A REGULAÇÃO DA UNIÃO EUROPEIA SOBRE CRIPTOMOEDAS E RISCOS DE LAVAGEM DE DINHEIRO

Uma análise crítica da Quinta Diretiva Antilavagem de Dinheiro frente aos provedores de serviços de criptomoeda

THE GREENS/EFA in the European Parliament

iris
INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

A REGULAÇÃO DA UNIÃO EUROPEIA SOBRE CRIPTOMOEDAS E RISCOS DE LAVAGEM DE DINHEIRO

Uma análise crítica da Quinta Diretiva Antilavagem de Dinheiro frente aos provedores de serviços de criptomoeda

PRODUZIDO POR
Instituto de Referência em Internet e Sociedade

SOLICITADO POR
The Greens/EFA group in the European Parliament

AUTORIA
Florencia Lorenzo
Gustavo Ramos Rodrigues
Lahis Pasquali Kurtz

REVISÃO
Luíza Couto Chaves Brandão

TRADUÇÃO
Gustavo Ramos Rodrigues
Lahis Pasquali Kurtz

PROJETO GRÁFICO, CAPA , DIAGRAMAÇÃO E FINALIZAÇÃO
Felipe Duarte

PRODUÇÃO EDITORIAL
Instituto de Referência em Internet e Sociedade

O IRIS é um instituto de pesquisa sem fins lucrativos, sediado no Brasil, que produziu este relatório, a pedido do Grupo dos Verdes/Aliança Livre Europeia no Parlamento Europeu. O tema foi pesquisado no 2º semestre de 2019 de maneira acadêmica e independente, considerando a experiência do Instituto no campo. Este documento, tradução do original em inglês (no prelo), apresenta os resultados encontrados.

COMO CITAR EM ABNT

KURTZ, Lahis; LORENZO, Florencia; RODRIGUES, Gustavo. **A regulação da União Europeia sobre criptomoedas e riscos de lavagem de dinheiro :** uma análise crítica da Quinta Diretiva Antilavagem de Dinheiro frente aos provedores de serviços de criptomoeda. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2020. Disponível em: <https://bit.ly/3cQIHM5>. Acesso em: dd mmm. AAAA.

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

SUMÁRIO

SUMÁRIO EXECUTIVO

Dez anos se passaram desde que o Bitcoin, a primeira e mais conhecida criptomoeda, foi lançado. Criptomoedas se tornaram, desde então, chavões, simbolizando o potencial, mas também os desafios relacionados à nova era da economia digital e da tecnologia financeira (fintech). Parte notável dessas preocupações deriva do fato de o Bitcoin ter sido originalmente desenvolvido com o objetivo explícito de evitar a vigilância e a regulação por parte do Estado. Tornou-se claro nos últimos anos - com um número crescente de episódios conhecidos - que as criptomoedas e os ativos virtuais também estão começando a representar um alto nível de risco em termos de lavagem de dinheiro e financiamento do terrorismo.

Em 2013, o sistema de pagamentos Liberty Reserve foi fechado com uma estimativa de 55 milhões de transações ilegais, e o Silk Road, um mercado digital que operava através do Bitcoin e permitia aos usuários comprar mercadorias ilícitas anonimamente, teve suas operações fechadas pelo Federal Bureau of Investigation (FBI). Após o Silk Road, houve outros episódios dos mercados da darknet, como Alphabay e Hansa, onde mercadorias ilícitas foram negociadas com ativos criptográficos. Esquemas de financiamento de grupos nazistas e fundamentalistas por meio de criptomoedas também foram revelados ao longo desta década. Em 2017 e 2018, mais de 10 milhões de euros em esquemas de lavagem de dinheiro foram desmantelados pelo FBI e pela Europol, a autoridade policial da União Europeia. Esses exemplos mostram claramente que estamos enfrentando um problema sério que não pode ser subestimado.

No entanto, a regulação de criptomoedas e ativos virtuais não é um exercício fácil e é altamente questionável que a legislação atual seja adequada para essa tarefa. Este novo estudo argumenta que a legislação da União Europeia precisa ser fortalecida.

A Quinta Diretiva Antilavagem de Dinheiro (AMLD5) da União Europeia foi aprovada em 2018, com previsão de transposição para as legislações dos Estados-Membros da UE até 10 de janeiro de 2020. A AMLD5 não é a primeira reação para regular os desafios gerados pelas criptomoedas, mas este passo inicial não é o suficiente. Mesmo com as melhorias implementadas por esta norma, a AMLD5 bastará para enfrentar os desafios impostos pelos ativos virtuais no combate à lavagem de dinheiro e ao financiamento do terrorismo.

As principais características dos ativos virtuais que levantaram desafios regulatórios são sua natureza descentralizada, transfronteiriça e pseudoanônima. Sua natureza descentralizada é um desafio para regulações que enfatizam instituições de crédito e instituições financeiras como “pontos de estrangulamento”. Sua natureza pseudoanônima dificulta a implementação das políticas “Conheça Seu Cliente” (Know Your Customer - KYC). Também é importante ressaltar que a eficiência dos instrumentos normativos contra a lavagem de dinheiro tem implicações diretas para iniciativas de combate à sonegação de impostos, uma vez que os crimes fiscais estão incluídos na diretiva de combate à lavagem de dinheiro na forma de origens potencialmente criminosas de ativos que podem ser lavados.

Após a aprovação do AMLD5 pelos colegisladores europeus em 2018, o Grupo de Ação Financeira Internacional (GAFI) emitiu um novo guia contendo diretrizes para ativos virtuais e provedores de serviços de ativos virtuais. Enquanto

a referência global em normatização contra a lavagem de dinheiro, há expectativa de que eles sejam transpostos para ordenamentos nacionais e regionais. As autoridades europeias de supervisão têm defendido repetidamente essa transposição. Espera-se que a nova Comissão Europeia apresente uma nova proposta legislativa para enfrentar os desafios relacionados às criptomoedas. Portanto, o estudo faz sugestões concretas sobre o que deve ser feito para lidar com os riscos de lavagem de dinheiro por meio de criptomoedas ou, como sugerido pelo glossário atualizado do GAFI, Ativos Virtuais.

A REGULAÇÃO DA UNIÃO EUROPEIA SOBRE CRIPTOMOEDAS E RISCOS DE LAVAGEM DE DINHEIRO

Principais Recomendações de Policy

As Recomendações de Policy de números 1 a 4 são consideradas críticas no sentido de que a falha em abordá-las adequadamente poderia comprometer todo o arcabouço legal antilavagem de dinheiro e contra o financiamento do terrorismo. As outras recomendações, por sua vez, se direcionam a preocupações mais específicas relacionadas a tópicos específicos associados a essa regulação, mas com os quais é, ainda assim, necessário lidar.

1. O conceito de financiamento do terrorismo deveria ser definido de modo a incluir não apenas fundos, mas também propriedades, dado que Ativos Virtuais não são explicitamente considerados como fundos.

2. O escopo de Entidades Obrigadas definido pela diretiva deve incorporar Provedores de Serviços Virtuais que não estão incluídos atualmente, como exchanges que conduzem transações somente entre Ativos Virtuais, e não entre eles e moeda fiduciária. Duas abordagens alternativas podem ser adotadas para tanto: i) Criar uma categoria de Provedores de Serviços Virtuais no tópico referente a Entidades Obrigadas, a qual será listada periodicamente pelas Autoridades Europeias de Supervisão. ii) Adicionar provedores de carteira em formato de software e exchanges que conduzem somente operações entre ativos virtuais à lista de Entidades Obrigadas, deixando espaço para que Estados-Membros deliberem, de acordo com suas próprias avaliações de risco, outros a serem enquadrados pela regulação.

3. O banimento de *mixers* e *tumblers*, aplicações de software que permitem transações anônimas, deve ser considerado, uma vez que eles apresentam desafios sérios para a aplicação de toda a regulação antilavagem de dinheiro e podem debilitar inteiramente os esforços regulatórios.

4. Transações ou contratos não intermediados por uma Entidade Obrigada devem ser tornados juridicamente inexequíveis, dado que a aplicação de toda a regulação antilavagem de dinheiro se alicerça nessas entidades. Essa estratégia também pode ser empregada como estímulo para a regularização do setor de Ativos Virtuais.

5. O termo “Moedas Virtuais” deve ser substituído por Ativos Virtuais para evitar seu enquadramento como “dinheiro” ou “moeda” e torná-lo mais consistente com sua natureza jurídica de propriedade.

6. Os Estados-Membros devem ser capazes de discriminar níveis

de risco no setor de provedores de serviços de ativos virtuais para que possam priorizar áreas específicas. A ausência da obrigação de realizar uma avaliação de risco subsetorial atua como um obstáculo para a discussão informada sobre onde é necessária uma regulação mais intensa.

7. Provedores de Serviços de Ativos Virtuais regulados que não estão registrados não devem ter permissão para operar. Os critérios para registro devem incluir a presença de um diretor executivo residente e presença substancial da equipe de gerência. A ausência desse padrão pode levar à implementação inconsistente dos requisitos de registro em nível nacional.

8. Provedores de Serviços Ativos Virtuais deveriam ser obrigados a buscar a aprovação prévia das autoridades para a realização de modificações substanciais em suas estruturas, operações de negócios e acionistas, a fim de garantir que sua equipe de gerência e seus beneficiários efetivos sejam pessoas adequadas e próprias.

9. Para assegurar que há um modo de monitorar e agir efetivamente para o cumprimento da regulação antilavagem de dinheiro e contra o financiamento do terrorismo, Provedores de Serviços de Ativos Virtuais que são filiais ou subsidiárias de uma empresa baseada em outro Estado Membro devem ser incluídos expressamente com outros serviços de pagamento ou câmbio que são obrigados a manter um contato central em seu Estado Membro.

1. Metodologia do Relatório

Este estudo consiste em uma avaliação da Quinta Diretiva de Combate à Lavagem de Dinheiro (AMLD) da União Europeia, levando em consideração as diretrizes recentemente publicadas pelo Grupo de Ação Financeira Internacional (GAFI) sobre ativos virtuais. A primeira parte do artigo apresenta fatos e dados relevantes sobre os ativos virtuais e explica como eles estão relacionados à atividade criminosa (lavagem de dinheiro e financiamento do terrorismo). Também discutimos os riscos que essas tecnologias representam. A segunda seção consiste em uma análise detalhada dos principais pontos que devem ser abordados para que a AMLD seja consistente com as recentes diretrizes do GAFI, seguidas dos tópicos que já são adequados.

2. Contexto, riscos e desafios

2.1. Fatos e dados sobre Ativos Virtuais

Dez anos se passaram desde o lançamento do Bitcoin, a primeira e mais conhecida criptomoeda. Desde então, esse tópico tem sido objeto de grande debate, com posições que variam de extremo otimismo, declarando o mérito de ativos financeiros descentralizados, a análises que atribuem um status intrinsecamente maligno a essa tecnologia[1].

As criptomoedas foram primeiro concebidas como uma "versão puramente par a par do dinheiro eletrônico [que] permitiria que os pagamentos online fossem enviados diretamente de uma parte para outra sem passar por uma instituição financeira"[2], por meio da tecnologia de Blockchain. Blockchain, por sua vez, pode ser caracterizado como "um conjunto de protocolos que possibilita o desenvolvimento de redes de transações nas quais os registros são distribuídos entre os participantes da rede, os quais agem como nós validadores"[3].

Uma transação de ativo virtual pode ser facilmente conduzida sem intermediários: o usuário deve ter uma conta na plataforma (chamada chave pública ou carteira), que vem com uma chave privada (análoga a uma senha) necessária para gerenciá-la. É possível receber e enviar criptomoedas de e para outras contas. Essa conta pode não ser associada a nenhuma identificação civil, como nome, endereço, etc., o que tornaria possível destacar quem é a pessoa por trás dela. A menos que o usuário empregue um serviço intermediário, como um custodiante, não há nada que conecte a identidade do usuário à da carteira. Nesse sentido, mesmo que as

1 Ver: KRUGMAN, P. Bitcoin is evil. **The New York Times**, v. 28. 2013.e KRUGMAN, P. Bubble, bubble, fraud and trouble. The New York Times. 2018. Disponível em: https://www.nytimes.com/2018/01/29/opinion/bitcoin-bubble-fraud.html. Acesso em: 23 out. 2019.

2 NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. **Satoshi Nakamoto Institute**. 2008. Disponível em: https://nakamotoinstitute.org/bitcoin/ Acesso em: 12 nov. 2019. O White Paper de Nakamoto é considerado o principal fundamento tecnológico para a Bitcoin.

3 RODRIGUES, G; KURTZ, L. **Criptomoedas e regulação antilavagem de dinheiro no G20**. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2019. Disponível em: http://bit.ly/2m9pOz0 Acesso em: 12 nov. 2019.

transações estejam publicamente disponíveis na Blockchain, as identidades das partes envolvidas são, de fato, anônimas. O anonimato é uma questão importante, porque não há um intermediário regulado (como um banco ou instituição financeira) e, portanto, as medidas de monitoramento tendem a ser ineficazes, pois o usuário não pode ser rastreado pelos dados no sistema.

Além disso, dado que é possível identificar o proprietário de uma conta se se souber qual sua chave pública e os registros na plataforma são públicos, vários mecanismos de aprimoramento do anonimato foram desenvolvidos, como mixers e tumblers, ferramentas que impedem a vinculação de transações a carteiras específicas. Para fazer isso, eles coletam fundos de diferentes transações e os redistribuem de maneira aparentemente aleatória, de modo a obscurecer o vínculo entre remetente e destinatário. O Serviço de Informação e Investigação Fiscal, em estreita cooperação com a Europol e as autoridades do Luxemburgo, encerrou recentemente um serviço de mixing multimilionário denominado BestMixer[4]. Há ainda as chamadas Criptomoedas de Anonimidade Elevada, como o DASH, que inclui um serviço chamado PrivateSend, que fornece anonimato por meio de um processo de mixing[5].

Os ativos virtuais representam um grande desafio para a maioria das estruturas legais atualmente em vigor e, como inovação tecnológica, levantam preocupações sobre seus possíveis impactos no sistema financeiro como um todo. Inerente a essas preocupações, está o fato de o Bitcoin ter sido originalmente desenvolvido com o objetivo explícito de evitar a vigilância do Estado[6], e a publicização de episódios como o do Silk Road[7] ajudou a conectar sua identidade a transações ilícitas.

É importante ressaltar que a obtenção de dados empíricos confiáveis sobre o assunto de ativos virtuais ainda é uma tarefa bastante complexa e a maioria dos esforços se baseia em dados publicamente disponíveis. Esse desafio é ainda maior ao abordar questões relacionadas aos riscos que essa tecnologia representa para lavagem de dinheiro, financiamento terrorista e sonegação de impostos, uma vez que esses são campos inevitavelmente ligados a uma quantidade escassa de dados disponíveis devido a sua natureza. No entanto, alguns dados exploratórios, extraídos principalmente de episódios criminais com repercussões consideráveis, sugerem que os ativos virtuais podem representar uma área importante de negligência regulatória e, portanto, uma alternativa viável às técnicas mais usadas de lavagem de dinheiro e sonegação de impostos.

Isso é particularmente relevante, pois seu surgimento coincide com um

4 Ver: EUROPOL. **Multi-million euro cryptocurrency laundering service bestmixer.io taken down**. 2019. Disponível em: https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down. Acesso em: 18 nov. 2019.

5 DASH. **Dash 101 - 7 What is PrivateSend? 2018**. Disponível em: https://www.youtube.com/watch?v=v_HwQAyIQns. Acesso em: 18 nov. 2019.

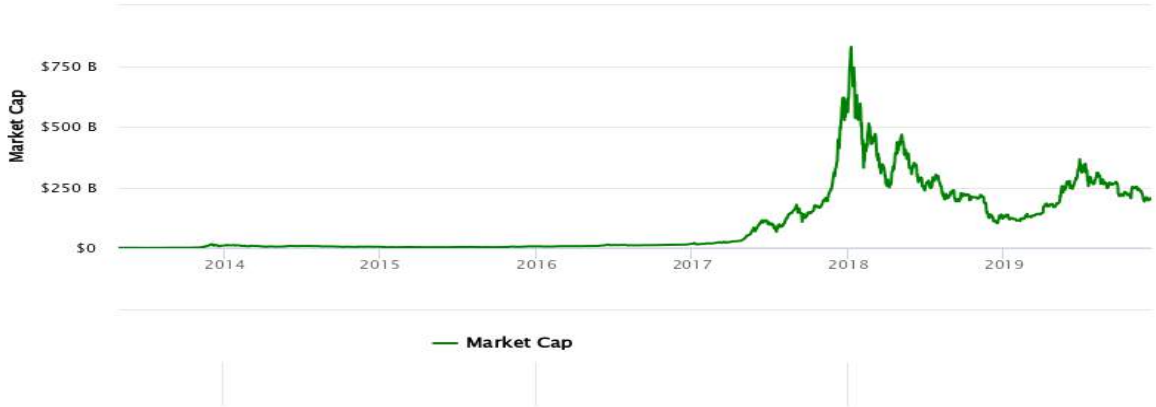
6 Sobre o movimento ideológico que sustentou o desenvolvimento da Bitcoin, ver: SWARTZ, L. What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. **Cultural Studies**, v. 32, n. 4, 2018. p. 623-650.

7 Ver Tabela 1 para explicação mais detalhada desse episódio.

período de avanços substanciais nos esforços para regular a sonegação de impostos e a lavagem de dinheiro: alguns autores chegaram a argumentar que as criptomoedas são potenciais "super paraísos fiscais"[8] que podem inviabilizar a governança global relacionada a esses esforços regulatórios. Afinal de contas, foi em 2009 que o G20 definiu em reunião que "o fim do sigilo bancário"[9] era um de seus objetivos, o mesmo ano em que o Bitcoin ganhou existência.

Embora os ativos virtuais continuem sendo uma parcela menor do sistema financeiro global, sua importância aumentou consideravelmente nos últimos anos. Por valores de 9 de dezembro de 2019, a soma da capitalização de mercado de todas as criptomoedas era de US $ 200.550.218.825 (180.886.269.869,21 €)[10]. O pico de capitalização de mercado de todas as criptomoedas ocorreu em 7 de janeiro de 2018, quando atingiu US $ 828.537.000.000,00[11]. O gráfico 1 exibe a variação ao longo do tempo. O gráfico 2 mostra sua distribuição em comparação a diferentes moedas.

Gráfico 1. Capitalização total de mercado das criptomoedas



Fonte: CoinMarketCap (2019)[12]

8 Ver MARIAN, O. Are cryptocurrencies super tax havens. **Mich. L. Rev. First Impressions**, v. 112, n. 38, 2013.

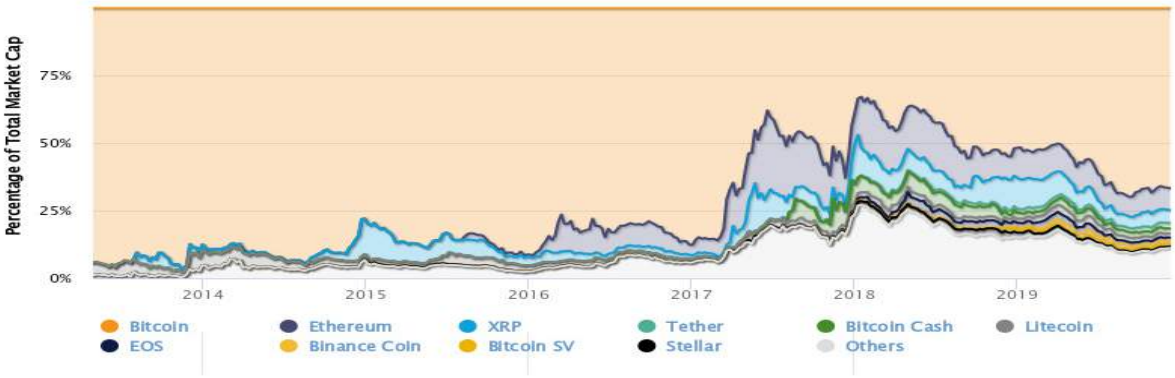
9 Ver G20. **The Global Plan for Recovery and Reform, Final Communique of the G20 Summit Held in London on 2 abr. 2009.** Disponível em: http://www.g20.utoronto.ca/2009/2009communique0402.pdf. Acesso em: 16 out. 2019.

10 Dados obtidos de COINMARKETCAP. **Capitalisation**. Disponível em: https://coinmarketcap.com Acesso em: 14 out. 2019. A capitalização de mercado das criptomoedas é calculada pela multiplicação do estoque total de uma criptomoeda por seu valor atual de mercado. Nós definimos as maiores criptomoedas como aquelas com maior capitalização de mercado. Como o valor das criptomoedas é particularmente volátil, esses números estão sujeitos a mudanças repentinas.

11 Dados de COINMARKETCAP. **Global Charts**. 2019. Disponível em: https://coinmarketcap.com/charts/. Accesso em: 16 nov. 2019.

12 COINMARKETCAP. **Global Charts**. 2019. Disponível em: https://coinmarketcap.com/charts/. Accesso em: 16 nov. 2019.

Gráfico 2. Porcentagem da capitalização total de mercado por criptomoeda



Fonte: CoinMarketCap (2019) Global Charts.[13]

Embora as evidências sobre o volume e a frequência do uso de criptomoedas para lavagem de dinheiro e financiamento do terrorismo não sejam suficientes[14], episódios envolvendo grupos radicais levantaram preocupações com as autoridades sobre o emprego atual dessa tecnologia para tais crimes. A Tabela 1 resume alguns dos episódios que ajudaram a construir tal identificação, explorando episódios de financiamento terrorista, mas também da lavagem de proventos ilícitos.

Tabela 1 - Episódios de elevada repercussão de financiamento terrorista ou lavagem de dinheiro envolvendo Ativos Virtuais

Episódio	Ano	Descrição
Liberty Reserve	2013	Este é considerado o maior esquema de lavagem de dinheiro online até o momento. Embora não empregasse a tecnologia Blockchain, mas moedas virtuais (Liberty Reserve Euro ou Liberty Reserve Dollar[15]), o protocolo de registro do sistema era laxo, o que permitia cadastros com informações falsas. Operou de 2006 a 2013, quando foi encerrado. Estima-se que seis milhões de dólares tenham sido lavados e que cerca de 55 milhões de transações tenham sido conduzidas, a maioria delas sendo ilegal.

13 Ibidem.

14 Ver: DION-SCHWARZ, C., MANHEIM, D., & JOHNSTON, P. B. **Terrorist Use of Cryptocurrencies**: Technical and Organizational Barriers and Future Threats. Rand Corporation, 2019.

15 GAFI - Grupo de Ação Financeira Internacional. **Virtual Currencies** - Key Definitions and Potential AML/CFT Risks. jun. 2014. Disponível em: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Acesso em: 12 dez. 2019.

Silk Road	2013	Silk Road foi um mercado que operou através do Tor, um software que possibilita navegação anônima, no qual bens ilícitos eram negociados. O mercado operou com Bitcoin e foi desvendado pelo FBI em 2013, após mais de 1.5 milhões de transações serem conduzidas em três anos de operações[16].
Arrecadação Terrorista Jihadistas	-	Em 2015, um adolescente da Virgínia chamado Ali Shukri Amin foi processado por explicar em sua conta do Twitter como enviar fundos para o ISIS através do Bitcoin. Esse episódio teve muitas repercussões e, desde então, houve muita especulação sobre se os jihadistas estão empregando ativos virtuais para se financiar. Este artigo no Wall Street Journal[17]cobre alguns episódios relacionados. Este artigo no New York Times[18] também demonstra como a proliferação desses usos está ocorrendo. Ainda assim, de acordo com um relatório da RAND Corporation, há algum consenso de que tal uso seja residual[19].
Financiamento neonazista	-	Houve certa cobertura na imprensa sobre o uso de criptomoedas para financiar grupos neonazistas de extrema direita, como se pode ver nessa entrada no Huffpost[20] e nessa texto da Foreign Policy[21]. Há, inclusive, um bot de Twitter[22] que alegadamente publica transações conduzidas por extremistas neonazistas e de extrema direita.

16 WEISER, B. Ross Ulbricht, creator of Silk Road website, is sentenced to life in prison. **The New York Times**. 29 Maio 2015. Disponível em: https://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html Acesso em: 12 dez. 2019.

17 FORREST, Brett. Jihadists See a Funding Boon in Bitcoin. **The Wall Street Journal**. 20 Feb. 2018. Disponível em: https://www.wsj.com/articles/jihadists-see-a-funding-boon-in-bitcoin-1519131601. Acesso em: 19 nov. 2019.

18 POPPER, Nathaniel. Terrorists Turn to Bitcoin for Funding, and They're Learning Fast. **The New York Times**. 18 ago. 2019. Disponível em: https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html?rref=collection%2Fbyline%2Fnathaniel-popper&action=click&contentCollection=undefined&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection. Acesso em: 19 nov. 2019.

19 DION-SCHWARZ, C., MANHEIM, D., & JOHNSTON, P. B. Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. Rand Corporation, 2019.

20 O'BRIEN, Luke. Who Gave Neo-Nazi Publisher Andrew Anglin A Large Bitcoin Donation After Charlottesville? **Huffpost**. 12 jun. 2019. Disponível em: https://www.huffpostbrasil.com/entry/andrew-anglin-bitcoin-mysterious-donor_n_5d011cc6e4b0304a12087e0c?ri18n=true. Acesso em: 19 Nov. 2019

21 GERARD, David. Neo-Nazis Bet Big on Bitcoin (And Lost). 19 mar. 2019. **Foreign Policy**. 2019. Disponível em: https://foreignpolicy.com/2019/03/19/neo-nazis-banked-on-bitcoin-cryptocurrency-farright-christchurch/. Acesso em: 19 nov. 2019.

22 TWITTER. Neonazi BTC Tracker. **Twitter**. 2019. Disponível em: https://twitter.com/NeonaziWallets. Acesso em: 19 nov. 2019.

AlphaBay e Hansa	2017	AlphaBay e Hansa eram dois mercados ilícitos que foram encerrados[23] em 2017 por um esforço colaborativo do FBI, da *US Drug Enforcement Agency* (DEA) e da *Dutch National Police*, wcom o apoio da Europol. Drogas, armas de fogo e outros bens ilícitos foram negociados lá, com uma estimativa conservadora de 1 bilhão de dólares em comércio. Bitcoin e outras criptomoedas eram empregados nas transações.
Lavagem de proventos oriundos do narcotráfico	2018	Uma operação da Europol derrubou[24] uma rede de lavagem de dinheiro do narcotráfico conduzida por meio de criptomoedas e cartões de crédito. O grupo estava operando através de uma exchange de ativos virtuais com sede na Finlândia. Estima-se que foram lavados mais de oito milhões de euros. Outra operação[25], executada pela Spanish Civil Guard e pela National Police of Colombia, desmantelou dois esquemas de lavagem de dinheiro, que somavam um total de 2.5 milhões de euros.

Fonte: adaptado do material de imprensa do site da EUROPOL

Olhando para a questão de outra perspectiva, o Banco de Compensações Internacionais apresenta algumas evidências sobre a conexão entre criptomoedas e atividades criminosas em seu relatório de 2018[26]: a queda de preço que o Bitcoin sofreu após o encerramento do Silk Road indica uma possível relação entre o uso dessa moeda e as atividades ilícitas do mercado. Ou seja, o fato de o preço do ativo ser afetado pelo encerramento de uma atividade ilegal possivelmente indica correlação, uma vez que os que o compraram deixaram de fazê-lo quando um mercado ilegal que o aceitou como meio de pagamento foi fechado. O mesmo relatório aponta que mais de 22.5% de todas as Ofertas Iniciais de Moeda[27] foram apontadas como fraudulentas.

23 EUROPOL. **Massive blow to criminal dark web activities after globally coordinated operation**. 20 jul. 2017. Disponível em: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation. Acesso em: 19 nov. 2019.

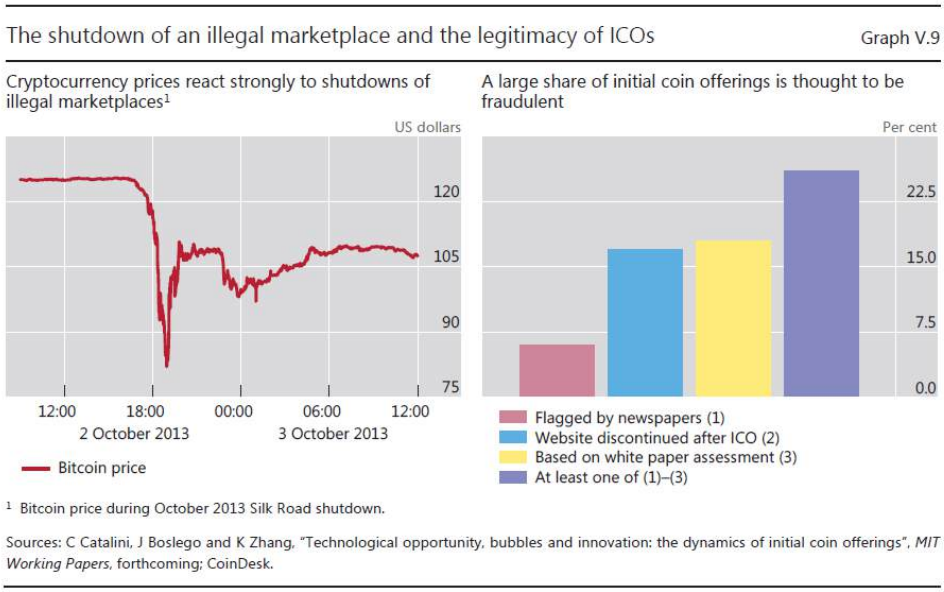
24 EUROPOL. **Illegal network used cryptocurrencies and credit cards to launder more than eur 8 million from drug trafficking**. 09 abr. 2018a. Disponível em: https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking. Acesso em: 19 nov. 2019..

25 EUROPOL. **Two criminal groups dismantled for laundering eur 2.5 million through smurfing and cryptocurrencies**. 11 jul. 2018b. Disponível em: https://www.europol.europa.eu/newsroom/news/two-criminal-groups-dismantled-for-laundering-eur-25-million-through-smurfing-and-cryptocurrencies. Acesso em: 19 nov. 2019.

26 BANCO DE COMPENSAÇÕES INTERNACIONAIS. **Cryptocurrencies**: looking beyond the hype. BIS Annual Economic Report 2018.

27 Uma Oferta Inicial de Moeda é um mecanismo de angariar capital para projetos relativos a criptomoedas. Também são conhecidos como venda de token, venda coletiva ou venda de moeda (tokensale, crowdsale ou coinsale). Normalmente, envolve vender tokens digitais de uma certa moeda através de ação e/ou inscrição antes de seu lançamento. Os tokens podem ser pagos em moeda fiduciária e/ou outra criptomoeda. Ver CHOHAN, Usman W. Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. **SSRN Electronic Journal**, [s.l.], p.1-6, 2017.

Imagem 1. Gráficos demonstrando a correlação entre a queda no preço do Bitcoin, a publicização das atividades do Silk Road e o encerramento ou suspeita sobre serviços de Oferta Inicial de Moeda



Fonte: BIS Annual Economic Report[28]

Em síntese, o risco que Ativos Virtuais representam foi estimulado pelo desenvolvimento de uma série de frameworks regulatórios. A introdução esperada de stablecoins[29] lastreadas por grandes empresas, como Facebook ou Telegram, também leva a preocupações de atores reguladores, incluindo em matéria de evasão fiscal, lavagem de dinheiro e financiamento do terrorismo[30]. Em 5 de Dezembro de 2019, a Comissão Europeia e o Conselho argumentaram, com relação a stablecoins, que "nenhum arranjo global de 'stablecoin' deve começar a operar na União Europeia até que os riscos e desafios regulatórios, legais e de supervisão tenham sido adequadamente identificados e abordados[31]" Na próxima subseção, apresentamos alguns dos principais desafios regulatórios.

28 BANCO DE COMPENSAÇÕES INTERNACIONAIS. op. cit., 2018. p. 107.

29 Stablecoins são criptomoedas que, para minimizar a volatilidade do valor em relação a um certo bem são atreladas a uma reserva de bens.

30 Ver, por exemplo: CŒURÉ, B. **Communiquée released by the Chair of the G7 working group on stablecoins**, Benoît Cœuré. 2019. Disponível em: https://www.bis.org/cpmi/speeches/sp190718.html. Accesso em: 17 out. 2019. O Banco de Compensações Internacionais recentemente apresentou um relatório no qual aborda desafios regulatórios que emergem da inserção de empresas Big tech no setor de finanças. Disponível em: https://www.bis.org/publ/arpdf/ar2019e3.pdf . Accessed: 5 dez. 2019.

31 UNIÃO EUROPEIA. Conselho da União Europeia e da Comissão Europeia. **Joint Statement on stablecoins**. 2019. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2019/12/05/joint-statement-by-the-council-and-the-commission-on-stablecoins/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Joint+statement+by+the+Council+and+the+Commission+on+%22stablecoins%22# Acesso em: 5 dez. 2019.

2.2. Anonimato e descentralização: principais desafios e esforços regulatórios

2.2.1. Contexto regulatório

A lavagem de dinheiro é compreendida, em termos gerais, como "o tratamento de receitas de origem, existência e/ou aplicação ilícita para ocultar e disfarçar essa ilegalidade"[32]. Nesse sentido, a maior parte da regulação antilavagem de dinheiro é concebida para abordar as etapas de colocação, estratificação e integração[33]. A colocação é entendida como a inserção inicial de receitas ilegais na economia formal. Por outro lado, a estratificação é a ocultação da trajetória passada de um ativo ilegal através da realização de uma série de operações. Finalmente, a integração é o momento em que as receitas ilícitas são definitivamente reinseridas na economia formal[34].

Esforços regulatórios internacionais em relação a esse crime estão em andamento desde o final do século XX. Em 1989, o G7 estabeleceu o Grupo de Ação Financeira Internacional (GAFI), um órgão intergovernamental com sede em Paris. Em abril de 1990, o GAFI elaborou seu famoso relatório com suas Quarenta Recomendações, onde forneceu um plano de ação a ser adotado pelos países para combater a lavagem de dinheiro. Em 2001, após o 11 de setembro, incluiu oito novas recomendações e a nona foi incluída em 2004, levando ao que hoje é conhecido como as 40 + 9 Recomendações do GAFI.[35].

Vandezande[36] aponta que a história das diretivas contra a lavagem de dinheiro no contexto europeu acompanhou de perto o desenvolvimento das Recomendações do GAFI e, uma vez que este é reconhecido como um normatizador internacional para combater a lavagem de dinheiro e o financiamento do terrorismo, há expectativa que suas recomendações serão adotadas pelas autoridades reguladoras nacionais e regionais. A AMLD4 situou a Abordagem Baseada em Risco no centro de sua estrutura regulatória, de acordo com as diretrizes de 2012 do GAFI[37] e, nesse

32 RODRIGUES; KURTZ. op. cit, 2019. p. 11.

33 GAFI - Grupo de Ação Financeira Internacional. **Frequently Asked Questions**. 2019. Disponível em: http://www.fatf-gafi.org/faq/moneylaundering/. Acesso em: 16 out. 2019.

34 Uma análise mais detalhada desse processo pode ser encontrada em: RODRIGUES, G; KURTZ, L.. **Criptomoedas e regulação antilavagem de dinheiro no G20**. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2019. Disponível em: http://bit.ly/2m9pOz0 Acesso em: 12 nov. 2019. p.12

35 GAFI - Grupo de Ação Financeira Internacional. **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation**, 2019. FATF, Paris, France. Disponível em: www.fatf-gafi.org/recommendations.html. Acesso em: 29 out. 2019.

36 VANDEZANDE, Niels. **Virtual currencies under EU anti-money laundering law**. Computer law & security review, v. 33, n. 3, p. 341-353, 2017.

37 ASE - Autoridades de Supervisão Europeias (ESA). **Joint Opinion Of The European Supervisory Authorities On The Risks Of Money Laundering And Terrorist Financing Affecting The European Union's Financial Sector**. 2019. Disponível em: https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf?retry=1. Acesso em: 4 out. 2019. p. 6.

sentido, abriu para debate a possibilidade da inclusão de moedas virtuais e Ativos Virtuais.

Durante as discussões sobre a AMLD4, a Autoridade Bancária Europeia publicou seus pareceres sobre moedas virtuais[38], demandando que elas fossem inseridas no quadro legal de combate à lavagem de dinheiro. Embora a diretiva argumentasse que as autoridades competentes e as entidades obrigadas devessem ser proativas no combate às inovações de lavagem de dinheiro derivadas de novas tecnologias - de forma consistente com a Abordagem Baseada em Risco -, os colegisladores europeus optaram por não incluir explicitamente as moedas virtuais[39].

Como argumentam Houben e Snyers[40], após a publicação da AMLD4, houve uma mudança no momento regulatório dos ativos virtuais, especialmente após os ataques terroristas ocorridos na França. Havia demanda crescente por parte do Conselho Europeu e da Comissão Europeia para abordar a posição de negligência regulatória em que os ativos virtuais estavam inseridos. A resposta à proposta original da Comissão foi um trílogo[41] com os colegisladores, recomendando a inclusão de "emissores, administradores, intermediários e distribuidores de moedas virtuais" no universo das Entidades Obrigadas, bem como administradores e provedores de sistemas de pagamento on-line, além de provedores de carteira de custódia e exchanges que faziam câmbio entre moedas virtuais e fiduciárias. No entanto, isso não foi integrado ao texto final da diretiva. Em síntese, a Quinta Revisão da AMLD foi proposta em abril de 2016[42] e o texto final foi acordado no final de 2017. Abordou muitas questões que antes eram negligenciadas, especialmente em questões de escopo de aplicação.

2.2.2. Riscos e desafios dos Ativos Virtuais

Como afirmado anteriormente, a falta de fontes empíricas consistentes leva a um estado de coisas em que a maioria dos desafios regulatórios é inferida a partir de proposições teóricas informadas[43]. Segundo essa literatura, as características do

38 ABE - Autoridade Bancária Europeia. **EBA's Opinion on virtual currency**. 4 julho 2014. Disponível em: https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf. Acesso em: 14 out. 2019.

39 VANDEZANDE, op. cit., 2017. p. 9

40 HOUBEN; SNYERS. op. cit., 2018. p. 63.

41 UNIÃO EUROPEIA. Parlamento Europeu. **Relatório sobre a proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera a Diretiva 2009/101/CE. 9 de março de 2017**. Comissão dos Assuntos Económicos e Monetários. Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos. Disponível em: https://www.europarl.europa.eu/doceo/document/A-8-2017-0056_PT.html. Accesso em: 19 nov. 2019

42 A ABE e o BCE apoiaram essa proposta. Ver: HOUBEN; SNYERS, op. cit., 2018, p. 66.

43 Ver CAMPBELL-VERDUYN, M.; GOGUEN, M. The mutual constitution of technology and global governance: Bitcoin, blockchains, and the international anti-money-laundering regime. In: CAMPBELL-VERDUYN, M. (org.). **Bitcoin and Beyond**: Cryptocurrencies, Blockchains and Global Governance. New York: Routledge, 2018. p. 69-87.

pseudoanonimato e dos fluxos financeiros descentralizados[44] dos ativos virtuais são facilitadores fundamentais para os riscos de lavagem de dinheiro e financiamento ao terrorismo. Por descentralização, entende-se a independência em relação às autoridades financeiras centralizadas, sejam bancos ou outras instituições financeiras. De acordo com Campbell-Verduyn[45], a descentralização permitida pela tecnologia de Blockchain apresenta um desafio substancial, pois evade o foco regulatório histórico em bancos e outras instituições financeiras, entendidos como 'pontos de estrangulamento'[46]. Na medida em que os ativos virtuais excluem esses intermediários como terceiros confiáveis, eles contornam regulações que os enfocaram[47].

Da mesma forma, sua natureza pseudoanônima compromete a capacidade de implementar políticas de "Conheça Seu Cliente", que estão no centro das regulações contra a lavagem de dinheiro. Esse é um recurso que deriva da natureza criptográfica dos ativos virtuais, na qual as transações na Blockchain são públicas e são conduzidas através da chave pública, embora a identidade do proprietário da chave seja oculta. A desconexão entre uma transferência de ativos e seus beneficiários dificulta a identificação de possíveis esquemas de lavagem de dinheiro. Embora muitos ativos virtuais não sejam tecnicamente anônimos, o processo de identificação do beneficiário real de uma transação exige um esforço significativo e técnicas complexas que impedem uma abordagem unificada[48]. Tal situação é exacerbada quando serviços como mixers e tumblers são incorporados à análise, o que torna praticamente impossível identificar o benefício efetivo. Por esse motivo, alguns analistas argumentaram que deveriam ser banidos por completo[49].

Para Houben e Snyers[50], uma das principais dificuldades na regulação de criptomoedas é produzir estruturas abrangentes e flexíveis que se adaptarão a futuras mudanças na tecnologia e, ao mesmo tempo, evitarão inibir inovação nessas tecnologias. Os mesmos autores argumentam que algumas questões que elevam o nível de dificuldade da tarefa são:

1. natureza transfronteiriça, isto é, o fato de terem um status jurídico ambíguo nas jurisdições em que operam.

2. o fato de não possuírem intermediários centralizados, ou seja,

44 Ver CAMPBELL-VERDUYN, M. Bitcoin, crypto-coins, and global anti-money laundering governance. **Crime, Law and Social Change**, v. 69, n. 2, 283–305, mar. 2018. p. 286

45 Ibidem, p. 286.

46 Ibidem, p. 286.

47 CAMPBELL-VERDUYN; GOGUEN. op. cit., 2017. p. 70.

48 HOUBEN, R.; SNYERS, A. Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. Study requested by the Tax3 committee of the Policy Department for Economic, Scientific and Quality of Life Policies European Parliament. European Union: Brussels, July 2018. Disponível em: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf. Acesso em: 14 out. 2019.

49 Ibidem, p. 82.

50 Ibidem, p. 56.

sua natureza descentralizada;

3. o fato das criptomoedas residirem 'nas brechas', isto é, se situarem num espaço legal ambíguo, e;

4. a linha tênue entre proteção de dados, privacidade e cibersegurança e regulação de criptomoedas, já que criptografia é um elemento central da proteção de dados pessoais[51].

Embora a implementação seja uma tarefa difícil, a Abordagem Baseada em Risco elaborada pelo GAFI é reconhecida como uma conquista importante, uma vez que "o fomento de redes descentralizadas de governança é considerado inovador e, em última análise, mais eficaz do que as formas tradicionais de coerção em uma era de mudança tecnológica veloz e imprevisível"[52]. Uma Abordagem Baseada em Risco, conforme definida pelas 40 + 9 Recomendações do GAFI, permite que os países adotem um conjunto de medidas mais flexíveis de acordo com o risco, a fim de garantir proporcionalidade e eficácia. Essa abordagem exige que os países "identifiquem, avaliem e compreendam os riscos de lavagem de dinheiro e financiamento do terrorismo para o país e (...) tomem medidas, incluindo a designação de uma autoridade ou mecanismo para coordenar ações para avaliar riscos e aplicar recursos, visando garantir que os riscos sejam mitigados de maneira eficaz"[53].

Por último, em seu parecer conjunto publicado em 4 de outubro de 2019, as Autoridades Europeias de Supervisão (AES) argumentaram que, segundo a sua pesquisa, a maioria das autoridades nacionais competentes considera que os riscos de branqueamento de capitais / financiamento do terrorismo relacionados com moedas virtuais[54] são devidos a (1) falta de conhecimento e compreensão por parte das empresas e autoridades competentes desses produtos e serviços, o que as impede de realizar uma avaliação de impacto adequada; (2) falta de regulação direta referente a moedas virtuais e produtos e serviços associados; (3) maior processamento de transações on-line, com apenas verificações de identificação e verificação de clientes limitadas sendo realizadas[55].

51 Ibidem, pp. 53-55.

52 CAMPBELL-VERDUYN, op. cit., 2018, p. 284.

53 GAFI. **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation**, FATF, Paris, France. Disponível em: www.fatf-gafi.org/recommendations.html. Accesso em: 29 out. 2019. p. 10.

54 A opinião conjunta menciona "moedas" e nós optamos pelo termo usado no documento. No entanto, essas questões também são aplicadas a Ativos Virtuais em geral.

55 ASE - Autoridades de Supervisão Europeias (ESA). **Joint Opinion Of The European Supervisory Authorities On The Risks Of Money Laundering And Terrorist Financing Affecting The European Union's Financial Sector**. 2019. Disponível em: https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf?retry=1. Acesso em: 4 out. 2019.

2.2.3. Implicações do arcabouço antilavagem de dinheiro para evasão fiscal

Na AMLD, os crimes tributários são crimes predicados à lavagem de dinheiro. Por causa do vínculo entre ambos, é importante avaliar o impacto que a estrutura de combate à lavagem de dinheiro tem sobre os impostos. Como este documento é direcionado a analisar a AMLD5[56] considerando as novas diretrizes do GAFI, apresentamos aqui apenas implicações de evasão fiscal que derivam do arcabouço antilavagem de dinheiro[57]. A regulação de combate à sonegação de impostos depende muito da eficácia de tais normas. Esse é o caso porque o anonimato é um grande facilitador da evasão fiscal. Como argumentam Houben e Snyers, "entrar em transações tributáveis de criptomoeda sem pagar impostos é evasão fiscal. Porém, quando uma autoridade tributária não sabe quem entra na transação tributável por causa do anonimato envolvido, ela não pode detectar nem sancionar essa sonegação"[58].

Na medida em que a regulação antilavagem de dinheiro seja eficaz na identificação do benefício efetivo de um ativo, as informações poderão ser acessadas pelas autoridades fiscais dessa jurisdição. De acordo com a AMLD, as entidades obrigadas devem relatar transações suspeitas, ou seja, devem cooperar "informando a UIF, inclusive apresentando um relatório, por sua própria iniciativa, na ocasião em que a entidade obrigada tome ciência, suspeite ou tenha motivos razoáveis para suspeitar que os fundos, independentemente da quantia envolvida, sejam o produto da atividade criminosa ou estejam relacionados ao financiamento do terrorismo e respondendo prontamente aos pedidos da UIF por informações adicionais nesses casos"[59]. A definição de atividades criminosas adotadas pela AMLD inclui crimes fiscais[60]. De acordo com o artigo 32, ponto 3, a UIF deve "ser responsável por

56 UNIÃO EUROPEIA. Parlamento Europeu. AMLD5. **Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho de 30 de maio de 2018 que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE (Texto relevante para efeitos do EEE)**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843. Acesso em: 19 nov. 2019.

57 Evasão fiscal como um todo é um campo amplo demais para ser coberto por este paper. Para mais informação sobre a relação entre evasão fiscal e ativos virtuasi, ver OZELLI, S. 'Virtual Drivers of Real Economic Growth: The EU's Complex Tax Policy Strategy', Tax Management International Journal (in Bloomberg Tax), v. 47, n. 452. e HADZIEVA, E. Impact of Digitalisation on International Tax Matters, Study for the Committee on Financial Crimes, Tax Evasion and Tax Avoidance, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019.

58 HOUBEN; SNYERS. op. cit., 2018, p. 53.

59 União Europeia, op. cit., 2018, AMLD5, Artigo 33, ponto 1, item a.

60 União Europeia, op. cit., 2018, AMLD5, Artigo 3, ponto 4, item f, inclui crimes tributários em "Todas as infrações, incluindo os crimes fiscais relacionados com impostos diretos e indiretos, na acepção do direito nacional de cada Estado-Membro, que sejam puníveis com pena ou medida de segurança privativa de liberdade de duração máxima superior a um ano ou, nos Estados-Membros cuja ordem jurídica preveja um limiar mínimo para as infrações, todas as infrações puníveis com pena ou medida de segurança privativa de liberdade de duração mínima superior a seis meses".

disseminar os resultados de suas análises e qualquer informação adicional relevante às autoridades competentes, quando houver motivos para suspeitar de lavagem de dinheiro, crimes predicados associados ou financiamento do terrorismo".

Houben e Snyers argumentam que havia preocupações sobre se as autoridades tributárias poderiam ser consideradas autoridades competentes, uma vez que esse conceito não está definido na AMLD. No entanto, os autores argumentam que a quinta revisão da Diretiva de Cooperação Administrativa em Tributação em 2016 garante que as autoridades fiscais tenham acesso às informações coletadas sobre os artigos 13 (Devida Diligência em relação ao Cliente), 30 (Registro de Benefício Efetivo das Empresas), 31 (Benefício Efetivo de Trusts e Análogos) e 40 (Armazenamento de registros)[61][62].

2.2.4. Além da AMLD5: as novas diretrizes do GAFI

O contexto de rápida transformação tecnológica exige que reguladores constantemente revisem os desenvolvimentos do ambiente de Ativos Virtuais. Desde a publicação da AMLD5, o GAFI fez algumas mudanças em suas diretrizes sobre regulação antilavagem de dinheiro relativa a Ativos Virtuais. O guia detalha como as recomendações da força-tarefa devem ser implementadas pelas jurisdições. A Autoridade Bancária Europeia arguiu, em um relatório recente, que a Comissão Europeia deve levar em consideração essas diretrizes atualizadas, especialmente sua reformulação conceitual e a ampliação de seu escopo. A Autoridades Europeia de Investimentos e Mercado e a Opinião Conjunta das Autoridades de Supervisão Europeia também seguem essa linha sobre os riscos da lavagem de dinheiro e financiamento de terrorismo afetarem o setor financeiro da União Europeia. Eles reafirmam sua posição anterior de que moedas virtuais não são tipicamente reguladas sob a lei financeira da UE e, por essa razão, clientes estão sujeitos a riscos.

3. Análise da AMLD5 à luz das diretrizes do GAFI

Nas subseções seguintes, nós abordamos quais são as mudanças significativas que a AMLD deve implementar para que seja consistente com as diretrizes do GAFI para Ativos Virtuais[63].

Os tópicos da Diretiva são usados como referência e são apresentados em dois grupos: o primeiro compreende um comentário sobre o que é regulado acerca do tópico, sua adequação às diretrizes do GAFI, questões deixadas em aberto e como abordar as lacunas, e o segundo compreende aspectos que devem mudar. A

61 HOUBEN; SNYERS, op.cit. 2018, p. 71.

62 UNIÃO EUROPEIA. Conselho Europeu. **Diretiva (UE) 2016/2258 do Conselho, de 6 de dezembro de 2016, que altera a Diretiva 2011/16/UE no que respeita ao acesso às informações antibranqueamento de capitais por parte das autoridades fiscais**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L2258&from=EN Acesso em: 21 nov. 2019.

63 GAFI, op. cit. VA Guidance, 2019.

comparação feita é resumida na Tabela 2.

Tabela 2. Índice de tópicos das diretrizes do GAFI checadas em referência à AMLD5

Grupo	Tópico	GAFI	AMLD5
Precisa adequação	Definições	Recomendação 15	Art. 1, par. 5
	Entidades Obrigadas	Glossário - VASP	Art 3, par. 1
	Abordagem Baseada em Risco	Recomendações 1, 2	Art. 6-8
	Registro e monitoramento	Recomendação 26, 27	Art. 47, 48, 59
	Cooperação Internacional	Recomendações 36-40	Art. 51-56; 65
	Controles Internos	Recomendação 18	Art. 45, 46
Adequado	Devida Diligência com Cliente	Recomendações 10-13, 17, 19	Art. 10-24
	Relatório de Transações Suspeitas	Recomendações 20, 21, 23	Capítulo VI
	Guarda de registros	Recomendação 11	Art. 40

Fonte: autoria própria

3.1. Aspectos que precisam de adequação às diretrizes do GAFI

A Tabela 3 consiste em um índice curto de questões que precisam de adequação, seguidas de nossa recomendação proposta. Nas subseções seguintes, nós abordaremos cada um desses tópicos mais detalhadamente.

Tabela 3. Principais questões e recomendações de policy

Aspecto	Questão	Recomendações de Policy
Defnições	A definição de financiamento terrorista compreende apenas “fundos”, um conceito que exclui Ativos Virtuais. Ativos Virtuais são isentos de serem considerados meios para cometer o crime em questão.	A definição de financiamento terrorista pode ser mudado para incluir não apenas fundos, mas também propriedade. O termo Moeda Virtual deve ser substituído por Ativos Virtuais.
Entidades Obrigadas	O escopo de aplicação é geralmente restrito demais para abordar os riscos existentes.	Duas possíveis abordagens: adicionar uma categoria de Provedor de Serviços de Ativos Virtuais (PSAV) à lista de Entidades Obrigadas ou expandir a lista para incluir, ao menos, câmbios virtual-para-virtual e provedores de custódia de carteira. Ainda, contratos que não envolvam Entidades Obrigadas devem ser inexequíveis judicialmente.
Abordagem Baseada em Risco	Estados Membros não são obrigados a produzir informação sobre perfis de risco associados com produtos e serviços específicos.	Estados Membros devem ser obrigados a exigir que autoridades nacionais identifiquem áreas subsetoriais sujeitas a um nível maior de risco no setor de PSAV.
Registro e monitoramento	Não há provisões específicas assegurando implementação consistente e conformidade efetiva com requisitos de registro.	Entidades Obrigadas devem ser compelidas a buscar aprovação prévia para mudanças substanciais em negócios, operações, acionistas e estruturas. Requisitos de registro devem incluir, ao menos, gerenciamento substancial e um diretor executivo residente.
Cooperação Internacional	Não há provisão efetiva de assistência à extradição por crimes relativos a Ativos Virtuais.	Incluir explicitamente assistência à extradição entre as medidas padrão para cooperação internacional em investigações criminais de lavagem de dinheiro e financiamento de terrorismo relativas a Ativos Virtuais.
Controles Internos	Entidades reguladas não são obrigadas a apontar uma pessoa central de contato encarregada de conformidade em filiais ou subsidiárias majoritárias localizadas em outro Estado Membro.	Prestadores de Serviços de Ativos Virtuais deveriam ser listados em equidade com instituições financeiras no Artigo 45, ponto 9, junto com serviços de câmbio de dinheiro e pagamento.

Fonte: Autoria própria.

3.1.1. Definições

3.1.1.1. O que a AMLD5 prescreve

A AMLD4 deixou espaço para debate sobre se ela seria aplicável ou não a transações com Ativos Virtuais. Ainda que a definição de propriedade apresentada no Artigo 3 (ponto 3) seja expansiva o suficiente para possivelmente englobar Ativos Virtuais, a ausência de quaisquer agentes do ecossistema de Ativos Virtuais na lista de Entidades Obrigadas fornecida no Artigo 2 teve o efeito de liberá-los, para todos os fins práticos, de ser trazido sob o âmbito de aplicação da Diretiva[64].

A AMLD5 mudou isso. O Artigo 3, ponto 18, formalmente definiu "moeda virtual" como uma "representação digital de valor que não seja emitida ou garantida por um banco central ou uma autoridade pública, que não esteja necessariamente ligada a uma moeda legalmente estabelecida e não possua o estatuto jurídico de moeda ou dinheiro, mas que é aceita por pessoas singulares ou coletivas como meio de troca e que pode possa ser transferida, armazenada e comercializada por via eletrônica". Isso, junto com o escopo ampliado de aplicação, que será explicado depois, torna explícito que essa regulação se aplica a Ativos Virtuais.

3.1.1.2. Adequação às diretrizes do GAFI

Em outubro de 2018, o GAFI mudou suas 40+9 Recomendações para incluir os termos Ativo Virtual e Provedor de Serviços de Ativo Virtual Virtual Asset Service Providers (VASPs)[65]. Em fevereiro de 2019, foi publicada a nota interpretativa sobre a Recomendação 15 emendada, que define Ativos Virtuais como "propriedade", "produto", "fundos", "outros bens", ou outro "valor correspondente". O conceito de Ativos Virtuais deriva da compreensão de que eles não são, no sentido propriamente dito, moedas[66].

As inovações da AMLD5, em conjunto com a amplitude da definição de propriedade, parecem o suficiente para assegurar que a Diretiva é aplicável à maioria dos Ativos Virtuais quando diz respeito ao combate à lavagem de dinheiro. Isso é consistente com a recomendação do GAFI para todos os termos baseados em valores, inclusive "propriedade", que serão interpretados compreendendo Ativos

64 HOUBEN; SNYERS. op. cit., p. 62. e VANDEZANDE, op. cit., p. 9. Ainda que a maioria das análises jurídicas considerem que a definição de Entidade Obrigada não se aplique a VASPs, houve episódios em que eles foram considerados como tais por cortes nacionais. Vandezande, por exemplo, mostra como uma corte estoniana considerou uma VASP como Entidade Obrigada.

65 GAFI - Grupo de Ação Financeira Internacional. **Public Statement**: Mitigating Risks from Virtual Assets. 2019. Disponível em: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html. Acesso em: 18 nov. 2019.

66 Há um grande debate sobre essa questão. De uma perspectiva legal, moedas são usualmente definidas por duas características: i) a moeda tem de ser emitida por uma autoridade monetária competente, usualmente um Banco Central; ii) valor legal, isto é, deve ser um meio lícito de cumprir obrigações financeiras que seja aceito ou obrigatório no alcance daquela jurisdição prescritiva. Para uma discussão aprofundada do conceito, ver GOLDBERG, Dror. Legal Tender. SSRN Electronic Journal, [sl], p.1-17, 2008. Elsevier BV. Ainda, a Autoridade Bancária Europeia e o Banco Central Europeu já defenderam que ativos virtuais não são moedas.

Virtuais[67].

Por outro lado, existe um problema com a forma como financiamento terrorista é definido na legislação. Enquanto que o Artigo 1, ponto 3 da AMLD5 se refere repetidamente a "propriedade" ao definir os meios pelos quais alguém comete lavagem de dinheiro, o mesmo artigo, no ponto 5, quando trata de financiamento terrorista, menciona apenas "fundos" como instrumentos para cometê-lo.

A definição de "fundos" não é encontrada no texto da norma, mas sim na Segunda Diretiva de Serviços de Pagamento, que formula o conceito como "notas de banco e moedas, moeda escritural ou moeda eletrônica" (Artigo 4, ponto 25) da mesma forma que a Segunda Diretiva sobre Moeda Eletrônica. Por sua vez, ela estabelece que moeda eletrônica é "o valor monetário armazenado eletronicamente, inclusive de forma magnética, representado por um crédito sobre o emitente e emitido após recepção de fundos para fazer operações de pagamento na acepção do ponto 5 do artigo 4 da Directiva 2007/64/CE e que seja aceito por uma pessoa singular ou coletiva diferente do emitente de moeda electrónica". Isso cria uma brecha pela qual Ativos Virtuais não são considerados fundos porque eles estão fora das categorias compreendidas, e em leitura estrita da AMLD, como não são propriedade, podem ser usados apenas para lavagem de dinheiro e não para financiamento terrorista - enquanto a realidade é que eles estão sendo usados para os dois.

3.1.1.3. Questões e riscos

Conforme o estudioso Niels Vandezande afirma, associar e-money com a emissão no recibo de fundos "essencialmente estabeleceu moeda eletrônica como bem pré-pago"[68], excluindo as criptomoedas. Isso as isenta de serem categorizadas como "fundos", e, assim, de serem enquadradas como meio de cometer o crime de financiamento de terrorismo, o que significa que a norma pode não compreender todos os potenciais usos desse tipo de bem[69].

3.1.1.4. Abordando as lacunas

Para os propósitos da AMLD5, uma possível solução seria mudar a definição de financiamento terrorista no Artigo 1, ponto 5, para incluir não apenas fundos, mas também propriedade, pois os Ativos Virtuais não estão explicitamente incluídos no conceito de fundos e, ainda assim, são usados como meio de financiamento. O conceito de Ativo Virtual deveria substituir o de Moeda Virtual tanto para melhor refletir os muitos usos e funções que essa tecnologia pode ter quanto para tornar mais claro que eles não são, de fato, moedas com validade legal.

67 GAFI, op. cit. VA Guidance, 2019. p. 20. (item 64).

68 Vandezande, N. (2017), op. cit., p. 5

69 Outra questão pode ser que essa definição exclui o controle de um banco central ou autoridade pública, o que pode limitar o escopo de aplicação no caso de moedas virtuais emitidas por autoridades públicas, como o Petro venezuelano. Este não é um problema prático, no entanto, porque os ativos virtuais que são controlados pelas autoridades centrais não apresentam os mesmos riscos em relação à lavagem de dinheiro e ao financiamento do terrorismo, porque fornecem um intermediário que pode ser responsabilizado por fornecer informações sobre usuários e transações.

3.1.2. Entidades obrigadas

3.1.2.1. O que a AMLD prescreve

Este é o ponto mais crucial para a regulação antilavagem de dinheiro em relação a Ativos Virtuais, já que a efetividade da execução depende da alocação de responsabilidade. A AMLD5, portanto, intentou definir aqueles que seriam responsáveis por manter o ambiente virtual a salvo de práticas de lavagem de dinheiro e financiamento de terrorismo. Os Recitais 8 e 9 da norma destacam o aparente vazio regulatório no qual serviços de câmbio virtual-para-fiduciário e provedores de custódia de carteira operavam antes da Diretiva, ademais do potencial que a anonimidade provida por essas tecnologias tem para o uso criminoso. Eles foram incluídos no espectro de Entidades Obrigadas (Artigo 2, ponto 3, "g" e "h"). "Prestador de serviços de custódia de carteira" foi definido como "uma entidade que presta serviços de salvaguarda de chaves criptográficas privadas em nome dos seus clientes, com vista a deter, armazenar e transferir moedas virtuais" (Artigo 3, ponto 19).

3.1.2.2. Adequação aos padrões do GAFI

Buscando abordar o problema de quais entidades devem ser reguladas, o GAFI incluiu o conceito de Provedor de Serviços de Ativo Virtual (Virtual Asset Service Provider - VASP) no glossário. É definido por eles como:

> QUALQUER pessoa legal ou natural que não esteja coberta em outro local sob as Recomendações e como empresa conduza uma ou mais das seguintes atividades ou operações para ou em favor de outra pessoa jurídica ou natural:
>
> 1. Câmbio entre ativos virtuais e moedas fiduciárias;
> 2. Câmbio entre uma ou mais formas de ativos virtuais;
> 3. Transferência de ativos virtuais;
> 4. Guarda e/ou administração de ativos virtuais ou instrumentos permitindo controle de ativos virtuais;
> 5. Participação em e provisão de serviços financeiros relacionados a uma oferta e/ou venda de ativo virtual.[70]

Pessoas naturais ou jurídicas podem ser enquadradas como tais se elas se engajarem nessas atividades, não obstante a tecnologia utilizada. O universo de entidades englobado por esta categoria é muito mais amplo que as duas classes de agentes de Ativos Virtuais regulados pela AMLD5. E enquanto as novas adições

70 GAFI. **Glossary U-Z.** Disponível em: https://www.fatf-gafi.org/glossary/u-z/. Accesso em: 15 out. 2019.

ao escopo de aplicação da Diretiva são há muito esperadas[71], eles permanecem restritivos demais para abordar riscos atuais impostos pelo nível de anonimidade e descentralização previamente descritas.

3.1.2.3. Problemas e riscos

Diversos agentes-chave no ecossistema de Ativos Virtuais foram excluídos do escopo da Diretiva: usuários, mineradores, serviços de câmbio que realizam apenas operações virtual-para-virtual, plataformas de troca descentralizada, provedores de software e hardware de carteira, inventores de moedas e *initial coin offerors*[72]. Ainda que algumas dessas exclusões sejam justificáveis (e.g. focar nos usuários não seria proporcional e pode ser tecnicamente impossível regular plataformas descentralizadas), outras podem representar pontos cegos que facilitam lavagem de dinheiro e financiamento de terrorismo se eles permanecerem desregulados e sem supervisão. Se anonimidade e descentralização tornam difícil supervisionar transações com Ativos Virtuais, essas entidades podem atenuar a situação, criando maneiras de identificar e rastrear o beneficiário e os fluxos de transações em muitos casos.

Um problema está na categoria de provedores de serviço de câmbio, que apenas inclui aqueles que lidam com dinheiro fiduciário. Essa inclusão, por si só, é um aprimoramento, pelo qual a Autoridade Bancária Europeia pressionou desde a AMLD4, e foi finalmente contemplada na AMLD5. Mas não é suficiente.

Para ter meios efetivos de prevenção à lavagem de dinheiro e fluxos ilícitos de capital, a ocultação precisa ser levada em conta. Ocultação é o processo pelo qual muitas transações são realizadas de forma a tornar difícil para uma autoridade sinalizar ou rastrear transações suspeitas. Não é o passo final da lavagem de dinheiro, portanto, não necessariamente envolve a conversão para dinheiro fiduciário. É apenas uma maneira de tornar a trajetória do fluxo de capital ilícito impossível de rastrear. Ainda que essa conversão provavelmente vá ocorrer no final da cadeia de transações e seja mais fácil controlar as transações que envolvem dinheiro fiduciário, essas não são as únicas que importam. Trocar por dinheiro fiduciário não é um passo obrigatório, pois esses bens podem ser transferidos para outra jurisdição antes da conversão, ou mesmo usados para compra de bens.

Assim, não são apenas serviços de câmbio que lidam com dinheiro fiduciário

71 O Guia do GAFI de 2015 sobre moedas virtuais defendia uma abordagem centrada em torno da regulação e monitoramento dos pontos de intersecção que proviam portas de entrada para o sistema financeiro regulado, em particular câmbios de moeda virtual conversível. Ver GAFI - Grupo de Ação Financeira Internacional. **Guidance for a Risk-Based Approach to Virtual Currencies** - Convertible Virtual Currency Exchangers. jun. 2015. p. 3. v. 5. Disponível em: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. Acesso em: 14 out. 2019. A Autoridade Bancária Europeia também recomendou incluir câmbios na categoria de Entidades Obrigadas. Ver ASE - Autoridades de Supervisão Europeias (ESA). **Joint Opinion Of The European Supervisory Authorities On The Risks Of Money Laundering And Terrorist Financing Affecting The European Union's Financial Sector**. 2019. Disponível em: https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf?retry=1. Acesso em: 4 out. 2019.

72 HOUBEN; SNYERS, op. cit., 2018, 76-79.

que devem ser Entidades Obrigadas, mas os que também só realizam transações entre moedas virtuais deveriam ser incluídos na lista. Isso é especialmente importante devido a recentes desenvolvimentos no ecossistema de Ativos Virtuais, como o advento de novos produtos e serviços (e.g. Criptomoedas de Anonimidade Elevada, *mixers* e *tumblers*) e o "crescente uso de esquemas de estratificação que intentam ofuscar ainda mais as transações de forma comparativamente fácil, barata e segura"[73]. Nesse cenário, restringir a regulação e supervisão a pontos de estrangulamento entre o sistema financeiro tradicional e o ambiente de Ativos Virtuais não é mais suficiente.

A categoria de provedores de custódia de carteira também deixa lacunas. Primeiramente, não considera provedores de carteira de software ou hardware como Entidades Obrigadas, excluindo-as do ambiente regulado. A diferença entre esses dois formatos de provedor de carteira é que custodiantes têm efetivo controle sobre chaves e senhas para acessar as carteiras dos clientes, como se elas fossem contas no banco e o custodiante fosse o banco. Softwares, por outro lado, são somente aplicativos que clientes acessam em seus dispositivos para gerenciar contas no livro-razão distribuído. Eles têm menos poder sobre seus usuários, pois não pode impor controle sobre transações ou solicitar informação a fim de permitir ao usuário realizá-las. Ainda assim, eles têm a possibilidade de checar a identidade do usuário quando da instalação do aplicativo de controle de carteira. Elas não têm o mesmo nível de controle sobre as transações, mas podem contribuir com identificação do usuário.

Carteiras de hardware, por sua vez, são dispositivos em que usuários podem armazenar suas chaves privadas para maior segurança. Na abordagem do GAFI, os manufatureiros dessas tecnologias não deveriam ser considerados como Povedores de Serviços de Ativos Virtuais porque eles não estão envolvidos em um negócio em uma das cinco atividades previamente mencionadas por ou em benefício de outra pessoa[74]. Entretanto, existe alguma ambiguidade sobre agentes que vendem esses itens porque eles podem ser regulados para coletar e armazenar informação relevante sobre o comprador do dispositivo (o mesmo que quando alguém compra um certificado digital, por exemplo).

3.1.2.4. Abordando as lacunas

Existem duas abordagens possíveis para superar a rigidez de atores do ecossistema de Ativos Virtuais regulados pela AMLD:

1. Adicionar pontos ao Artigo 3, ponto 1, considerando os dois seguintes aspectos: i) o trecho sobre Entidades Obrigadas deveria incluir provedores de software de carteira e câmbios virtual-para-virtual além dos pontos já existentes (provedores de custódia de carteira e câmbios virtual-para-fiduciária); ii) Estados Membros podem adicionar Entidades Obrigadas à lista, de acordo com sua avaliação do risco; há provedores de serviço equivalentes a um

73 GAFI, op. cit., 2019 VA Guidance. p. 6. (item 4).

74 GAFI, op. cit., 2019 VA Guidance. p. 17. (item 48).

negócio de câmbio ou transferência de valores que estão abertos a discussão, como: serviços de Ativo Virtual para contrato de garantia, que permitem substituir o dinheiro fiduciário por esses ativos na transação; ofertantes e emissores, incluindo *initial coin offerors*; serviços de corretagem que facilitam a emissão e troca de Ativos Virtuais em nome dos clientes de uma pessoa jurídica; serviço de câmbio com reserva de pedidos que calcula e reúne pedidos de Ativos Virtuais para compradores e vendedores engajados[75]. Existem agentes que não deveriam ser definidos como Entidades Obrigadas, como usuários e manufatureiros de hardware, porque esse tipo de controle potencialmente inibiria o desenvolvimento e a adoção de novas tecnologias, ou plataformas de transação *peer-to-peer* em que apenas acordos são feitos, mas pessoas envolvidas efetuam transações fora delas.

2. Criar uma categoria de Provedor de Serviço de Ativo Virtual na seção de Entidades Obrigadas da AMLD. O GAFI incluiu essa definição no seu glossário em outubro de 2018. O conceito é amplo o suficiente para ser compatível com uma variedade de sistemas legais e administrativos, neutros em relação às plataformas tecnológicas, e busca manter igualdade de circunstâncias tanto entre Provedores de Serviços de Ativos Virtuais quanto entre eles e outros tipos de Entidades Obrigadas. Se essa segunda abordagem for adotada por uma futura emenda da AMLD, ela substituiria o Artigo 2, ponto 3, pontos g e h, e iria prescrever que uma lista desses serviços considerados Entidades Obrigadas para propósitos de lavagem de dinheiro deveria ser elaborada na regulação europeia pelas Autoridades Europeias de Supervisão ou uma autoridade competente designada. Isso permitiria à Diretiva manter-se a par da inovação e adaptar a mudanças, porque a lista de provedores de serviço seria facilmente atualizada sem a necessidade de fazer emendas à Diretiva, e um corpo de especialistas estaria encarregado de avaliar os riscos.

É importante sublinhar que a regulação via Entidades Obrigadas não é suficiente para assegurar que a anonimidade seria evitada como um todo, já que as transações com Ativos Virtuais podem ser realizadas sem recorrer a qualquer ente centralizador. Uma estratégia possível seria que essas transações e contratos, que não envolvem uma Entidade Obrigada regulada, não fossem exequíveis judicialmente. Ainda que isso não resolva completamente o problema do potencial uso criminal de Ativos Virtuais, é um estímulo para a regularização desse ecossistema.

75 De acordo com seu princípio da neutralidade tecnológica, é relevante à abordagem do GAFI se uma plataforma de comércio é centralizada ou não. Entretanto, conforme notado anteriormente, plataformas descentralizadas de comércio que somente funcionam através de *software* não são providas por uma pessoa singular, natural ou jurídica, que poderia ser responsabilizada, portanto, não é factível executar regulações aplicáveis a elas.

3.1.3. Abordagem Baseada em Risco

3.1.3.1. O que a AMLD5 prescreve

Como dito anteriormente, uma abordagem baseada em risco consiste em um conjunto mais flexível de medidas que pode abordar risco de forma proporcional, bem como adaptar regulações conforme mudanças tecnológicas são implementadas. A fim de ser efetiva, países e jurisdições precisam fomentar a identificação de riscos potenciais de novos dispositivos tecnológicos. Buscando adotar essa abordagem, a AMLD declara, em sua seção de avaliação de risco, que a Comissão deve avaliar riscos de lavagem de dinheiro e financiamento de terrorismo afetando mercado interno e atividades transfronteiriças (Artigo 6, ponto 1), incluindo riscos associados com: áreas de mercado interno de maior risco, cada setor relevante, e os principais meios usados por criminosos para cometer lavagem de dinheiro (ponto 2). A Comissão deve também aconselhar Estados Membros sobre como abordar esses riscos adequadamente (ponto 4).

Estados Membros devem também avaliar e mitigar riscos "bem como quaisquer preocupações conexas em matéria de proteção de dados"[76] (Artigo 7, ponto 1). Essas avaliações devem ser mantidas atualizadas e identificar setores ou áreas de maior risco, bem como campos para Entidades Obrigadas aplicarem medidas antilavagem de dinheiro e aplicarem medidas para combater o financiamento do terrorismo (ponto 4). Seus resultados devem auxiliar Estados Membros na alocação de recursos e estabelecimento de regras para cada setor ou área de acordo com seu nível de risco.

Estados Membros também são obrigados a certificar-se de que Entidades Obrigadas ajam em proporção ao seu tamanho e natureza, para identificar lavagem de dinheiro e financiamento de terrorismo (Artigo 8), considerando fatores como "os associados aos seus clientes, a países ou zonas geográficas, produtos, serviços, operações ou canais de distribuição"[77] (ponto 1). Essas entidades devem também ser obrigadas a ter políticas, controles e procedimentos efetivos em curso para reduzir riscos, incluir Devida Diligência do Cliente, Relatório de Transações Suspeitas, guarda de registros, controles internos, e, quando apropriado, um responsável pelo gerenciamento de conformidade e uma função de auditoria independente (ponto 4).

3.1.3.2. Adequação às diretrizes do GAFI

Em termos amplos, isso é consistente com as avaliações de risco nacionais coordenadas, defendidas pelo GAFI[78]. Enquanto o trecho sobre dados pessoais é vagamente descrito, pode ser facilmente interpretado como um requisito para que Países Membros harmonizem seus regimes antilavagem de dinheiro e seus regimes de combate ao financiamento de terrorismo com as normas de privacidade e proteção de dados, especialmente à luz de diversas outras referências à obrigação

76 União Europeia, op. cit., 2018, AMLD5, Artigo 7, ponto 1.

77 União Europeia, op. cit., 2018, AMLD5, Artigo 8, paragraph 1.

78 GAFI, op. cit. VA Guidance, 2019 p. 19. (item 60).

contidas na Diretiva[79].

As previsões do Artigo 8 também são adequadas na medida em que refletem preocupações em tornar não somente Estados Membros mas também entidades do setor privado participantes ativos na implementação da Abordagem Baseada em Risco de uma maneira adequada e proporcional.

3.1.3.3. Problemas e riscos

Um problema que emerge, possivelmente devido à natureza[80] e à estrutura[81] da Diretiva, é que provisões mais específicas sugeridas pelo GAFI não são implementadas. Por exemplo, aquela de produzir uma avaliação de risco que expressamente permita aos países entender "como produtos e serviços específicos de VA funcionam, se enquadram e afetam todas as jurisdições relevantes para os propósitos de antilavagem de dinheiro e combate ao financiamento de terrorismo (e.g. mecanismos de pagamento e transferência de valores, quiosques de VA, commodities de VA, valores mobiliários de VA ou atividades relacionadas, etc. [...]) [82]. A ausência de obrigação para realizar avaliação de risco funciona como um obstáculo para discutir quais Provedores de Serviços de Ativos Virtuais deveriam ser mais intensivamente regulados de maneira informada.

Países deveriam estar aptos a discriminar entre níveis de risco no setor de Ativos Virtuais para que eles possam priorizar áreas específicas (i.e. Criptomoedas de Anonimidade Elevada e mixers ou serviços que apenas facilitem virtual-para-virtual). Essa granularidade é necessária mesmo se o país escolher classificar o setor inteiro de Ativos Virtuais como de alto risco[83]. Uma abordagem como essa é fundamental para abordar diferentes agentes de maneira proporcional e efetiva, permitindo melhor alocação de recursos de monitoramento. Isso tornaria possível às autoridades priorizarem provedores de serviço com alto nível de risco baseado em seus perfis de negócios e outras características, como aquelas que realizam transações à distância e não lidam com dinheiro fiduciário.

3.1.3.4. Abordando as lacunas

Uma possível solução a essa questão seria incluir uma previsão no Artigo 6 para que países obriguem as autoridades nacionais a identificar não somente os riscos associados com cada setor, mas áreas subsetoriais que sejam sujeitas a alto nível de risco. Isso permitiria melhor alocação de recursos de monitoramento, porque seria possível concentrar esforços em serviços que sejam de maior risco, de acordo com sua propensão a servir como instrumento de lavagem de dinheiro ou financiamento terrorista naquele Estado Membro. Isso produziria informação

79 Ver União Europeia, op. cit., 2018, Considerandos 28, 36, 38, e 46. Ver também AMLD5, Artigo 30, ponto 5, Artigo 31, pontos 4, 9, Artigo 39, ponto 5, Artigo 43, Artigo 45, ponto 1, 3, 4, Artigo 46, ponto 1, Artigo 48, ponto 2, and Artigo 60, ponto 3.

80 Uma regulação possivelmente teria maior detalhamento acerca de sua implementação.

81 A Seção II, que concerne à avaliação do risco, refere-se à Entidades Obrigadas amplamente, não a subcategorias específicas delas.

82 GAFI, op. cit. VA Guidance, 2019 p. 19. (item 60).

83 GAFI, op. cit. VA Guidance, 2019 p. 36. (item 151).

mais acurada e facilitaria o estabelecimento de serviços que não representem alto risco dentro do setor. É necessária, portanto, uma avaliação pelos co-legisladores europeus a fim de verificar se isso realmente resulta em uso mais eficiente dos recursos.

3.1.4. Registro e monitoramento

3.1.4.1. O que a AMLD5 prescreve

Estados Membros devem certificar-se que provedores de custódia de carteira e câmbios virtual-fiduciário sejam registrados (Artigo 47, ponto 1), e autoridades competentes sejam obrigadas a assegurar que a equipe de gerência ou o beneficiário final sejam "competentes e idôneos" (ponto 2).

Estados Membros são obrigados a garantir poderes e recursos adequados para as autoridades competentes realizarem suas tarefas, incluindo aquela de compelir a produção de informação que é relevante para monitorar observância e realizar checagens (Artigo 48, ponto 2).

Isso é expandido no Artigo 58, que reafirma que as autoridades devem ter todos os poderes investigativos e supervisores necessários para o exercício de suas funções, como aquela de imposição de sanções e medidas administrativas[84] (ponto 1) a Entidades Obrigadas que estejam em desacordo. Da mesma forma, o Artigo 59, ponto 2, define um espectro de sanções e medidas dissuasivas, efetivas e proporcionais aplicáveis em caso de descumprimento, inclusive retirada ou suspensão da autorização da entidade para operar (ponto c) e banimento temporário das pessoas naturais responsáveis pela falha (ponto d).

3.1.4.2. Adequação às diretrizes do GAFI

A exigência de registro está alinhada com o padrão mínimo do GAFI que Provedores de Serviço de Ativo Virtual sejam registrados e licenciados na jurisdição onde foram criados, se elas forem uma pessoa jurídica[85]. A segunda provisão está de acordo com a instrução do GAFI para que os países adotem medidas para evitar que criminosos e seus associados tenham uma posição de gerência ou controle, ou sejam o beneficiário final, de um lucro significativo nesse tipo de negócio.

Entretanto, as recomendações do GAFI de que essas medidas necessariamente incluem a exigência de que essas entidades "'busquem prévia aprovação dessas autoridades para mudanças substantivas em acionistas, operações de negócios e estruturas[86]. Similarmente, autoridades devem ser obrigadas a criar critérios específicos para esses agentes serem registrados. Esses critérios devem idealmente incluir ter um diretor executivo residente, e presença substantiva da gerência, na

84 No Artigo 58 da AMLD5, Estados Membros não são obrigados a conceder poder às autoridades de impor sanções criminais em caso de violação. Alinhado com esta provisão, o ponto 2 permite aos Estados Membros não definir regras para sanções ou medidas sujeitas a sanções criminais na lei nacional. No entanto, eles devem certificar-se de que autoridades que tomem conhecimento de violações sejam obrigados a informar autoridades legais de maneira ágil.

85 GAFI, op. cit. VA Guidance, 2019. p. 22 (item 78).

86 GAFI, op. cit. VA Guidance, 2019. p. 23. (item 83).

jurisdição do registro[87], dependendo da natureza e tamanho da entidade.

As provisões concernentes a poderes e deveres das autoridades estão geralmente de acordo com as diretrizes do GAFI[88] para poderes, recursos e obrigações de autoridades em relação a Provedores de Serviços de Ativos Virtuais.

3.1.4.3. Problemas e riscos

A falta de requisitos mais específicos pode levar à implementação inconsistente de requerimentos de registro no nível nacional, o que pode resultar em diferenças substanciais entre regimes regulatórios de Estados Membros. Isso é uma questão devido ao funcionamento decentralizado dos fluxos de Ativos Virtuais, em que usuários e serviços podem se distribuir através de diferentes países e a transação realizada por um serviço pode acabar envolvendo outro, que não é obrigado a registrar-se e, portanto, não está submetido ao mesmo nível de controle, de forma que uma análise caso a caso se torna obrigatória a fim de calcular o risco. Similarmente, a exigência que a gerência e o beneficiário final sejam "aptos e adequados" pode ser aplicada de maneira frouxa na ausência de mudanças significativas na estrutura condicional à aprovação prévia de autoridades.

3.1.4.4. Abordando as lacunas

O Artigo 47 deve ser emendado para requerer que Estados Membros exijam que Entidades Obrigadas a buscar aprovação prévia de autoridades antes de realizar mudanças substanciais em operações de negócios, sócios e estruturas. O registro deveria ser uma condição de funcionamento. Deve ser estabelecido um conjunto mínimo de critérios ao qual os Provedores de Serviços de Ativos Virtuais devem atender a fim de ser registrado. Esses critérios devem incluir, ao menos, a presença de gerência substantiva e um diretor executivo residente para permitir o cumprimento da lei e monitoramento do negócio pelas autoridades locais. Além disso, para fazer transações envolvendo um provedor de serviços não-registrado em outro país, deveria ser obrigatório realizar uma avaliação de risco da transação. Deveria ser explícito que isto é em proporção ao tamanho e natureza do Provedor de Serviços de Ativos Virtuais para que isso não represente um obstáculo a essas tecnologias ou leve à alocação ineficiente de recursos pelo setor público.

3.1.5. Controles internos

3.1.5.1. O que a AMLD5 prescreve

Requisitos para controles internos são dispostos na AMLD5 nos Artigos 45 e 46. O Artigo 45 requer que Entidades Obrigadas "que fazem parte de um grupo apliquem políticas e procedimentos a nível do grupo, nomeadamente políticas em matéria de proteção de dados e políticas e procedimentos de partilha de informações no âmbito do grupo, para efeitos de ABC/CFT [anti branqueamento de

87 GAFI, op. cit. VA Guidance, 2019. p. 23. (item 80).

88 GAFI, op. cit. VA Guidance, 2019. p. 24. (item 86).

capitais/combate ao financiamento do terrorismo]. Essas políticas e procedimentos são aplicados de forma eficaz a nível das sucursais e das filiais participantes majoritariamente situadas nos Estados-Membros e em países terceiros" (ponto 1). Quando Entidades Obrigadas tiverem filiais ou subsidiárias majoritárias operando em países terceiros com requerimentos antilavagem de dinheiro e requerimentos para combate ao financiamento do terrorismo que forem menos rígidos que aqueles dos Estados Membros, aquelas filiais e subsidiárias devem observar os padrões do Estado Membro (ponto 3). Isto, é claro, é limitado pela extensão permitida pela lei do país terceiro. Mas quando as leis de países terceiros não permitirem essa implementação, Estados Membros e Autoridades Europeias de Supervisão devem informar uma à outra (ponto 4).

Caso as leis do país terceiro não permitam a implementação de medidas de controle interno conforme descrito no ponto 1, a Entidade Obrigada deve aplicar medidas adicionais para lidar com o risco. E, na extensão em que as medidas forem ineficientes, autoridades competentes devem fazer supervisão adicional, incluindo pedido para que atividades em países terceiros sejam encerradas quando necessário.

O ponto 9 prescreve que Estados Membros podem requerer aos emissores de dinheiro eletrônico e provedores de serviços de pagamento estabelecidos no seu território em formas diversas de filial, e cuja sede está localizada em outro Estado Membro, que apontem um ponto de contato central em seu território para assegurar, em nome da instituição designada, compliance com regras antilavagem de dinheiro e combate ao financiamento de terrorismo, e para facilitar supervisão por autoridades competentes, incluindo a provisão de documentos e informação sobre o pedido às autoridades competentes[89]. Essa definição não incluiria Provedores de Serviços de Ativos Virtuais, já que eles não são concebidos conceitualmente como instituições financeiras ou de crédito para os propósitos de combate à lavagem de dinheiro e financiamento de terrorismo, ainda que suas atividades sejam, algumas vezes, muito similares àquelas realizadas por tais entidades - como câmbio, transferência e gerenciamento de valores que podem ser usados como pagamento.

O Artigo 46, por outro lado, requer que Entidades Obrigadas adotem medidas para que seus empregados estejam cientes das provisões estabelecidas pela AMLD5, que podem incluir empregados participando de programas especiais de treinamento. Estados Membros também são responsáveis por certificar que Entidades Obrigadas tenham informação atualizada das práticas de lavagem de dinheiro e financiamento de terrorismo. Também prevê que Entidades Obrigadas devem identificar um membro, no nível de gerência, que seja responsável por implementar as medidas necessárias para observância da AMLD5.

3.1.5.2. Adequação às diretrizes do GAFI

A recomendação 18 do GAFI advoga que países assegurem que Provedores de Serviços de Ativos Virtuais que são parte de um grupo estejam adotando as medidas adequadas para realizar controle interno, seja doméstico ou no exterior, em suas filiais ou subsidiárias majoritárias. Especificamente, argumenta que os controles

89 União Europeia, AMLD 5, op. cit, p. 47

internos devem incluir: (1) responsabilidades por combate lavagem de dinheiro e financiamento de terrorismo claramente alocadas no nível de gerenciamento, (2) controles para monitorar a integridade da equipe e (3) controles de auditoria independente.

Em uma perspectiva ampla, os requisitos de controles internos da AML5 estão de acordo com as recomendações do GAFI. No entanto, seria interessante incluir Provedores de Serviço de Ativos Virtuais no artigo 45, ponto 9, já que eles não são enquadrados nas definições de e-money e serviços de pagamentos.

3.1.5.3. Problemas e riscos

A ausência de obrigação aos Provedores de Serviço de Ativos Virtuais em relação a apontar uma pessoa central de contato encarregada de compliance, em filiais ou subsidiárias majoritárias que estão localizadas em outro Estado Membro, pode causar dificuldades para monitoramento e supervisão por autoridades competentes. É importante, para assegurar a observância, que a informação sobre registros, transações e toda a documentação sobre compliance de uma filial ou subsidiária seja de fácil acesso às autoridades do Estado Membro da sede.

3.1.5.4. Abordando as lacunas

Para assegurar que filiais ou subsidiárias de Provedores de Serviços de Ativos Virtuais observem a AMLD no Estado da sede, elas devem ser listadas ao lado das instituições financeiras no Artigo 45, ponto 9, junto com serviços de pagamento e câmbio. Como suas funções são essencialmente as mesmas das instituições financeiras, eles também devem ser responsáveis por conformidade regional e cooperação com autoridades.

3.2. Aspectos que estão adequados quando confrontados com as diretrizes do GAFI

3.2.1. Devida Diligência com o Cliente

Os Artigos 10-24 da AMLD5 dizem respeito a medidas de Devida Diligência com o Cliente, incluindo e mantendo aspectos recomendados que contribuem para o controle de lavagem de dinheiro e financiamento do terrorismo envolvendo Ativos Virtuais, como quais transações precisam de monitoramento, como a devida diligência pode ser feita, casos especiais em que devida diligência avançada ou simplificada se aplica, diretrizes para avaliação de risco, regras para países terceiros de alto risco e a proibição de anonimato em contas para instituições financeiras ou de crédito, assim como para entidades com as quais elas fazem negócios. Eles estão, em geral, de acordo com as diretrizes do GAFI sobre Devida Diligência com o Cliente, o que compreende as Recomendações 10-13, 17 e 19, que envolvem avaliação de risco para países e atividades, negócios e transações ocasionais acima do limite para Ativos Virtuais, procedimentos para devida diligência avançada ou simplificada, dever de reportar situações suspeitas, verificação de identidade de beneficiário final, guarda de registros e supervisão e monitoramento de transações. Essas medidas

podem ser consideradas suficientes, pois os Provedores de Serviços de Ativos Virtuais, conquanto estejam listados corretamente como Entidades Obrigadas, não inovam quanto à necessidade de checagem do cliente.

3.2.2. Relatório de Transações Suspeitas

Na Seção sobre Relatórios de Transações Suspeitas (Capítulo IV), a AMLD5 incluiu a obrigação de reportar, para além das transações suspeitas de financiamento terrorista ou lavagem de dinheiro, também tentativas de transação, assim como a obrigação de prover Unidades de Inteligência Financeira com toda informação necessária. Também prescreve que países devem exigir que Entidades Obrigadas não prossigam com a transação quando suspeita até receber avisos e instruções da Unidade de Inteligência Financeira, a não ser que isso seja impossível ou sabidamente resulte em tornar impossível identificar o beneficiário, caso no qual elas devem comunicar sobre isso à unidade imediatamente após a transação. Assim, a diretiva está adequada às recomendações do GAFI no que tange a Relatório de Transação Suspeita. Com os Provedores de Serviços de Ativos Virtuais listados corretamente como Entidades Obrigadas, é possível à Unidade de Inteligência Financeira identificar o beneficiário em transações realizadas através deles.

3.2.3. Guarda de registros

Entidades Obrigadas devem manter um registro de documentos e informações para os propósitos de investigar, detectar e prevenir financiamento de terrorismo e lavagem de dinheiro por Unidades de Inteligência Financeira ou outras autoridades competentes por um período de cinco anos depois do fim da relação comercial com seus clientes ou depois da data de uma transação ocasional (Artigo 40, ponto 1). A documentação e informação que deve ser mantida é (1) aquela necessária a adequar-se a obrigações de Devida Diligência ao Cliente e (2) a evidência que comprova as transações. Ambas devem ser mantidas em um formato aceitável sob procedimentos judiciais de acordo com a lei nacional, sejam originais ou cópias. Quando o período de retenção expira, Estados Membros podem também permitir ou solicitar um período maior que cinco anos, desde que uma avaliação da necessidade e proporcionalidade disso seja feita. Finalmente, Estados Membros devem assegurar que dados pessoais sejam deletados depois do fim do período de guarda obrigatória, a não ser que a lei nacional prescreva de forma diversa sobre o assunto.

O GAFI recomenda que países se certifiquem de que todos os registros de transações sejam mantidos por ao menos cinco anos (Recomendação 11). Eles aconselham que informações sejam mantidas acerca de identificação de partes relevantes, chaves públicas (ou identificadores equivalentes), endereços ou contas envolvidas (ou identificadores equivalentes), a natureza e data da transação e a quantia transferida[90]. Nesse sentido, desde que a Devida Diligência do Cliente esteja em conformidade, também estarão as recomendações sobre guarda de registros.

90 GAFI op. cit. Recommendations, p. 27

Considerações finais

Este relatório buscou contribuir para o framework regulatório para Ativos Virtuais na UE em relação aos riscos que esses serviços agregam em relação à lavagem de dinheiro e ao financiamento terrorista. Algumas das questões recentemente foram reconhecidas pela principal entidade supervisora na área, o GAFI, e ainda precisam ser incorporadas na AMLD. Os pontos principais que devem ser abordados de acordo com nossas recomendações são:

- O conceito de propriedade deve ser incorporado na definição de financiamento terrorista, já que a definição de fundos não engloba Ativos Virtuais.
- O termo Moeda Virtual deve ser substituído por Ativo Virtual.
- Uma das seguintes abordagens deve ser adotada para tornar o escopo de Entidades Obrigadas adequado: 1) incluir uma categoria de Provedores de Serviços de Ativos Virtuais, listada pelas Autoridades de Supervisão Europeia, ou 2) incluir câmbios virtual-para-virtual e provedores de software de wallet, e deixar aberto para cada Estado Membro adicionar Provedores de Serviços de Ativos Virtuais de acordo com sua avaliação de risco.
- Contratos que não envolvem Entidades Obrigadas devem ser sem validade jurídica.
- Estados Membros devem ser obrigados a compelir autoridades nacionais a identificar áreas subsetoriais sujeitas a nível maior de risco no setor de ativos virtuais.
- Entidades obrigadas devem ser compelidas a buscar autorização para mudanças substanciais em operações de negócios, sócios e estruturas.
- Requisitos de registro devem ser uma condição para operar e devem incluir, ao menos, ter gerenciamento substantivo e um diretor executivo localmente residente.
- Incluir assistência de extradição explicitamente entre as medidas padrão para cooperação internacional em lavagem de dinheiro relacionadas a ativos virtuais e investigações criminais de financiamento do terrorismo.
- Provedores de Serviços de Ativos Virtuais devem ser listados em paridade com instituições financeiras no artigo 45, ponto 9, junto com serviços de pagamento e câmbio.

Ao fazer os ajustes considerando os pontos e sugestões aqui apresentados, será possível abordar as principais lacunas dos atuais padrões normativos sobre Ativos Virtuais. Dessa forma, a AMLD incorporará uma Abordagem Baseada em Risco mais efetiva para combater a lavagem de dinheiro e o financiamento ao terrorismo, adequando novos atores do ecossistema econômico e novas possibilidades a um ambiente de direitos e monitoramento, que pode ser adaptado de acordo com novos avanços tecnológicos e seu uso para transações.

Referências

ABE - Autoridade Bancária Europeia. **EBA's Opinion on virtual currency**. 4 julho 2014. Disponível em: https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf. Acesso em: 14 out. 2019.

ABE - Autoridade Bancária Europeia. **Report with advice for the European Commission on Crypto-Assets.** 2019. Disponível em: https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1. Acesso em: 14 nov. 2019.

ASE - Autoridades de Supervisão Europeias (ESA). **Joint Opinion Of The European Supervisory Authorities On The Risks Of Money Laundering And Terrorist Financing Affecting The European Union's Financial Sector**. 2019. Disponível em: https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf?retry=1. Acesso em: 4 out. 2019.

BANCO DE COMPENSAÇÕES INTERNACIONAIS. **Cryptocurrencies**: looking beyond the hype. BIS Annual Economic Report 2018.

CAMPBELL-VERDUYN, M.; GOGUEN, M. The mutual constitution of technology and global governance: Bitcoin, blockchains, and the international anti-money-laundering regime. In: CAMPBELL-VERDUYN, M. (org.). **Bitcoin and Beyond:** Cryptocurrencies, Blockchains and Global Governance. New York: Routledge, 2018. p. 69-87.

CAMPBELL-VERDUYN, M. Bitcoin, crypto-coins, and global anti-money laundering governance. **Crime, Law and Social Change**, v. 69, n. 2, 283–305, mar. 2018. p. 286

CHOHAN, U. W. **Initial Coin Offerings (ICOs)**: Risks, Regulation, and Accountability. SSRN Electronic Journal, [s.l.], p.1-6, 2017.

CHOO, K. R. Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks?. In: CHUEN, David Lee K. (ed.) **Handbook of digital currency**: Bitcoin, Innovation, Financial Instruments, and Big Data. Academic Press, 2015. pp. 283-306.

CŒURÉ, B. **Communiquée released by the Chair of the G7 working group on stablecoins**, Benoît Cœuré. 2019. Disponível em: https://www.bis.org/cpmi/speeches/sp190718.html. Accesso em: 17 out. 2019.

COINMARKETCAP. **Capitalisation**. Disponível em: https://coinmarketcap.com Acesso em: 14 out. 2019.

COINMARKETCAP. **Global Charts**. 2019. Disponível em: https://coinmarketcap.com/charts/. Accesso em: 16 nov. 2019.

UNIÃO EUROPEIA. Conselho Europeu. **Convenção Europeia de Extradição**. 1957. Disponível em: https://rm.coe.int/168096525e. Acesso em: 22 nov. 2019.

DASH. **Dash 101** - 7 What is PrivateSend? 2018. Disponível em: https://www.youtube.com/watch?v=v_HwQAyIQns. Acesso em: 18 nov. 2019.

DION-SCHWARZ, C., MANHEIM, D., & JOHNSTON, P. B. **Terrorist Use of Cryptocurrencies:** Technical and Organizational Barriers and Future Threats. Rand Corporation, 2019.

AEVM - Autoridade Europeia dos Valores Mobiliários e dos Mercados. **Advice on Initial Coin Offerings and Crypto-Assets**. Disponível em: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf. Acesso em: 14 nov. 2019.

EUROPOL - Serviço Europeu de Polícia. **Illegal network used cryptocurrencies and credit cards to launder more than eur 8 million from drug trafficking**. 09 abr. 2018a. Disponível em: https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking. Acesso em: 19 nov. 2019.

EUROPOL. **Massive blow to criminal dark web activities after globally coordinated operation**. 20 jul. 2017. Disponível em: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation. Acesso em: 19 nov. 2019.

EUROPOL. **Multi-million euro cryptocurrency laundering service bestmixer.io taken down**. 2019. Disponível em: https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down. Acesso em: 18 nov. 2019.

EUROPOL. **Two criminal groups dismantled for laundering eur 2.5 million through smurfing and cryptocurrencies.** 11 jul. 2018b. Disponível em: https://www.europol.europa.eu/newsroom/news/two-criminal-groups-dismantled-for-laundering-eur-25-million-through-smurfing-and-cryptocurrencies. Acesso em: 19 nov. 2019.

FORREST, Brett. Jihadists See a Funding Boon in Bitcoin. **The Wall Street Journal**. 20 Feb. 2018. Disponível em: https://www.wsj.com/articles/jihadists-see-

a-funding-boon-in-bitcoin-1519131601. Acesso em: 19 nov. 2019.

G20, **The Global Plan for Recovery and Reform**, Final Communique of the G20 Summit Held in London on 2 abr. 2009. Disponível em: http://www.g20.utoronto.ca/2009/2009communique0402.pdf. Acesso em: 16 out. 2019.

GAFI - Grupo de Ação Financeira Internacional. **Frequently Asked Questions**. 2019. Disponível em: http://www.fatf-gafi.org/faq/moneylaundering/. Acesso em: 16 out. 2019.

GAFI - Grupo de Ação **Financeira Internacional, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation**, 2019. FATF, Paris, France. Disponível em: www.fatf-gafi.org/recommendations.html. Acesso em: 29 out. 2019.

GAFI - Grupo de Ação Financeira Internacional. **Glossary U-Z**. 2019. Disponível em: https://www.fatf-gafi.org/glossary/u-z/. Acesso em: 15 out. 2019.

GAFI - Grupo de Ação Financeira Internacional. **Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers**. 2019. Disponível em: https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf. Acesso em: 19 nov. 2019.

GAFI - Grupo de Ação Financeira Internacional. **Guidance for a Risk-Based Approach to Virtual Currencies** - Convertible Virtual Currency Exchangers. jun. 2015. p. 3. v. 5. Disponível em: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. Acesso em: 14 out. 2019.

GAFI - Grupo de Ação Financeira Internacional. **Public Statement:** Mitigating Risks from Virtual Assets. 2019. Disponível em: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html. Acesso em: 18 nov. 2019.

GAFI - Grupo de Ação Financeira Internacional. **Virtual Currencies** - Key Definitions and Potential AML/CFT Risks. jun. 2014. Disponível em: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Acesso em: 12 dez. 2019.

GERARD, David. Neo-Nazis Bet Big on Bitcoin (And Lost). 19 mar. 2019. **Foreign Policy**. 2019. Disponível em: https://foreignpolicy.com/2019/03/19/neo-nazis-banked-on-bitcoin-cryptocurrency-farright-christchurch/. Acesso em: 19 nov. 2019.

GOLDBERG, Dror. Legal Tender. **SSRN Electronic Journal**, [sl], p.1-17, 2008. Elsevier BV.

HADZIEVA, E. **Impact of Digitalisation on International Tax Matters**: challenges and remedies. Policy Department for Economic, Scientific and Quality of Life Policies. European Parliament: Luxembourg, 2019. Disponível em: https://www.europarl.europa.eu/cmsdata/161104/ST%20Impact%20of%20Digitalisation%20publication.pdf Acesso em: 16 out. 2019.

HAKELBERG, L. **Redistributive tax co-operation:** automatic exchange of information, US power and the absence of joint gains. 2016.

HOUBEN, R.; SNYERS, A. **Cryptocurrencies and blockchain**: Legal context and implications for financial crime, money laundering and tax evasion. Study requested by the Tax3 committee of the Policy Department for Economic, Scientific and Quality of Life Policies European Parliament. European Union: Brussels, July 2018. Disponível em: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf. Acesso em: 14 out. 2019.

HÜTTEN, M., & THIEMANN, M. Moneys at the margins: From political experiment to cashless societies. In: CAMPBELL-VERDUYN, M. (org.). **Bitcoin and Beyond:** Cryptocurrencies, Blockchains and Global Governance. New York: Routledge, 2018.

KRUGMAN, P. Bitcoin is evil. **The New York Times**, v. 28. 2013.

KRUGMAN, P. Bubble, bubble, fraud and trouble. **The New York Times**. 2018. Disponível em: https://www.nytimes.com/2018/01/29/opinion/bitcoin-bubble-fraud.html. Acesso em: 23 out. 2019.

MARIAN, O. Are cryptocurrencies super tax havens. **Mich. L. Rev. First Impressions**, 112, 38, 2013.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. **Satoshi Nakamoto Institute**. 2008. Disponível em: https://nakamotoinstitute.org/bitcoin/ Acesso em: 12 nov. 2019.

O'BRIEN, L. Who Gave Neo-Nazi Publisher Andrew Anglin A Large Bitcoin Donation After Charlottesville? **Huffpost**. 12 jun. 2019. Disponível em: https://www.huffpostbrasil.com/entry/andrew-anglin-bitcoin-mysterious-donor_n_5d011cc6e4b0304a12087e0c?ri18n=true. Acesso em: 19 Nov. 2019

OZELLI, S. 'Virtual Drivers of Real Economic Growth: The EU's Complex Tax Policy Strategy'. **Tax Management International Journal** (in Bloomberg Tax), v. 47 n. 452, 2018.

POPPER, N. Terrorists Turn to Bitcoin for Funding, and They're Learning Fast. **The New York Times**. 18 ago. 2019. Disponível em: https://www.nytimes.

com/2019/08/18/technology/terrorists-bitcoin.html?. Acesso em: 19 nov. 2019.

RODRIGUES, G; KURTZ, L.. **Criptomoedas e regulação antilavagem de dinheiro no G20.** Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2019. Disponível em: http://bit.ly/2m9pOz0 Acesso em: 12 nov. 2019.

SWARTZ, L. What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. **Cultural Studies**, v. 32, n. 4, 2018. p. 623-650.

TWITTER. **Neonazi BTC Tracker**. 2019. Disponível em: https://twitter.com/NeonaziWallets. Acesso em: 19 nov. 2019.

UNIÃO EUROPEIA. Conselho da União Europeia e da Comissão Europeia. **Joint Statement on stablecoins**. 2019. Disponível em: https://bit.ly/2WQs3GL Acesso em: 5 dez. 2019.

UNIÃO EUROPEIA. Conselho Europeu. **Diretiva (UE) 2016/2258 do Conselho, de 6 de dezembro de 2016, que altera a Diretiva 2011/16/UE no que respeita ao acesso às informações antibranqueamento de capitais por parte das autoridades fiscais**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L2258&from=EN Acesso em: 21 nov. 2019.

UNIÃO EUROPEIA. Parlamento Europeu. AMLD5. **Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho de 30 de maio de 2018 que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE** (Texto relevante para efeitos do EEE). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843. Acesso em: 19 nov. 2019.

UNIÃO EUROPEIA. Parlamento Europeu. **Diretiva (UE) 2018/1673 do Parlamento Europeu e do Conselho de 23 de outubro de 2018 relativa ao combate ao branqueamento de capitais através do direito penal**. 23 out. 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32018L1673&from=PT. Acesso em: 22 nov. 2019.

UNIÃO EUROPEIA. Parlamento Europeu. **Relatório sobre a proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera a Diretiva 2009/101/CE. 9 de março de 2017**. Comissão dos Assuntos Económicos e Monetários. Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos. Disponível em: https://www.europarl.europa.eu/doceo/document/A-8-2017-0056_PT.html. Acesso em: 19 nov. 2019

VANDEZANDE, Niels. **Virtual currencies under EU anti-money laundering law. Computer law & security review**, v. 33, n. 3, p. 341-353, 2017.

WEISER, B. Ross Ulbricht, creator of Silk Road website, is sentenced to life in prison. **The New York Times**. 29 Maio 2015. Disponível em: https://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html Acesso em: 12 dez. 2019.

iris