, acesso em 03/08/2022.

BLOOMBERG. **'Hundreds' of Crypto Cases Coming, IRS Criminal Chief Says.** Disponível em: <<https://news.bloombergtax.com/crypto/hundreds-of-crypto-cases-coming-irs-criminal-chief-says>>, acesso em 03/12/2022.

BLOOMBERG. **Binance CEO Advocates for Fundamental Crypto Rights.** Disponível em: <<https://www.bloomberg.com/news/articles/2021-11-16/binance-ceo-cz-zhao-advocates-for-fundamental-crypto-rights>>, acesso em 01/12/2022.

BONFIM, Márcia Monassi Mougenot; BONFIM, Edilson Mougenot. **Lavagem de Dinheiro.** 2. Ed. Malheiros Editores, 2005.

BONGER, Willem. **Criminalité et conditions économiques.** University of Michigan Library: 1905.

BRASIL. Decreto-Lei nº 2.848/1940, de 7 de dezembro de 1940. **Código Penal.** Brasília, DF: Diário Oficial da União, 1940 e retificado em 3.1.1941.

BRASIL. FAZENDA. **Fases da lavagem de dinheiro.** Disponível em: <<https://www.fazenda.gov.br/assuntos/prevencao-lavagem-dinheiro#fases-da-lavagem-de-dinheiro>>, acesso em 20/09/2022.

BRASIL. FAZENDA. **Prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo.** Disponível em: <<http://www.fazenda.gov.br/assuntos/prevencao-lavagem-dinheiro>>, acesso em 17/12/2021.

BRASIL. Lei 1.521/1951, de 26 de dezembro de 1951. **Altera dispositivos da legislação vigente sobre crimes contra a economia popular.** Brasília, DF: Diário Oficial da União, 1951.

BRASIL. Lei nº 12.683/2012, de 9 de julho de 2012. **Altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro.** Brasília, DF: Diário Oficial da União, 2012.

BRASIL. Lei nº 13.974/2020, de 7 de janeiro de 2020. **Dispõe sobre o Conselho de Controle de Atividades Financeiras (Coaf), de que trata o art. 14 da Lei nº 9.613, de 3 de março de 1998.** Brasília, DF: Diário Oficial da União, 2020.

BRASIL. Lei nº 14.478/2022, 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.** Brasília, DF: Diário Oficial da União, 2022.

BRASIL. Lei nº 4.595/1964, de 31 de dezembro de 1964. **Dispõe sobre a Política e as Instituições Monetárias, Bancárias e Creditícias, Cria o Conselho Monetário Nacional e dá outras providências.** Brasília, DF: Diário Oficial da União, 1964.

BRASIL. Lei nº 7.492/1986, de 16 de junho de 1986. **Define os crimes contra o sistema financeiro nacional, e dá outras providências.** Brasília, DF: Diário Oficial da União, 1986.

BRASIL. Lei nº 9.613/1998, de 3 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.** Brasília, DF: Diário Oficial da União, 1998.

BRASIL. Superior Tribunal de Justiça. **Conflito negativo de competência nº 161.123/SP.** Relator Ministro Sebastião Reis Júnior, Terceira Seção, julgado em 28/11/2018, publicado no DJe em 5/12/2018.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus n. 699.416.** Relator Ministro Antonio Saldanha Palheiro, Publicado no DJe em 02/12/2021.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus n. 161.635/DF.** Relator Ministro Ribeiro Dantas, Quinta Turma, julgado em 23/8/2022, publicado no DJe em 30/8/2022.

BRASIL. Tribunal de Justiça do Estado de São Paulo. **Habeas Corpus nº 2216677-24.2022.2022.8.26.0000**, Relator: Mens de Mello, julgado em 26/09/2022 pela 7ª Câmara de Direito Criminal.

BRASIL. Tribunal Regional Federal (4. Região). **Habeas Corpus nº 5044182-02.2021.4.04.0000.** Impetrante: Marcelo Almeida e Adrielle Santos em favor de Claudio Jose de Oliveira. Impetrado: Juízo da 23ª Vara Federal de Curitiba. Oitava Turma, Relator: Carlos Eduardo Thompson Flores Lenz. Porto Alegre, 24 novembro de 2021.

BRASIL. Tribunal Regional Federal (4. Região). **Habeas Corpus nº 5017581-56.2021.4.04.0000.** Impetrante: Alexandre Collares, Pedro Machado de Almeida Castro, Octavio Orzari, Vinícius André de Sousa e Bruno Henrique de Moura em favor de Angelo Ventura da Silva. Impetrado: Juízo Federal da 7ª Vara Federal de Porto Alegre/RS. Sétima Turma, Relatora Bianca Georgia Cruz Arenhart. Porto Alegre, 17 de agosto de 2021.

BURNISKE, Chris; TATAR, Jack. **Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond.** Publisher: McGraw-Hill Education; 1st Edition, 2017.

CALLEGARI, André Luís. Direito penal econômico e lavagem de dinheiro: aspectos criminológicos. Porto Alegre: Livraria do Advogado, 2003.

CALLEGARI, André Luís; WEBER, Ariel Barazzetti. **Lavagem de dinheiro.** São Paulo: Atlas, 2014.

CHAINANALYSIS. **The 2022 Crypto Crime Report.** disponível em: <<https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>>, acesso em 31/07/2022.

CHRISTIN, Nicolas. **Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace.** Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/2488388.2488408>>, publicado em 2013, acesso em 05/03/2023.

CLICRBS, Gaucha Zh. **Caso Unick: Polícia Federal conclui inquérito sobre esquema que teria lesado clientes da empresa em R\$ 12 bilhões.** Disponível em: <<https://gauchazh.clicrbs.com.br/seguranca/noticia/2021/05/caso-unick-policia-federal-conclui-inquerito-sobre-esquema-que-teria-lesado-clientes-da-empresa-em-r-12-bilhoes-ckoltpoya006w01807t4pcr26.html>> acesso em 22/06/2022.

COINTELEGRAPH. **COAF investiga 674 mil pessoas por lavagem de dinheiro e 4 mil casos envolvem Bitcoin.** Disponível em: <<https://cointelegraph.com.br/news/coaf-investiga-674-mil-pessoas-por-lavagem-de-dinheiro-e-casos-tambem-envolvem-bitcoin>>, acesso em 23/06/2022.

COINTELEGRAPH. **Ministério Público de Santa Catarina cria o CyberGaeco para combater crimes que envolvam bitcoin e criptomoedas.** Disponível em: <<https://cointelegraph.com.br/news/public-ministry-of-santa-catarina-creates-cybergaeco-to-fight-crimes-involving-bitcoin-and-cryptocurrencies>>, acesso em 03/08/2022.

CONSILIUM. **Digital finance: agreement reached on European crypto-assets regulation (MiCA).** Disponível em: <<https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>>, acesso em 03/12/2022.

CORNELL. **18 U.S. Code § 1956 - Laundering of monetary instruments.** Disponível em: <<https://www.law.cornell.edu/uscode/text/18/1956>>, acesso 10/10/2022.

CVM. **Parecer de Orientação CVM 40.** Disponível em: <<https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/pareceres-orientacao/anexos/Pare040.pdf>>, acesso em 05/03/2022.

DINORO, Rinatis. **The Truth About Liberty Reserve.** Epub Kindle Edition.

DUPUIS, D. GLEASON, K. **Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic.** Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3681297>, acesso em 03/08/2022.

ELROM, Elad. **The Blockchain Developer.** Publisher: Apress; 1st ed. Edition, 2019.

ENGELMANN, Wilson. MELO, Milena Petters. **Liberdade e anonimato no contexto da cibercultura**. Revista De Direitos E Garantias Fundamentais, 18(2): 2018.

ESTELLITA, Heloisa. **Criptomoedas e lavagem de dinheiro**. Revista Direito GV [online]. 2020, v. 16, n. 1 [Acessado 1 Dezembro 2022], e1955. Disponível em: <<https://doi.org/10.1590/2317-6172201955>>. Epub 27 Abr 2020. ISSN 2317-6172. <https://doi.org/10.1590/2317-6172201955>.

EUROPOL. **Cryptocurrencies tracing the evolution of criminal finances**. Disponível em: <<https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf>>, acesso em 31/07/2022.

EXAME. **Polícia brasileira recebe treinamento do FBI sobre crimes com criptomoedas**. Disponível em: <<https://exame.com/future-of-money/policia-brasileira-recebe-treinamento-do-fbi-sobre-crimes-com-criptomoedas/>>, acesso em 23/06/2022.

FATF. **Guidance for a risk-based approach: virtual currencies**. Disponível em <<https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>>, acesso em 10/07/2022.

FATF. **Operational Issues Financial Investigations Guidance**. Disponível em: <https://www.fatf-gafi.org/media/fatf/documents/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf>, acesso em 10/09/2022.

FATF. **Targeted update on Implementation of the Fatf standards on virtual Assets and virtual asset Service providers**. Disponível em: <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf>>, acesso em 03/12/2022.

FATF. **Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing**. Disponível em: <<https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>>, acesso em 03/08/2022.

FATF. **Virtual Currencies: Key Definitions and Potential AML/CFT Risks**. Disponível em <<https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html>>, acesso em 23/06/2022.

FATF/GAFI. Padrões internacionais de combate à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação, as recomendações do GAFI. Disponível em: <<http://www.fazenda.gov.br/orgaos/coaf/arquivos/as-recomendacoes-gafi>>, acesso em 03/12/2021.

FIGUEIREDO, Leonardo Vizeu. **Lições de direito econômico**. Rio de Janeiro: Forense, 2017. ed. 7.

FORBES. **A short history of bitcoin an cryptocurrency everyone should read**. Disponível em: <<https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#2341a4773f27>>, acesso em 03/09/2021.

FORBES. **The False Narrative of Bitcoin's Role in Illicit Activity**. Disponível em: <<https://www.forbes.com/sites/haileylennon/2021/01/19/the-false-narrative-of-bitcoins-role-in-illicit-activity/?sh=4c682ef93432>>, acesso em 03/08/2022.

FORTUNE. **How to Steal \$500 Million in Cryptocurrency**. Disponível em: <<https://fortune.com/2018/01/31/coincheck-hack-how/>>, acesso em 03/08/2022.

FORTUNE. **What the media gets wrong in its persistent crypto criticism**. Disponível em: <<https://fortune.com/2022/07/06/media-crypto-criticism-downturn-bear-markets-tech-defi-miller-whitehouse-levine/>>, acesso em 03/08/2022.

FSB. **Crypto-assets and Global "Stablecoins"**. Disponível em <<https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/crypto-assets-and-global-stablecoins/>>, acesso em 07/11/2022.

FSB. **FSB proposes framework for the international regulation of crypto-asset activities**. Disponível em <<https://www.fsb.org/2022/10/fsb-proposes-framework-for-the-international-regulation-of-crypto-asset-activities/>>, acesso em 07/11/2022.

FSB. Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements: Consultative report. Disponível em < <https://www.fsb.org/wp-content/uploads/P111022-4.pdf>>, acesso em 03/12/2022.

GAO, U.S. Government Accountability Office. **Trafficking: Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking**. Disponível em: <<https://www.gao.gov/products/gao-22-105101>>, acesso em 01/06/2022.

GAO. **As Virtual Currency Use in Human and Drug Trafficking Increases, So Do the Challenges for Federal Law Enforcement**. Disponível em: <<https://www.gao.gov/blog/virtual-currency-use-human-and-drug-trafficking-increases-so-do-challenges-federal-law-enforcement>>, acesso em 02/08/2022.

GAWKER. **The Underground Website Where You Can Buy Any Drug Imaginable**. Disponível em: <<https://www.gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160>>, acesso em 31/07/2022.

GOV.UK. **Government sets out plan to make UK a global cryptoasset technology hub.** Disponível em: <<https://www.gov.uk/government/news/government-sets-out-plan-to-make-uk-a-global-cryptoasset-technology-hub>>, acesso em 03/12/2022.

GRABOSKY, Peter. **The prevention and control of economic crime.** Disponível em: <<http://press-files.anu.edu.au/downloads/press/p228301/pdf/ch091.pdf>> acesso em 04/10/2021.

GRZYWOTZ, Johanna. **Virtuelle Kryptowährungen und Geldwäsche.** Berlin: Duncker & Humblot.

GUARAGNI, Fábio André. BACH, Marion. MARIA SOBRINHO, Fernando Martins. **Direito Penal Econômico Administrativização do direito penal, criminal compliance e outros temas contemporâneos.** Londrina, PR: Thoth, 2017.

GURREA-MARTINEZ, Aurelio; REMOLINA, Nydia. **The Law and Finance of Initial Coin Offerings. Ibero-American Institute for Law and Finance, Working Paper Series, n. 4, 2018.** Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182261>, acesso em 10/11/2022.

HGTV. **How to buy real estate with bitcoin.** Disponível em: <www.hgtv.com/lifestyle/real-estate/how-to-buy-real-estate-with-bitcoin>, acesso em 03/08/2022.

ICE. **Ross Ulbricht, aka Dread Pirate Roberts, sentenced to life in federal prison for creating, operating 'Silk Road' website.** Disponível em: <<https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating>>, acesso em 31/07/2022.

INFOMONEY. **CDI: O que é, como funciona e como se relaciona com seus investimentos.** Disponível em: <<https://www.infomoney.com.br/guias/cdi/>>, acesso em 02/08/2022.

INVESTOPEDIA, **Bitcoin Exchange.** Disponível em: <<https://www.investopedia.com/terms/b/bitcoin-exchange.asp>>, acesso em 07/09/2021.

INVESTOPEDIA. **Roots of Money.** Disponível em: <https://www.investopedia.com/articles/07/roots_of_money.asp>, acesso em 27/05/2023.

INVESTOPEDIA. **The 6 Most Private Cryptocurrencies.** Disponível em: <<https://www.investopedia.com/tech/five-most-private-cryptocurrencies/>>, acesso em 03/08/2022.

IRS. **2022 Annual Report.** Disponível em: <<https://www.irs.gov/pub/irs-pdf/p3583.pdf>>, acesso em 03/12/2022.

JESCHECK, Hans-Heinrich; WEIGEND, Thomas. **Tratado de derecho penal: Parte general.** 5. ed. atual. e ampl. Trad. Miguel Olmedo Cardenete. Granada: Colmares, 2002.

JUSTICE. **Cryptocurrency Fraudster Sentenced for Money Laundering and Securities Fraud in Multi-Million Dollar Investment Scheme.** Disponível em: <<https://www.justice.gov/opa/pr/cryptocurrency-fraudster-sentenced-money-laundering-and-securities-fraud-multi-million-dollar>> acesso em 20/10/2022.

JUSTICE. **Government Seized \$3.6 Billion in Stolen Cryptocurrency Directly Linked to 2016 Hack of Virtual Currency Exchange.** Disponível em <<https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launders-45-billion-stolen-cryptocurrency>>, acesso em 15/09/2022.

JUSTICE. Liberty Reserve Founder Arthur Budovsky Sentenced In Manhattan Federal Court To 20 Years For Laundering Hundreds Of Millions Of Dollars Through His Global Digital Currency Business. Disponível em <<https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years>>, acesso em 20/10/2022.

JUSTICE. The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets. Disponível em: <<https://www.justice.gov/ag/page/file/1535236/download>>, acesso em 22/10/2022.

JUSTICE. **Two Arrested for Alleged Conspiracy to Launder \$4.5 Billion in Stolen Cryptocurrency.** Disponível em: <<https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launders-45-billion-stolen-cryptocurrency>>, acesso em 05/10/2022.

JUSTICE. **Two Estonian Citizens Arrested in \$575 Million Cryptocurrency Fraud and Money Laundering Scheme.** Disponível em: <<https://www.justice.gov/opa/pr/two-estonian-citizens-arrested-575-million-cryptocurrency-fraud-and-money-laundering-scheme>>, acesso em 25/11/2022.

KASPERSKY. **O que é criptomoeda e como funciona?** Disponível em: <<https://www.kaspersky.com.br/resource-center/definitions/what-is-cryptocurrency>>, acesso em 28/05/2023.

LABOISSIÈRE, Paula. **Operação combate lavagem de dinheiro no mercado de criptomoedas.** Agência Brasil. Disponível em: <<https://agenciabrasil.ebc.com.br/geral/noticia/2022-09/operacao-combate-lavagem-de-dinheiro-no-mercado-de-criptomoedas>>, acesso em 22/10/2022.

LEITE, Eduardo de oliveira. **A monografia jurídica**. 5 ed. São Paulo: Revista dos Tribunais, 2001.

LEWIS, Antony. **The Basics of Bitcoins and Blockchains**. Editora: Mango; Illustrated Edition, 2018.

LIN, Lindsay X. **Deconstructing decentralized exchanges**. <<https://assets.pubpub.org/ob89i66u/61573938834913.pdf>>, acesso em 03/08/2022.

LIN. X. L., Legal Counsel at Interstellar and Stellar Development. (2019). **Deconstructing Decentralized Exchanges**. **Stanford Journal of Blockchain Law & Policy**. Disponível em <<https://stanford-jblp.pubpub.org/pub/deconstructing-dex>>, acesso em 01/12/2022.

LUCAS, Ana Paula. **Direito Penal Econômico, Revista Saber Direito**. Disponível em <http://www.stf.jus.br/repositorio/cms/portaITvJustica/portaITvJusticaNoticia/anexo/SABER_DIREITO_AULA_Ana_Claudia_Lucas.doc>, acesso em 20/10/2021.

LUI, Alison; RYDER, Nicholar. **Fintech, Artificial intelligence and the law**. Published in 2021: by Routledge, New York.

MASI, Carlo Velho. **Direito Penal Econômico: do que estamos falando?** Canal Ciências Criminais, 2016. Disponível em: <<https://canalcienciascriminais.com.br/direito-penal-economico-do-que-estamos-falando/>>, acesso em 20/12/2021.

MELCHIORI, Juliano Callegari. **As criptomoedas e o crime de evasão de divisas**. Disponível em: <<https://www.conjur.com.br/2021-nov-20/juliano-melchiori-criptomoedas-crime-evasao-divisas>>, acesso em 02/08/2022.

MENDRONI, Marcelo Batlouni. **Tópicos essenciais de lavagem de dinheiro**. São Paulo: Revista dos Tribunais, maio 2001, citado por Castellar, João Carlos. Lavagem de Dinheiro – a questão do bem jurídico. Rio de Janeiro: Revan, 2004.

MORAIS, Fábio Luiz de. FALCÃO, Rondinelli Melo Alcântara. **A regulação de criptomoedas como instrumento de prevenção à lavagem de dinheiro**. Cadernos Técnicos da CGU, v. 3 (2022): Coletânea de Artigos Correccionais, novembro de 2022. Disponível em: <https://revista.cgu.gov.br/Cadernos_CGU/article/view/607/337>, acesso em 02/12/2022.

MORO, Sergio Fernando. **Crime de lavagem de dinheiro**. São Paulo: Saraiva, 2010.

MOSLAVAC. **Cryptocurrency tumbler: legality, legalization, criminalization**. Disponível em: <<http://www.mpce.mp.br/wp-content/uploads/2019/12/ARTIGO-12.pdf>>, acesso em 02/08/2022.

MPRS. **Cybergaeco: mprs cria grupo especializado em combater crimes praticados na internet.** Disponível em: <<https://www.mprs.mp.br/noticias/53708/>>, acesso em 03/08/2022.

MPSC. **MPSC alinha parceria com MPSP para replicar em Santa Catarina o Cyber GAECO.** Disponível em: <<https://mpsc.mp.br/noticias/mpsc-alinhava-parceria-com-mpsp-para-replicar-em-santa-catarina-o-cyber-gaeco>>, acesso em 03/08/2022.

MULLER, Christian H. KALIN, John G. Goldsworth. **Anti-money-laundering: international law and practice.** Editora: John Wiley & Sons; edição: 2007.

MUNHOZ, Vanessa da Costa. Vulnerabilidade externa e controle de capitais no Brasil: uma análise das inter-relações entre câmbio, fluxos de capitais, IOF, juros e risco-país. Nova Economia [online]. 2013, v. 23, n. 2 [Acessado 2 Agosto 2022], pp. 371-402. Disponível em: <https://doi.org/10.1590/S0103-63512013000200005>, acesso em 05/03/2023.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System.** Disponível em: <<https://bitcoin.org/bitcoin.pdf>>, acesso em 10/09/2021.

NUNES, Leandro Bastos. **Evasão de Divisas.** Editora Juspodivm, 2017.

O GLOBO. **FBI fecha Silk Road, site secreto para comércio de drogas ilícitas.** <<https://g1.globo.com/tecnologia/noticia/2013/10/fbi-fecha-silk-road-site-secreto-para-comercio-de-drogas-ilicitas.html>>, acesso em 31/07/2022.

OCCPR. Report: **Money Laundering via Cryptocurrencies up 30% in 2021.** Disponível em: <https://www.occrp.org/en/daily/15898-report-money-laundering-via-cryptocurrencies-up-30-in-2021#:~:text=Money%20laundering%20via%20cryptocurrencies%20increased,by%20blockchain%20analysis%20firm%20Chainalysis>. Acesso em 31/07/2022.

ORMSBY, Eileen. Silk Road. Macmillan: Pan Macmillian Australia. published in 2014.

PACELLI, Eugênio. FISCHER, Douglas. **Comentários ao Código de Processo Penal e sua jurisprudência.** – 9. ed. rev. e atual. – São Paulo: Atlas, 2017.

PARKER, Selwyn. The Great Crash: How the Stock Market Crash of 1929 Plunged the World into Depression. Piatkus Books; Digital original edition: 2008.

PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática.** 14 ed. ver., atual. e ampl. Florianópolis: Empório Modara, 2018.

PEDROSO, Fernando Gentil Gizzi de Almeida; HERNANDES, Luiz Eduardo Camargo Outeiro. **Direito Penal Econômico.** Salvador: Editora Juspodivm.,2017.

PIFFER, C.; CRUZ, P. M.; TEIXEIRA, A. V. **Da transnacionalidade financeira de Bretton Woods às moedas digitais**. Revista Justiça do Direito, v. 34, n. 1, p. 6-28, 30 abr. 2020.

PIMENTEL, Manoel Pedro. **Direito penal econômico**. São Paulo: Revista dos Tribunais, 1973.

POPPER, Nathaniel. Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money. Editora: Harper Paperbacks; Reprint edição, 2016.

PRADO, Luiz Regis. **Direito Penal Econômico**. Rio de Janeiro: Forense, 2019, 8. Ed

PRADO, Luiz Regis. Direito penal econômico: ordem econômica, relações de consumo, sistema financeiro, ordem tributária, sistema previdenciário. São Paulo: Revista dos Tribunais, 2004.

QUINTERO OLIVARES, Gonzalo. El derecho penal ante la globalización. Reflexiones sobre las leyes penales y los penalistas españoles. Madrid: Civitas, 2004.

REBOUÇAS, Sérgio. **Evasão de divisas e retroatividade da Resolução 4.844/2020 do CMN**. <Disponível em: <https://www.conjur.com.br/2020-ago-17/opiniao-evasao-divisas-retroatividade-resolucao-cmn>>, acesso em 20/09/2021.

RECEITA FEDERAL. Instrução Normativa RFB Nº 1888, de 03 de Maio de 2019. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Publicado(a) no DOU de 07/05/2019, seção 1, página 14. Disponível em: <<http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592>> Acesso em 15.08.2022.

REUTERS. **Crypto money laundering rises 30% in 2021 -Chainalysis**. <<https://www.reuters.com/technology/crypto-money-laundering-rises-30-2021-chainalysis-2022-01-26/>>, acesso em 23/06/2022.

REUTERS. **Cryptocurrency and anti-money laundering enforcement**. Disponível em: <<https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26>> acesso em 01/12/2022.

REUTERS. **Cryptocurrency crime surges, losses hit \$4.4 billion by end-September: CipherTrace report**. Disponível em: <<https://www.reuters.com/article/us-crypto-currencies-crime-idUSKBN1Y11WH>>, acesso em 13/12/2021.

SAADI, Ricardo Andrade. **Cooperação jurídica internacional em matéria penal**. Disponível em: <<https://www.justica.gov.br/sua-protecao/lavagem-de>>

dinheiro/institucional-2/publicacoes/arquivos/cartilha-penal-09-10-14-1.pdf.>, acesso em 13/12/2021.

SENADO. **Senado aprova mercado de criptomoedas com incentivo para energia.** Disponível em: <<https://www12.senado.leg.br/noticias/materias/2022/04/26/senado-aprova-mercado-de-criptomoedas-com-incentivo-para-energia-renovavel>>, acesso em: 01/05/2022.

SEU DINHEIRO. **Aceita bitcoin: Tráfico de drogas no Rio de Janeiro aceitava criptomoedas por WhatsApp; envolvidos são presos.** Disponível em: <<https://www.seudinheiro.com/2021/bitcoin/trafico-de-drogas-bitcoin-criptomoedas-whatsapp/>>, acesso em 02/08/2022.

SOLON, Olivia. **Police crackdown on Silk Road following first drug dealer.** Disponível em: <<https://www.wired.co.uk/article/silk-road-crackdown>>, acesso em 20/06/2022.

SOUZA, Artur de Brito Gueiros; AZEVEDO, Juliana de. **Inovações no direito penal econômico: prevenção e repressão da criminalidade empresarial.** Brasília: ESMPU, 2018. Santa Rosa Câmara.

SULLIVAN, Kevin. **Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business.** Editora Apress: 2015, California/USA.

SUPREMECOURT. **ROSS WILLIAM ULBRICHT, PETITIONER v. UNITED STATES OF AMERICA.** Disponível em: <https://www.supremecourt.gov/DocketPDF/17/17-950/24860/20171222095855755_Ulbricht%20cert%20petition.pdf>, acesso em 31/07/2022.

SUTHERLAND, Edwin. **White-collar criminality.** *American Sociological Review*, 5(1), 1–12: 1940.

TECNOBLOG. **GAS Consultoria Bitcoin tem R\$ 38 bilhões bloqueados e deixa de pagar clientes.** Disponível em <<https://tecnoblog.net/noticias/2021/09/16/gas-consultoria-bitcoin-tem-r-38-bilhoes-bloqueados-e-deixa-de-pagar-clientes/>>, acesso em 22/06/2022.

TELEGRAPH. **The history of money from barter to bitcoin.** Disponível em: <<https://www.telegraph.co.uk/finance/businessclub/money/11174013/The-history-of-money-from-barter-to-bitcoin.html>>, acesso em 03/09/2021.

TÓRTIMA, José Carlos. **Crimes Contra o Sistema Financeiro.** Editora Lumen Juris: 2011.

TRANSPARENCY.ORG. **Corruption perceptions index**. Disponível em: <<https://www.transparency.org/en/cpi>>, acesso em 23/12/2021.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasoç. 2014.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig von Mises Brasoç. 2014.

WASHINGTON POST. **First she documented the alt-right. Now she's coming for crypto**. Disponível em: <<https://www.washingtonpost.com/technology/2022/05/29/molly-white-crypto/>>, acesso em 03/08/2022.

WEBSTER. **Non fungible token**. Disponível em: <<https://www.merriam-webster.com/dictionary/non-fungible%20token>>, acesso em 28/05/2023.

WIRED. **The Untold Story of Silk Road, Part 1**. Disponível em: <<https://www.wired.com/2015/04/silk-road-1/>>, acesso em 31/07/2022.

WSJ. **Cryptocurrency-Based Crime Hit a Record \$14 Billion in 2021**. Disponível em: <<https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073>>, acesso em 03/12/2022.

ZUMAS, Vytautas Fabiano Silva. **Criptomoedas, criptocrime e criptoinvestigação**. Disponível em: <<https://www.direitonet.com.br/artigos/exibir/11637/Criptomoedas-criptocrime-e-criptoinvestigacao>>, acesso em 23/06/2022.