O BRANQUEAMENTO DE CAPITAIS COM RECURSO A CRIPTOATIVOS

Ângela Coutinho Da Costa

Orientação: Professor Doutor Paulo de Sousa Mendes

Mestrado em Direito e Prática Jurídica
Especialidade: Direito Penal

2023

Advertências

Na redação da presente dissertação:

I. Todas as citações de trechos são realizadas em português, mediante tradução livre.

II. As expressões ou palavras em língua estrangeira serão destacadas mediante a utilização de *itálico*.

III. Foram observadas as regras do novo Acordo Ortográfico, no entanto, as citações bibliográficas e transcrições foram reproduzidas com respeito pela ortografia utilizada pelos autores aquando do momento da publicação das suas obras.

Agradecimentos

Aos meus pais, irmão e namorado, por todo o amor, carinho, preocupação e apoio, sempre.

Resumo

Este trabalho visa analisar a temática da prática do crime de branqueamento de capitais com recurso a criptoativos. Para tanto, efetuou-se uma abordagem estruturada e analítica, fornecendo um enquadramento conceptual, nomeadamente no que diz respeito à origem e natureza dos criptoativos e das formas através das quais podem estes ser utilizados para a prática do crime. Foi feita, ainda, uma análise das legislações europeia e norte-americana relacionadas com o branqueamento de capitais, com especial enfoque nas disposições que se aplicam aos criptoativos, com o intuito de aferir da sua adequação e suficiência na prevenção e repressão do crime de branqueamento de capitais através da utilização deste fenómeno tecnológico e financeiro.

Palavras-Chave: Criptoativos; Branqueamento de Capitais; Blockchain; Descentralização; Anonimato.

Abstract

This work aims to analyze the practice of money laundering with the use of cryptoassets. To this end, a structured and analytical approach was carried out, providing a conceptual framework, namely with regard to the origin and nature of cryptoassets and the ways in which they can be used to commit the crime. An analysis was also made of the European and North American legislation related to money laundering, with a special focus on the provisions that apply to cryptoassets, in order to assess their adequacy and sufficiency in the prevention and repression of money laundering crime through the use of this technological and financial phenomenon.

Keywords: Cryptoassets; Money Laundering; Blockchain; Decentralization; Anonymity.

Glossário de Abreviaturas e Siglas

AML – *Anti Money Laundering* (em português: antibranqueamento de capitais)

BCE – Banco Central Europeu

CASP (ou VASP) - *Crypto Asset Service Provider* ou *Virtual Asset Service Provider* (em português: prestador de serviços de criptoativos ou prestador de serviços de ativos virtuais)

CE – Comissão Europeia

CHF – *Cryptographic Hash Functions* (em português: funções *hash* criptográficas)

CP – Código Penal

CPU – *Central Processing Unit* (em português: unidade central de processamento)

CFTC - *Commodity Futures Trading Commission* (em português: Comissão de Negociação de Contratos Futuros de Commodities)

DLT - *Distributed Ledger Technology* (em português: tecnologia de registo distribuído)

DOJ – *Department of Justice* (em português: Departamento de Justiça dos Estados Unidos)

EBA – *European Banking Authority* (em português: Autoridade Bancária Europeia)

EM – Estado-Membro

ESMA - *European Securities and Markets Authority* (em português: Autoridade Europeia dos Valores Mobiliários e dos Mercados)

EUA – Estados Unidos da América

FAFT – *Financial Action Task Force* (em português: GAFI - Grupo de Ação Financeira Internacional)

FBI – *Federal Bureau of Investigation* (em português, Departamento Federal de Investigação)

FinCen - *Financial Crimes Enforcement Network* (em português: Rede de Repressão aos Crimes Financeiros)

ICO – *Inicial Coin Offering* (em português: oferta inicial de moedas)

KYC - *Know-Your-Customer* (em português: conheça o seu cliente)

MiCA - Markets in Cryptoassets (em português: Mercados em Criptoativos)

P2P – *Peer-to-peer* (em português: par a par)

PIB – Produto Interno Bruto

PJ – Polícia Judiciária

PoS – *Proof of Stake* (em português: prova de participação ou interesse)

PoW – *Proof of Work* (em português: prova de trabalho)

TFUE – Tratado sobre o Funcionamento da União Europeia

SEC - *Securities and Exchange Commission* (em português: Comissão de Valores Mobiliários)

UE – União Europeia

UIF – Unidade de Informação Financeira

Índice

Introdução

O tema objeto de estudo na presente dissertação é a utilização de criptoativos na prática do crime de branqueamento de capitais, um fenómeno atual, com crescente relevância jurídico-penal, económica, política e social.

Este tema assume relevância uma vez que a globalização e consequente abertura dos mercados trouxe consigo novos desafios ao combate à atividade criminal. Para o que a presente dissertação interessa, cumpre discorrer que a prática do crime de branqueamento de capitais proliferou com a sofisticação de novos métodos e técnicas, com a abertura de fronteiras (e consequente possibilidade de mais fácil transferência de fundos além-fronteiras) e, sobretudo, com o desenvolvimento tecnológico.

Com efeito, não obstante o avanço de tecnologia disruptiva permitir eficiência, segurança e transações instantâneas, também transporta consigo preocupações, em particular, no que diz respeito à instrumentalização de tais tecnologias para o exercício de atividades ilegais.

No que aos criptoativos diz respeito, estes surgiram e tornaram-se bastante populares ao longo dos últimos anos, atraindo investidores, e, bem assim, o interesse de governos e reguladores. Enquanto alguns olham para o fenómeno dos criptoativos como sendo uma revolução financeira, outros, dada a sua alta volatilidade e falta de regulamentação, consideram-nos arriscados e meramente especulativos.

A prática de branqueamento de capitais com recurso a criptoativos é uma das formas mais recentes e sofisticadas de ocultação de proventos criminosos. E isto é possível porque, uma vez que as transações com criptoativos são descentralizadas, não rastreáveis e anónimas, são ocultadas as informações da operação correspondentes à identificação da origem e destino dos fundos, ou de quaisquer outras pessoas envolvidas nas transações.

Assim, é por demais evidente que a nova “modalidade” de branquear vantagens ilicitamente obtidas utilizando criptoativos é um desafio emergente

para as autoridades regulatórias e de aplicação da lei em todo o mundo devido às características intrínsecas dos criptoativos (de anonimato, privacidade, descentralização e falta de regulamentação) e, por isso, é necessário que seja dada uma resposta legislativa harmonizadora a nível internacional.

A verdade, é que os criptoativos são um produto complexo e, antes de aferir da adequabilidade da legislação, importa conhecer, em traços gerais, a tecnologia a estes subjacente.

Destarte, nesta dissertação começaremos por fornecer um enquadramento conceptual, versado na matéria dos criptoativos, bem como na sua origem, nas suas características do ponto de vista tecnológico e, ainda, na forma como podem ser utilizados para facilitar o branqueamento de capitais. Serão, aqui, discutidos mais aprofundadamente os recursos que tornam os criptoativos atraentes para a prática de atividades ilícitas, como sejam o anonimato, a descentralização e a facilidade de transferência transfronteiriça. Analisar-se-ão, ainda, diferentes métodos utilizados no branqueamento de capitais com criptoativos, como a mistura de moedas, transações p2p, o uso de serviços de câmbio não regulamentados, entre outras.

Numa segunda fase, será realizada uma análise da evolução da legislação antibranqueamento de capitais existente na Europa e, lateralmente, nos Estados Unidos, com foco nas medidas adotadas para combater o branqueamento de capitais relacionado com os criptoativos, destacando as principais características desses normativos, incluindo requisitos de identificação do cliente, monitorização de transações e relatórios de atividades suspeitas.

No final, serão apresentadas as conclusões decorrentes da análise realizada, onde serão discutidas as lacunas e desafios enfrentados na aplicação dessas leis, considerando a natureza descentralizada, anónima e global dos criptoativos.

PARTE I

ENQUADRAMENTO CONCEPTUAL

1. Branqueamento de capitais com recurso a criptoativos

1.1. Branqueamento de Capitais

De acordo com José Luís Braguês[1], o branqueamento de capitais é assim designado uma vez que "*descreve, com perfeição o circuito de lavagem do dinheiro, desde a introdução num ciclo de transações até sair do outro lado legalizado*". Ainda no seu entendimento, a prática de branqueamento de capitais compreende o "*encobrimento ou dissimulação, através de um conjunto de operações praticadas através do sistema económico, com primordial presença do financeiro, da origem ilícita ou criminosa dos bens obtidos*" e é, em suma, a "*atividade ou processo pela qual se procura dissimular a origem criminosa de bens ou produtos obtidos através da prática de alguns factos ilícitos, procurando dar-lhes uma aparência legal*".

O branqueamento de capitais tem como pressuposto a realização de um ilícito a montante, de onde são provenientes as vantagens que se desejam ocultar, sendo, por este motivo, considerado um crime derivado, de segundo grau ou induzido de outras atividades.

Com efeito, o branqueamento de capitais, i.e., o processo através do qual os criminosos ocultam a origem ilegal dos seus bens ou rendimentos, é habitualmente caracterizado por três fases[2], em concreto: *(i)* a fase inicial, também conhecida como "fase de colocação" (*placement*), a saber, o momento em que os produtos ilegais são introduzidos no sistema financeiro, muitas vezes divididos em montantes mais pequenos; *(ii)* a segunda fase, ou "fase de

[1] (Braguês, 2009 pp. 7 - 8)
[2] (European Union (EU), 2020 p. 4)

circulação" (*layering*), onde os fundos são deslocados ou convertidos de forma a camuflar a sua origem; e, por último, *(iii)* a terceira fase, ou "fase de integração" (*integration*), que se apresenta como a etapa em que os criminosos gastam ou investem o produto do branqueamento de capitais, agora legitimado, na economia.

No entendimento de Braguês[3], a este processo é, ainda, possível acrescentar uma quarta fase, a "fase de segurança", que consiste na atividade levada a cabo, durante todo o processo, pelos líderes das organizações criminosas, por forma a assegurarem que não são, também eles, defraudados.

Quando concluído com sucesso, explicam Miguel Viegas e Carlos Sarmento[4], o branqueamento de capitais retrata "*a última etapa da atividade criminosa, culminando na consagração do transgressor*".

Conforme clarificam Elizabeth Vallery Mulig e L. Murphy Smith[5], não obstante para a maioria das pessoas o crime de branqueamento de capitais, em si, poder não ser considerado como sendo altamente censurável, a verdade é que dá aos criminosos acesso ao seu produto. E, tais receitas podem, posteriormente, ser utilizadas pelos perpetradores do crime de branqueamento de capitais para o financiamento de uma miríade de outros crimes, assim favorecendo as ambições dos criminosos e comprometendo a integridade dos mercados.

Atualmente considerado como integrando o domínio da criminalidade particularmente grave com dimensão transfronteiriça[6], o bem jurídico violado aquando da prática do crime de branqueamento de capitais é a administração da justiça e a sua incriminação procura garantir a prossecução e o confisco dos proventos de atividades criminosas graves, dificultando a impunidade do perpetrador e desencorajando, então, a prática desses crimes[7].

---

[3] (2009 p. 9)
[4] (2022 p. 3)
[5] (Mulig, et al., 2008)
[6] *Cfr*. artigo 83.º, n.º 1, do TFUE.
[7] (Cheniaux, 2021 p. 38)

É a criatividade do agente criminoso que limita a escolha de veículos para o branqueamento de capitais do produto da sua atividade. O dinheiro pode ser lavado, ou branqueado, através de empresas de câmbio, corretoras de ações, negociantes de ouro, casinos, concessionários de automóveis, companhias de seguros e empresas comerciais. Também os serviços bancários privados, os bancos *offshore*, as empresas de fachada, as zonas de comércio livre, os sistemas de transferência e o financiamento do comércio possuem todos a capacidade de mascarar atividades ilegais[8].

Desta forma, a prevenção e o combate ao branqueamento de capitais revestem capital importância na proteção da integridade do sistema financeiro, na prevenção do financiamento do terrorismo e no combate ao crime organizado. Para tanto, os países têm implementado leis, regulamentações e diretrizes específicas, como as Diretivas da UE, para identificar, reportar e impedir transações suspeitas, além de estabelecerem requisitos de *due diligence*, de registos e de controlo interno para entidades financeiras e outras instituições.

O branqueamento de capitais é, sem grande polémica, considerado crime em várias jurisdições e, no ordenamento jurídico português, a sua incriminação está prevista no artigo 368.º-A do CP, punível com pena de prisão até 12 (doze) anos e, não estando prevista qualquer forma de negligência, é um crime que se caracteriza pelo tipo subjetivo doloso.

O GAFI identifica diversas modalidades através das quais é possível branquear capitais, cada um com diferentes características e implicações, e que se diferenciam entre si conforme sejam levadas a cabo de forma autónoma do crime precedente, pelo autor do crime precedente ou por terceiros alheios à prática do crime anterior, ou, até, quando seja concretizado de forma profissional e organizada.

O branqueamento de capitais independente ou autónomo refere-se à prossecução da infração de branqueamento de capitais de forma independente, ou seja, quando não há indícios da verdadeira origem do produto ou de uma

[8] (United States Department of State (USDS), 2001)

infração principal específica[9]. Isto pode ser particularmente relevante, designadamente, quando não existam provas suficientes da infração principal que dá origem ao produto do crime ou, até, em situações em que não exista jurisdição territorial sobre a infração principal.

Nesta modalidade da prática de ocultação de produtos do crime, podemos estar perante branqueamento realizado pelo arguido perpetrador da infração principal (autobranqueamento) ou por um terceiro (branqueamento de capitais por terceiros)[10].

Por sua vez, o autobranqueamento de capitais[11] consiste na execução do branqueamento por quem tenha estado envolvido na prática da infração principal[12], na medida em que são os próprios indivíduos autores da atividade criminosa inicial que ocultam o produto do seu próprio crime. Já o branqueamento de capitais por terceiros é, por maioria de razão, executado por uma pessoa que não esteve envolvida na prática da infração a montante[13][14].

Por fim, o branqueamento de capitais profissional é um subtipo do branqueamento por terceiros, compreendendo a atuação de organizações e indivíduos que oferecem profissionalmente os seus serviços para branquear capitais em troca de honorários, comissões ou outra forma de remuneração. Habitualmente, atuam de forma bastante sofisticada e organizada, utilizando

[9] (Jersey Financial Services Commission, 2022)
[10] (Financial Action Task Force (FAFT), 2013 - 2021 p. 116)
[11] No âmbito do artigo 368.º-A do Código Penal (desde a entrada em vigor da Lei n.º 11/2004, de 27 de março), prevê a prática do crime de branqueamento de capitais com recurso a "*vantagens, obtidas por si ou por terceiro*". E, o Acórdão do Supremo Tribunal de Justiça de fixação de jurisprudência n.º 13/2007, de 22 de março, cristalizou a possibilidade de punição do autor do crime precedente, admitindo expressamente a existência de concurso efetivo entre o ilícito que gerou a vantagem e o crime de branqueamento
[12] (Financial Action Task Force (FAFT), 2013 - 2021 p. 116). Segundo o GAFI, nesta modalidade, habitualmente, as quantias envolvidas são menores e é utilizado o modelo tradicional de branqueamento de capitais.
[13] Por exemplo, no caso de um membro da família ou de um amigo que utilize a sua conta bancária pessoal ou profissional para facilitar transações financeiras em nome de um traficante de droga
[14] (Financial Action Task Force (FATF), 2018 pp. 10 - 11)

estruturas complexas e opacas, transações entre jurisdições e movimentando quantias significativas de dinheiro[15].

De acordo com o GAFI[16], os autores da prática de branqueamento de capitais profissional utilizam uma série de instrumentos e técnicas, como sejam o branqueamento de capitais baseado no comércio, mecanismos de gestão de contas e plataformas bancárias clandestinas e alternativas. Para conferir um verniz de legitimidade às suas atividades, estes profissionais podem trabalhar com indivíduos corruptos especializados na prestação de serviços legítimos (por exemplo, banqueiros, advogados, contabilistas), para além da sua atividade criminosa de branqueamento de capitais.

Os profissionais do branqueamento de capitais trabalham frequentemente para mais do que um criminoso ou organização criminosa. Assim sendo, uma ação penal bem-sucedida contra um branqueador de capitais profissional pode ter um impacto potencial na atividade de diversos clientes criminosos.

[15] (Financial Action Task Force (FATF), 2018 pp. 10 - 11)
[16] (2018)

1.2. Utilização de criptoativos na prática de branqueamento de capitais

Os criptoativos proporcionaram às pessoas a possibilidade de realizar transferências financeiras rápidas, quase instantâneas e a baixo custo, com garantias intrínsecas de privacidade e segurança. Para além disso, com os criptoativos, em concreto, com a criação da Bitcoin, foi concebida a tecnologia *blockchain* – depois utilizada e desenvolvida por outros criadores de criptoativos -, que potenciou a inovação das mais diversas áreas[17].

Desde o lançamento da Bitcoin, outros criptoativos foram criados com base no mesmo conceito.

E assim, tais benefícios, acrescidos da relevância crescente do *e-commerce* e da atratividade do processamento de transações eletrónicas sem a necessidade de intermediação por uma entidade financeira, levaram a um aumento do interesse nos novos métodos de pagamento digitais, nomeadamente em criptoativos como a *Bitcoin*, e, bem assim, na tecnologia *blockchain* a esta subjacente[18].

A utilização de tecnologias *online* combinadas com criptografia resultou, então, num sistema de transferências completamente novo, onde um pagamento seguro passou a poder ser remetido diretamente para o destinatário sem recurso a intermediários, como um banco central ou autoridade pública[19].

O ano de 2017 foi considerado como decisivo para o fenómeno dos criptoativos, e uma das razões para tal foi o fenómeno "*boom ICO*", que

[17] Para sectores que lidem com grandes quantidades de dados e de informação, a *blockchain* permite uma gestão mais fácil do sistema e dos fluxos de trabalho e com os *smart contracts* disponíveis na *blockchain* da *ethereum*, passou a ser possível às indústrias utilizar aplicações da *blockchain* na criação de contratos.
[18] (Banco de Portugal working group on crypto-assets, 2020 p. 3)
[19] (Europol, 2021 p. 5)

correspondeu ao lançamento de centenas de *tokens*[20], sob a narrativa de se estar a construir uma economia descentralizada[21].

Em 2018, a Comissão Europeia[22] reconheceu que a inovação tecnológica conduziu a diversos tipos de novos ativos financeiros, especificamente os criptoativos, que, em conjunto com a tecnologia *blockchain*, seriam promissores para os mercados e infraestruturas financeiras.

Em Portugal, entre julho de 2021 e junho de 2022, os negócios com recurso a criptoativos movimentaram mais de € 30.000.000,00 (trinta mil milhões de euros), correspondentes a 14% do PIB português em 2021[23].

O facto de os criptoativos serem bens totalmente digitais, facilmente transferíveis, pseudoanónimos[24] e que operam numa base descentralizada, torna-os particularmente atrativos para a prática de crimes[25], sobretudo na ausência de regulamentação eficaz[26].

A verdade é que já existe uma relação perfeitamente identificada entre a utilização de criptoativos e a prática de atividades criminosas, seja através da prática de crime puramente informático, seja através de novas formas de cometer crimes tradicionais[27].

Algumas das formas mais conhecidas de utilização de criptoativos para fins criminosos incluem a sua utilização na *dark web*[28] (com o intuito de facilitar transações em mercados ilegais), práticas como o *ransomware* (requerendo o

[20] Os *tokens* são um tipo de criptoativo, conforme adiante se explicará melhor.
[21] (Ferreira, et al., 2021 pp. 4, 5)
[22] (Comissão Europeia p. 3)
[23] (Garcia, 2022)
[24] Sendo que, com a utilização de tecnologias específicas de reforço do anonimato, podem tornar-se até mesmo completamente anónimos.
[25] (Houben, et al., 2020 p. 45)
[26] (Europol, 2021 p. 4)
[27] (Ramalho, et al., 2020 p. 91)
[28] A *dark web* (uma camada da *deep web*) é um ramo anónimo da internet, acessível através de redes como o *The Onion Router*, I2P ou *Riffle*, que utilizam encriptação em camadas para ocultar a identidade e localização dos utilizadores, sendo, geralmente, considerada um paraíso para atividades ilícitas e ilegais. Já a *deep web* é toda a parte da internet que não é indexada pelos motores de busca normais, como o Google.

pagamento em criptoativos de forma a restaurar o acesso a arquivos ou sistemas) e, incontestavelmente, o branqueamento de capitais.

De facto, a Europol[29] reconheceu que a utilização de criptoativos para a prática de atividades criminosas tem crescido nos últimos anos em termos de volume e sofisticação e está predominantemente associada a transações *online* de bens e serviços ilícitos, fraude e branqueamento de capitais. Inclusive, durante a pandemia COVID-19, muitas redes criminosas confiaram neste tipo de ativo como meio de pagamento[30].

Com a ampla disponibilidade de ferramentas para a utilização de criptoativos e com o estabelecimento de serviços dedicados à canalização de capitais de origem criminosa, a utilização transgressora de criptoativos passou a relevar em todos os tipos de crime que requeiram a transmissão de dinheiro[31].

Em matéria de criptoativos, e no que ao branqueamento de capitais diz respeito, a CE[32] reconheceu os benefícios, mas também os riscos, tendo considerado que os "*criptoativos e a tecnologia de cadeia de blocos subjacente são promissores para os mercados financeiros e as infraestruturas financeiras. A sua utilização também implica riscos, como foi demonstrado pela forte volatilidade dos criptoativos, pelas fraudes e deficiências e vulnerabilidades operacionais nas plataformas de negociação de criptoativos. A nível da UE, já foram tomadas medidas para dar resposta a alguns riscos específicos. As ameaças e vulnerabilidades das moedas virtuais e o* ***branqueamento de capitais*** *e o financiamento do terrorismo foram avaliados como correspondendo a uma* ***exposição elevada ou mesmo muito elevada*** *no relatório da Comissão sobre a avaliação dos riscos de branqueamento de capitais e de financiamento do terrorismo*" (destacado nosso).

[29] (Europol, 2021 p. 3)
[30] (Europol, 2021 p. 12)
[31] (Europol, 2021 p. 4)
[32] (2018 p. 3)

Como bem explicam David Silva Ramalho e Nuno Igreja de Matos[33], nas fases de colocação de e integração[34], a utilização de criptoativos, devido às suas particularidades, permite agilizar a operação de colocação de produtos de atividade ilícita no sistema financeiro, que, de outra forma, seguindo os percursos financeiros tradicionais, seria mais demorada e estaria sujeita a mecanismos de controlo no contexto das instituições financeiras tradicionais, e, bem assim, exposta a um maior risco de deteção pelas autoridades. Depois, a pseudanonimização surge como uma vantagem para indivíduos já sinalizados pelos sistemas de prevenção de branqueamento de capitais tradicionais, uma vez que, de outro modo, dificilmente passariam o crivo dos controlos das entidades financeiras obrigadas.

Depois, a tecnologia *blockchain*, o "livro-razão digital" por detrás dos criptoativos, é praticamente inviolável e não requer qualquer tipo de monitorização, o que levanta a possibilidade de as novas regras regulatórias poderem gerar a intenção (não intencional) de empurrar o dinheiro produto do crime ainda mais para trás das *firewalls* e para a *dark web*[35].

Para Andrew Haynes e Peter Yeoh[36], a forma como os criptoativos (em especial, a Bitcoin) operam e que os torna ideais para a prática de branqueamento de capitais, sugere que, em última análise, as novas leis terão de acabar com o anonimato dos endereços das carteiras e aumentar a transparência das empresas de câmbio e dos seus utilizadores.

Pode, então, afirmar-se que a descentralização, (pseudo)anonimidade e a instantaneidade das transações características criptoativos constituem a sua mais-valia, mas são também estes os atributos que os tornam especialmente expostos à prática do branqueamento de capitais, uma vez que permitem a circulação do dinheiro nos ângulos cegos dos sistemas de prevenção do branqueamento, facilitando a possibilidade de criptoativos provenientes de

[33] (2020 p. 104)
[34] Respetivamente, a primeira e terceira fases do branqueamento de capitais, *cfr*. descrição do ponto 1.1. *supra*.
[35] (Haynes, et al., 2020 p. 171)
[36] (2020 p. 171)

atividades criminosas percorrerem as diferentes fases ou etapas do crime de branqueamento[37].

Antes do seu encerramento pelo FBI em 2013, o afamado mercado Silk Road chamou à atenção a possibilidade da utilização de criptoativos como método de pagamento preferencial para atividades criminosas e, desde o seu desaparecimento, seguiram-se numerosos mercados na *dark web* para transações criminosas.

Assim, embora a prática de branqueamento de capitais com recurso a criptoativos seja um desafio relativamente recente, já existem novos casos que também despertaram o interesse dos reguladores, como os casos BTC-e e Liberty Reserve, que, devido às implicações para a regulamentação deste tipo de instrumento, evidenciaram algumas das lacunas na regulamentação existente relativa ao combate ao branqueamento de capitais, destacando a necessidade de normas mais rígidas para plataformas financeiras digitais, bem como a importância da cooperação internacional no combate à utilização ilícita desses serviços.

À medida que o ecossistema de criptoativos evolui, é provável que surjam novos eventos e desafios.

[37] (Ramalho, et al., 2020)

1.2.1. O caso Liberty Reserve

De acordo com o GAFI[38], o caso Liberty Reserve foi, até à data, o maior caso de branqueamento de capitais *online* da história.

Desmantelada em 2013, a plataforma internacional de transação baseada em sistemas de pagamentos através de criptoativos Liberty Reserve (à data, acessível através do endereço www.LibertyReserve.com) foi concebida por Arthur Budovsky por forma a evitar o escrutínio regulamentar e policial e, deste modo, possibilitar a criminosos a realização de transações financeiras anónimas e indetetáveis, permitindo-lhes distribuir, armazenar e branquear produtos resultantes da fraude de cartões de crédito, de roubos de identidade, de fraudes em investimentos, de pirataria informática, de tráfico de drogas e de pornografia infantil[39].

Esta plataforma comportou mais de um milhão de utilizadores em todo o mundo e nela foram operadas cerca de cinquenta e cinco milhões de transações, quase todas com fito criminoso. Durante um período de sete anos, estima-se que tenha processado e branqueado 6.000.000,00 USD (seis mil milhões de dólares)[40].

Embora a plataforma exigisse informações básicas de identificação, as mesmas não eram minimamente validadas, o que permitiu aos utilizadores a criação de contas sob nomes e endereços falsos. Este comportamento por parte da plataforma foi entendido como sendo propositado, de maneira a facilitar aos seus utilizadores a transferência, não rastreável, de dinheiro proveniente de conduta criminosa[41].

[38] (2014 p. 10)
[39] De acordo com a BBC News, a plataforma Liberty Reserve publicitou-se como sendo o processador de pagamentos mais antigo, mais seguro e mais popular da Internet, servindo milhões de pessoas em todo o mundo (2016).
[40] (Exploring the links between AML, digital currencies and blockchain technology, 2019 p. 521)
[41] (Sanction Scanner, 2019)

Para acrescentar uma camada adicional de anonimato, a plataforma Liberty Reserve exigia aos seus utilizadores que fizessem depósitos e levantamentos através de empresas de transmissão de dinheiro que operavam em território russo e em vários outros países sem supervisão ou regulamentação governamental significativa, à data, em matéria de branqueamento de capitais, como a Malásia, Nigéria e Vietname.

Ademais, a plataforma também não permitia aos utilizadores a transferência direta de dinheiro para as suas contas de utilizador a partir de contas bancárias “normais”. Em vez disso, obrigava a que todos os depósitos fossem efetuados por meio de empresas de câmbio externas, que possuíam contactos financeiros diretos com a Liberty Reserve e compravam LR (a moeda da plataforma) em grandes quantidades em troca de dinheiro fiduciário. Outrossim, os utilizadores da plataforma que pretendessem levantar LR das suas contas, teriam de enviar o seu dinheiro LR para uma empresa de câmbio que, posteriormente, lhes devolvia uma quantia equivalente em moeda fiduciária[42].

Ao evitar depósitos e levantamentos diretos de utilizadores, a Liberty Reserve não recolhia informações sobre os mesmos através de transações bancárias, uma vez que, caso assim não fosse, seria criado um rasto central. Ademais, por uma "taxa de privacidade" extra, os utilizadores podiam esconder os números das suas contas Liberty Reserve ao transferir fundos, tornando as transferências completamente indetetáveis.

Este caso impactou indiretamente o sector bancário, uma vez que os fatores que facilitaram a conduta foram a falta de informação sobre os beneficiários efetivos dos clientes e a inexistência de um quadro antibranqueamento de capitais para a comunicação de transações suspeitas com criptoativos.[43]

[42] (Sanction Scanner, 2019)
[43] (Exploring the links between AML, digital currencies and blockchain technology, 2019 p. 521)

1.2.2. O caso BTC-e

Este caso diz respeito, uma vez mais, a uma investigação relacionada com branqueamento de capitais, desta feita envolvendo uma plataforma de câmbio de criptoativos, a BTC-e, operada por Alexander Vinnik, um cidadão russo.

A plataforma foi fundada em 2011 e apreendida em 2017 pelo facilitamento de transações financeiras relacionadas com crimes de corrupção, tráfico de droga e outros crimes, sendo que as investigações revelaram que, durante as suas operações, a BTC-e processou mais de 4.000.000.000 USD (quatro mil milhões de dólares) em criptoativos[44].

Para utilizar esta plataforma, os utilizadores criavam uma conta acedendo ao sítio na internet da BTC-e (www.btc-e.com), não necessitando, para o efeito, de fornecer informações de identificação básicas (como o nome, data de nascimento, morada), apenas um nome de utilizador, uma palavra-passe e um endereço de correio eletrónico. Ademais, a BTC-e não exigia aos seus utilizadores que validassem a sua identidade através do fornecimento de documentos de identificação oficiais[45].

As atividades facilitadas pela plataforma BTC-e incluíram o branqueamento das receitas resultantes da compra de criptoativos através da utilização de receitas ilícitas e da transferência de fundos[46], permitindo a conversão dos fundos ilicitamente obtidos noutros criptoativos ou em moeda fiduciária.

A plataforma não dispunha de qualquer controlo ou política de combate ao branqueamento de capitais e acredita-se ter recebido receitas criminosas proveniente de ataques de *ransomware*, esquemas de roubo de identidade, *hacking* e outros incidentes de pirataria informática, bem como de funcionários públicos corruptos e redes de distribuição de estupefacientes, estimando-se que

[44] (Haig, 2019)
[45] (Anderson, et al., 2019)
[46] (Europol, 2021 p. 12)

entre 2011 e dezembro de 2016, os endereços de Bitcoin e as carteiras digitais associadas à BTC-e receberam mais de nove milhões de criptoativos[47].

[47] (BankInfoSecurity, 2020)

1.2.3. O caso português

Também em Portugal este tipo de criminalidade já não é novidade.

A Rita e o Pedro, um casal português que, em 2017, montou um esquema de compra e venda de drogas a partir de Trás-os-Montes e com destino a dezenas de países um pouco por todo o mundo, foi detido pela Unidade Nacional de Combate ao Tráfico de Estupefacientes da PJ, na chamada "Operação BIT"[48].

O casal utilizava, sob o nickname "Dailyfix", a plataforma Alphabay Market, um mercado negro de venda de estupefacientes, anunciando uma vasta listagem de tipos de drogas para venda. Rita e Pedro enviavam os produtos em envelopes almofadados dos CTT, para os mais variados destinos, dentro ou fora da Europa[49].

Foram identificados três esquemas de branqueamento dos produtos obtidos por Pedro e Rita[50]:

(i) Pagamento em Bitcoins, e posterior mistura com Bitcoins de terceiros, sendo que, posteriormente, o casal fazia passar as mesmas por um misturador, vendendo-as, depois, e recebendo dinheiro fiduciário;
(ii) Utilização de um site para converter as Bitcoins em dinheiro fiduciário, com posterior transferência para outra plataforma (situada em Malta), no qual se encontrava associado um cartão de débito, que lhes permitia gastar o dinheiro em qualquer parte;
(iii) Após a passagem das Bitcoins pelos misturadores, quer dos próprios mercados de venda de produtos estupefacientes na *darknet*, quer por misturadores exteriores, mas ainda na *darknet*, faziam o depósito das Bitcoins misturadas na conta física do computador, após o que as transferiam para uma conta num site (situado em Hong Kong), onde

[48] (Polícia Judiciária, 2017)
[49] (Darknetlive, 2019)
[50] (Diário de Notícias, 2019)

se encontrava associado um cartão de débito que permitia gastar os valores de bitcoins.

2. Criptoativos

Até à data, não existe uma definição consensual e unitária do conceito de criptoativos. Há muitos termos que são utilizados indiscriminadamente, como "criptoativos", "*tokens*[51]", "criptotokens", "ativos virtuais", "ativos digitais", e a variedade de definições propostas ilustra a falta de compreensão sobre o que são os criptoativos, resultando na falta de uniformidade na abordagem à definição de criptoativos, com algumas das definições referentes à criptografia, outras à DLT, e algumas à dimensão económica[52].

Apesar de não existir um conceito unanime os para definir, existe uma série de reflexões tendencialmente aceites.

Na aceção do BCE[53], os criptoativos dizem respeito a qualquer ativo que se encontre registado em formato digital e que não seja, nem represente, um direito financeiro ou um passivo financeiro de qualquer pessoa singular ou coletiva, e não incorpore um direito de propriedade de qualquer entidade. No entanto, um criptoativo é considerado um ativo valioso pelos seus utilizadores, quer seja como um investimento, quer como um meio de troca.

Definição semelhante é oferecida pelo Banco de Portugal[54], que diz que os criptoativos são "*representações digitais de valores ou de direitos que podem ser transferidos e armazenados eletronicamente. Apesar de poderem ser usados para fazer pagamentos, como o valor dos criptoativos oscila muito, são sobretudo utilizados como ativos de investimento. Um dos mais conhecidos é a Bitcoin*".

A EBA[55] referiu que os criptoativos são um tipo de ativo financeiro que faz uso de criptografia e de DLT como parte do seu valor inerente ou percebido.

[51] Na versão portuguesa, "criptoficha".
[52] (Ferreira, et al., 2021 p. 10)
[53] (2019 p. 5)
[54] (2020)
[55] (European Banking Authority (EBA), 2019)

A FCA[56] refere que os criptoativos, no geral, são representações digitais, criptograficamente protegidas, de valor ou de direitos contratuais, através da tecnologia DLT, e que podem ser armazenados, transferidos ou negociados eletronicamente.

De acordo com Haynes & Yeoh[57], os criptoativos são moeda digital ou virtual não emitida por uma autoridade central, que emprega criptografia para providenciar segurança e verificar transações na sua rede e são um sistema *blockchain* P2P, que tem por base regras de funcionamento autónomo baseadas em códigos, por sua vez, baseados em transações.

Segundo Houben, et al.[58], os criptoativos caracterizam-se por serem registados com recurso a criptografia e tecnologia DLT ou outra tecnologia semelhante, não serem emitidos nem garantidos pela banca central ou por uma autoridade pública, e poderem ser utilizados como meio de troca, para fins de investimento ou até para aceder a bens ou serviços.

Conforme bem explicam Trozze, A., Kamps, J., Akartuna, E.A. *et al.*[59], os criptoativos partilham de três princípios, e são eles: *(i)* a descentralização, já que em vez de serem geridos por uma instituição, são administrados por via de uma rede P2P[60], cuja maioria de utilizadores tem de concordar com quais as transações e ramo de uma DLT (a *blockchain*) são válidas; *(ii)* a pseudoanonimidade[61], porque, para identificar os utilizadores, em vez de nomes de utilizador ou números de conta, são usadas *hashes*[62] de chaves públicas, formando um sistema de gestão de identidade descentralizada; e *(iii)* a

[56] (Financial Conduct Authority, 2019)
[57] (Regulatory and Legal Issues, 2020, p. 7)
[58] (2020 p. 17)
[59] (2022 p. 2)
[60] Nome dado à arquitetura de redes de computadores onde cada um dos pontos da rede funciona tanto como cliente e/ou como servidor, permitindo, assim, a partilha de dados e serviços sem intervenção de um servidor central.
[61] Os criptoativos são considerados apenas "pseudoanónimos" ao invés de "anónimos" devido à característica da transparência das transações.
[62] Puzzles de cifragem

transparência, uma vez que todas as transações que ocorrem são gravadas publicamente na *blockchain*.

2.1. Tipos de criptoativos

Os criptoativos podem ter diversas formas e características, sendo que, habitualmente, são divididos em duas grandes categorias, em concreto, repartem-se entre criptomoedas e *tokens*[63].

Por sua vez, as criptomoedas podem ser divididas em duas categorias principais[64], por um lado, as criptomoedas não garantidas (ou *non-backed cryptocurrencies*), que derivam o seu valor da expectativa de que serão utilizadas no futuro e, por outro lado, as criptomoedas garantidas (ou *stablecoins* ou *backed cryptocurrencies*), que são suportadas por algum tipo de ativo, moeda fiduciária, combinação de ativos numa reserva ou, até mesmo, apoiadas por outras criptomoedas, não garantidas ou garantidas (algorítmicas).

O primeiro tipo de criptoativo a surgir (a *Bitcoin*), foi uma criptomoeda não garantida, desenhada com o intento de ser utilizada como dinheiro, como uma forma comum de meio de troca e, no fundo, de forma a providenciar uma alternativa ao dinheiro emitido pela banca central[65].

Porém, a alta volatilidade deste tipo de criptoativos fez com que a sua utilização enquanto moeda se tenha tornado muito complicada[66], uma vez que a falta de estabilidade faz com que não sejam capazes de cumprir a terceira função do dinheiro, o elemento de reserva de valor[67].

[63] Podendo, ainda, existir uma terceira categoria de criptoativos, do tipo híbrido, quando reúnam as duas caraterísticas ou partes delas
[64] (Cryptocurrencies and fiat money: The end of a public good?, 2022 p. 3)
[65] (European Parliament, 2020)
[66] (Houben, et al., 2020 p. 18 e 19)
[67] (Cryptocurrencies and fiat money: The end of a public good?, 2022 p. 4)

Tal visão é coerente com a posição do Regulador português[68], que considera que, apesar de, muitas vezes, serem chamados de “moedas virtuais”, os criptoativos não podem ser considerados verdadeiras moedas “[p]*or um lado, porque, como são muito voláteis, não permitem estabelecer um preço para os bens, nem preservar o poder de compra. Por outro, porque não são garantidos pelo Banco de Portugal nem por qualquer outra autoridade nacional ou europeia e porque não existe qualquer proteção legal que confira direitos de reembolso ao consumidor*”.

Já os *tokens*, de acordo com o PE[69], a segunda geração de criptoativos, são representações digitais de interesses ou direitos de aceder a certos ativos, produtos ou serviços, normalmente emitidos através de uma plataforma ou *blockchain*.

Habitualmente, os *tokens* podem ser divididos[70] entre *tokens* de ativos ou *asset-backed tokens* (cripto-tokens associados a ativos físicos ou digitais, financeiros e não financeiros, que podem representar tokens de segurança e de investimento, bem como registos digitais[71]), *tokens* de pagamento ou *payment tokens* (cripto-tokens utilizados para efetuar pagamentos digitais; o termo refere-se principalmente a criptomoedas, que são uma forma específica de moeda digital construída sobre livros-razão) e *tokens* de utilidade ou *utility tokens*[72] (os *tokens* que fornecem uma determinada utilidade aos utilizadores, como direitos de acesso, direitos de membro, ou identificação e autenticação, ou que servem de recompensa).

[68] (Banco de Portugal, 2020)
[69] (European Parliament, 2020 p. 18)
[70] (Crypto Tokens and Token Systems, 2023 p. 6)
[71] Um exemplo de um *token* de ativos é o "BNK token" do Bankera, que confere ao seu detentor o direito a uma comissão semanal a ser paga em *Ether* (European Parliament, 2020 p. 21)
[72] Alguns exemplos de tokens de utilidade incluem o Golem (GNT) e o Filecoin (FIL), cada um dos quais facilita o acesso a um serviço específico, ou seja, poder de computação (Golem) e armazenamento de dados (Filecoin). (European Parliament, 2020 p. 21)

Depois, é ainda possível dividir os *tokens* entre aqueles que são fungíveis e aqueles que não são fungíveis (NTF's).

Conforme esclarece o PE[73], nalguma literatura jurídica e documentação política, as criptomoedas são também referidas como "*tokens* de pagamento", "*tokens* de troca" ou "*tokens* de moeda". Esta terminologia é confusa e não está isenta de problemas, porém, enquanto os *tokens* representam tipicamente um direito a algum bem ou direito, as criptomoedas - ou pelo menos as criptomoedas tradicionais não garantidas - geralmente não incorporam direitos intrínsecos.

Cumpre ainda referir que as *stablecoins* devem ser distinguidas dos *tokens*, em vez de serem identificadas com estes.

Apesar de, tal como os *tokens*, as *stablecoins* serem normalmente emitidas numa *blockchain* existente e incorporarem um crédito (em relação a um emitente identificável ou a ativos que suportam as moedas), por sua vez, os *tokens* são emitidos com uma funcionalidade muito específica ou para um objetivo específico (por exemplo, para conferir aos seus detentores direitos de propriedade e/ou direitos semelhantes a dividendos, ou para permitir o acesso a um produto ou serviço específico). Já as *stablecoins* não têm geralmente essa funcionalidade, destinando-se a ser utilizadas como um meio de troca para fins gerais (para permitir a compra e venda de um bem ou serviço fornecido por alguém que não o emitente)[74].

[73] (2020 p. 18)
[74] (European Parliament, 2020 p. 20)

2.2. A Tecnologia *blockchain*

A tecnologia de registo distribuído, ou DLT, funciona como uma base de dados ou um registo de informação, que é partilhada através de uma rede e onde não existe necessidade de existência de um processo de validação centralizado. Podemos estar perante uma base de dados sem restrições e com conteúdo público, ou, pelo contrário ser uma base de dados restrita a um grupo específico de utilizadores, com conteúdo visível apenas para os participantes avaliados[75].

A tecnologia DLT diz respeito aos protocolos e infraestrutura de suporte que permitem que computadores em diferentes locais proponham e validem transações e atualizem registos de forma sincronizada através de uma rede, cuja ideia subjacente é a de um livro-razão, um registo comum de atividade, partilhado em computadores em diferentes locais[76].

A *blockchain* é uma forma particular de tecnologia DLT[77], que, como vimos, consiste numa forma de gravar e partilhar dados por múltiplos armazenamentos de dados (ou *ledgers*), sendo que, cada um, contém exatamente os mesmos registos de dados, que são mantidos e controlados coletivamente por uma rede de servidores informáticos, os nós (ou *nodes*)[78].

Segundo a Europol[79], a *blockchain* pode ser definida como uma base de dados transacional e como um tipo ou subconjunto específico da chamada tecnologia DLT. A *blockchain* emprega um método de encriptação conhecido como criptografia e utiliza algoritmos matemáticos específicos para criar e verificar uma estrutura de dados em crescimento contínuo, à qual só podem ser adicionados dados e da qual os dados existentes não podem ser removidos. Não

[75] (Bullmann, et al., 2019 p. 7).
[76] (Alcarva, 2018)
[77] Conforme afirma, e bem, Pedro Ferreira Malaquias, "[a] *DLT de referência é a blockchain, sem dúvida a mais conhecida e divulgada base de dados na área dos criptoativos*" - (2021)
[78] (Houben, et al., 2018 p. 15)
[79] (Europol, 2021)

existe um proprietário central da rede e do *software* e são distribuídas cópias idênticas do livro-razão a todos os nós da rede.

De acordo com a explicação de Houben & Snyers[80], a *blockchain* é um mecanismo que emprega um método de criptografia e utiliza (um conjunto de) algoritmos matemáticos específicos para criar e verificar uma estrutura de dados em crescimento contínuo. Nesta estrutura de dados, a única ação possível é a adição de dados e a informação já existente não pode ser alterada ou removida. Isto forma uma cadeia de "blocos de transação", que funciona como um *distributed ledger.*

A *blockchain*, ou cadeia de blocos, atua como um livro-razão público, que mostra todas as transações, embora as identidades dos participantes estejam ocultadas. O bloco central é o bloco original e cada participante adiciona o seu bloco. Cada transação inclui a função criptográfica (CHF[81]) do bloco anterior, conectando-os entre si[82] e cada adição de um bloco ligado à cadeia torna mais difícil para um mineiro ou (*miner*) desonesto roubar Bitcoin, reescrevendo a sequência de transações[83].

Criptoativos como a *Bitcoin* são protegidos com esta técnica, sendo utilizado um engenhoso sistema de chaves digitais públicas e privadas[84].

A tecnologia *blockchain* permite que duas partes que não se conhecem, cheguem a um consenso através de uma história digital comum. Uma vez que os ativos e as transações digitais são, em teoria, fáceis de falsificar e duplicar, a tecnologia *blockchain* veio resolver este problema sem fazer uso de um intermediário financeiro[85].

---

[80] (Houben, et al., 2018 p. 15)
[81] Equação utilizada para verificar a validade dos dados, que traduz dados de vários comprimentos – a mensagem – para uma cadeia de tamanho fixo – o *hash*, e caracteriza-se pela dificuldade em reverter e recriar a informação utilizada para o criar (Jake Frankenfield, 2022).
[82] (Haynes, et al., 2020 pp. 11 - 12)
[83] (Haynes, et al., 2020 p. 11)
[84] (Houben, et al., 2018 p. 20)
[85] (Alcarva, 2018 p. 67)

De acordo com o GAFI[86], uma das principais vantagens da tecnologia *blockchain* é o facto de permitir simplificar a execução de uma grande variedade de transações que normalmente exigiriam a intermediação de um terceiro (por exemplo, um depositário, um banco, um sistema de liquidação de valores mobiliários, corretores, um repositório de transações, ...), pelo que, na sua essência, a *blockchain* tem tudo a ver com a descentralização da confiança e com o facto de permitir a autenticação descentralizada das transações.

O atual sistema de transferências, onde os bancos atuam como intermediários, permitiu o aumento exponencial das transações entre várias geografias. Todavia, devido à forte componente centralizadora da banca tradicional, não é possível aumentar a velocidade das transferências e custos de ineficiência, e é aqui que entram as moedas virtuais, descentralizadas, com maior rapidez e menores custos[87].

A *blockchain* tornou todas as promessas de criar uma moeda digital que pudesse ser utilizada para transferências de valor sem requerer a intervenção de intermediários possíveis graças à segurança e confiabilidade do sistema e à verificação das transações sem a necessidade de utilização de uma autoridade central.

Nas *permissionless blockchains* ou *blockchains* públicas, como a Bitcoin e a Ethereum, o acesso é público e a gestão de rede é efetuada através dos mecanismos de consenso[88]. Estas *blockchains* são totalmente descentralizadas, praticamente qualquer pessoa pode: aderir à rede; enviar e receber transações; operar um nó; ver, copiar e contribuir para o código; e participar no processo de consenso.

Devido aos problemas associados ao consenso necessário em redes descentralizadas e abertas, foram criadas *permissioned blockchains* ou *blockchains* privadas, onde existe controlo sobre a rede por parte de uma entidade ou número de entidades, que, recorrendo a um conjunto de critérios de

[86] (2019)
[87] (Alcarva, 2018 p. 66)
[88] (Santos, 2021 pp. 34 - 35)

admissibilidade, consegue decidir quem são os participantes da rede, qual a informação que pode ser inserida e validada e efetuar alterações às regras da rede[89].

[89] (Santos, 2021)

2.3. Sistemas de Consenso Distribuído

Os sistema de consenso distribuído são a forma utilizada para estabelecer o acordo entre as múltiplas partes de uma transação sobre alguma informação (como seja a propriedade de um bem, por exemplo). De forma a provar a autenticidade de tal informação, é utilizada a assinatura criptográfica de dados[90].

Assim, tal como no problema dos generais bizantinos[91], em que é necessário confiar nas mensagens dos generais de modo a chegar a um consenso, nos criptoativos é necessário confiar na integridade das transações registadas na *blockchain*. Todavia, ao contrário do problema dos generais bizantinos, onde mensagens falsas podem ser enviadas por traidores, no contexto dos criptoativos o objetivo é projetar um sistema resistente a ataques de indivíduos mal-intencionados que tentem manipular as transações ou enganar o sistema.

Há diversos tipos de sistemas ou mecanismos de consenso, donde se destacam o PoW e o PoS.

No mecanismo PoW, utilizado, por exemplo, pela *Bitcoin*, o principal objetivo é chegar a acordo sobre um único estado da *blockchain*, pelo que, para o efeito, um dos *nodes* (ou nós) participantes tem que comprovar que o trabalho por si realizado e submetido é preciso, auferindo, assim, o direito de acrescentar mais transações à blockchain[92].

Por forma a construir o próximo bloco da *blockchain*, é necessária a resolução de um desafio criptográfico. A primeira pessoa a encontrar a solução torna-se encarregada por fechar e entregar o bloco, o *leader* - este processo chama-se mineração e é levado a cabo pelos chamados “mineiros” (ou *miners*)

[90] (Debus, 2017 p. 4)
[91] Problema clássico da ciência da computação, formulado em 1982 por Leslie Lamport, que descreve uma situação em que um grupo de generais bizantinos deve chegar a um consenso sobre um plano de ação, mas alguns dos generais podem ser traidores e enviar mensagens falsas.
[92] (Lepore, et al., 2020 p. 11)

que, ao confirmarem a informação da transação, tornam os pagamentos na rede seguros e confiáveis.

O *leader* recebe uma recompensa como resultado do seu trabalho para gerar o bloco, e esta recompensa é o incentivo que a rede utiliza para garantir que mantém os nós leais ou honestos. Enquanto a maioria dos nós honestos forem encorajados a encontrar uma solução para o desafio criptográfico, a maioria do poder da CPU estará em mãos honestas, o que preserva a honestidade do sistema. Aumentando o número de *miners*, diminui-se a probabilidade de mineiros desonestos conseguirem controlar 51% da CPU, fazendo com que cada tentativa de defraudar a rede seja inexequível[93].

Por seu turno, o mecanismo PoS foi inventado como alternativa à PoW.

Neste mecanismo de consenso, os titulares dos nós, de forma a poderem registar novos blocos e serem devidamente remunerados com novos criptoativos e respetivas comissões das transações, têm de provar que possuem um número de criptoativos determinado pela rede[94].

Os *stakers* (alternativa aos mineiros) bloqueiam fundos num *smart contract* especial e, sempre que um novo bloco é necessário, um algoritmo disponibiliza, de forma aleatória, a oportunidade a um *staker* específico de publicar o próximo bloco.

No mecanismo PoS, um nó participa no processo de consenso (gera ou valida o bloco seguinte) proporcionalmente às apostas que faz, sendo que, quanto mais se aposta, mais influência se tem na validação do bloco seguinte e, diferentemente do mecanismo PoW, no PoS os nós não precisam de competir uns com os outros para resolver um problema matemático, o que resulta num processo mais eficiente e energeticamente mais sustentável[95].

[93] (Lepore, et al., 2020 p. 14)
[94] (Santos, 2021 p. 37)
[95] (Lepore, et al., 2020 p. 15)

Caso seja registado um bloco com a informação errada e os restantes *stakers* não aceitem esse novo bloco, são retirados os criptoativos que esse detentor tinha em "*stake*".

De tal modo, os sistemas de consenso são um elemento fundamental nos criptoativos e na tecnologia *blockchain*, projetados de forma a permitir que os participantes de uma rede distribuída concordem com o estado atual do sistema e validem transações de forma confiável, mesmo quando alguns participantes possam ser desonestos ou mal-intencionados.

Cada sistema tem suas vantagens e desvantagens, e diferentes criptoativos e *blockchains* podem escolher o algoritmo que melhor se adapte às suas necessidades de segurança, eficiência e governança.

2.4. Bitcoin

No livro branco de Satoshi Nakamoto[96] (cuja verdadeira identidade ainda é alvo de mistério), o principal motivo dado para a criação do sistema de pagamento eletrónico baseado em provas criptográficas foi o facto de o comércio *online* sofrer das fraquezas inerentes ao modelo baseado na confiança, por depender quase exclusivamente das instituições financeiras, que servem como terceiros de confiança no processamento dos pagamentos eletrónicos.

Desse modo, Nakamoto indicou ser necessário um sistema de pagamento eletrónico baseado em provas criptográficas, em vez da confiança, permitindo às partes transacionar diretamente entre si sem a necessidade de terceiros.

No livro branco que elaborou, propôs uma solução para o problema do "duplo gasto" *(double spending)*[97] das moedas virtuais, através da utilização de um servidor *timestamp* distribuído P2P para gerar prova computacional da ordem cronológica das transações. Neste documento, é afirmado que o sistema seria seguro desde que os *nodes*[98] "honestos" controlassem coletivamente mais poder de CPU do que qualquer grupo cooperante de *nodes* "atacantes".

Assim, o ideal que nasceu com a *Bitcoin* foi o de uma moeda que não serve interesses geopolíticos, imune a pressões e interesses de uma certa geografia ou sistema, neutra, gerada e gerida por código e por regras que estão definidas desde o dia um (o código da *Bitcoin* não é alterado e não é alterável).

---

[96] (Nakamoto, 2008)

[97] O *double spending*, ou duplo gasto, acontece quando alguém tenta fazer uma transação de *Bitcoin* para dois destinatários diferentes, de forma simultânea (Haynes, et al., 2020 p. 8)

[98] É o nome dado aos computadores da *blockchain* que validam e retransmitem as transações.

2.5. Ethereum

A Ethereum foi publicada em 2015 por Vitalik Buterin e, de acordo com o seu livro branco[99], a sua intenção foi a de criar um protocolo alternativo para a construção de aplicações descentralizadas, fornecendo, para tal, um conjunto diferente de compensações, com ênfase nas situações onde releve a rapidez do desenvolvimento, a segurança de aplicações pequenas e pouco usadas e a capacidade de diferentes aplicações interagirem de forma eficiente.

Para tal, a Ethereum criou uma *blockchain* com uma linguagem de programação Turing-completa[100] integrada, permitindo a qualquer pessoa a possibilidade de programar e escrever *smart contracts* e aplicações descentralizadas, onde possam criar as suas próprias regras de propriedade arbitrárias, formatos de transação e funções de transição de estado.

Assim, a Ethereum é uma *blockchain* e tem uma moeda nativa conhecida, a Ether, que é utilizada para pagar a atividade da *blockchain* Ethereum. O Ether também pode ser negociado em empresas de câmbio de criptoativos, permitindo aos usuários a compra, venda ou troca dessa criptomoeda por outras ou por moedas fiduciárias.

A principal diferença entre a Ethereum e a Bitcoin no que diz respeito à arquitetura da *blockchain*, é que, ao contrário da Bitcoin, os blocos da Ethereum contêm uma cópia da lista de transações e do estado mais recente. Para além disso, dois outros valores, o número do bloco e a dificuldade, são também armazenados no bloco.

---

[99] (Ethereum, 2023)

[100] A completude de Turing refere-se a uma caraterística das plataformas de computação em que um computador considerado Turing-completo pode executar todos os programas que uma máquina de Turing seria capaz de executar. No universo dos criptoativos, as máquinas de Turing são importantes porque ajudam a definir aquilo que é um criptoativo de segunda geração: a Ethereum possui uma linguagem de programação Turing-completa, o que significa que pode ser utilizada para expressar e resolver qualquer problema de computador solucionável conhecido (crypto.bi).

2.6. Integração dos criptoativos na banca tradicional

Embora, num momento inicial, os criptoativos tenham surgido como uma alternativa descentralizada e independente ao sistema bancário, hodiernamente encontram-se, de várias formas, a integrar gradualmente o sistema financeiro convencional.

Os bancos tradicionais, reconhecendo a crescente demanda por criptoativos como um tipo de investimento, começaram a oferecer aos seus clientes a opção de investir em criptoativos por meio de produtos de investimento especializados ou parcerias com empresas de câmbio, permitindo-lhes, além dos ativos tradicionais, diversificar as suas carteiras de investimento[101].

A banca começou também a explorar serviços de custódia para criptoativos, i.e., o armazenamento seguro e a gestão das chaves privadas dos clientes, garantindo a segurança dos seus ativos digitais, fornecendo, assim, um ambiente confiável e regulamentado para que os seus clientes mantenham os criptoativos de que são proprietários[102].

Além disso, graças à tecnologia *blockchain*, os criptoativos comportam o potencial de simplificar pagamentos e remessas internacionais. Desse modo, os bancos começaram a analisar a utilização de criptoativos com vista ao melhoramento da eficiência, velocidade e custo-efetividade das transações internacionais, o que pode ser particularmente benéfico em regiões com acesso limitado a serviços bancários tradicionais.

---

[101] O Bank of America permite aos seus clientes que invistam em criptoativos de uma das suas subsidiárias, a Merrill Edge, uma plataforma de negociação eletrónica lançada em 2010, o Chase Bank permite que os utilizadores se liguem à bolsa Coinbase para comprar e vender criptoativos, a Goldman Sachs, em 2022, começou a oferecer aos clientes interessados acesso aos fundos Ethereum emitidos pela Galaxy Digital (CreditDonkey, 2022)

[102] Em Portugal, o Bison Bank, S.A. lançou uma subsidiária em janeiro de 2023, a Bison Digital Assets, que oferece serviços de depósito, troca, levantamento e custodia de criptoativos, tornando-se, assim, no primeiro prestador de serviços de ativos virtuais detido por um banco em Portugal (Jornal de Negócios, 2023)

Depois, de forma a poderem manter-se competitivos e devidamente adaptados às preferências em constante mudança dos clientes, os bancos tradicionais começaram a explorar parcerias e colaborações com empresas *fintech* e *startups* de *blockchain*, que visam aproveitar os avanços tecnológicos da indústria de criptoativos para desenvolver soluções financeiras inovadoras.

2.7. Formas de branquear capitais utilizando criptoativos

O branqueamento de capitais com recurso a criptoativos pode ocorrer de várias maneiras, sendo que, ao criminoso, basta ter imaginação.

Por exemplo, através da utilização de empresas de câmbio não regulamentadas, que não cumpram práticas antibranqueamento de capitais e não efectuem verificações de identidade rigorosas e completas, é possível efectuar transacções de criptoativos sem uma forma apropriada de identificação, permitindo, assim, a livre transação de criptoativos pelo mercado financeiro[103].

Ou, então, por recurso à técnica denominada "*exchange hopping*", onde os criminosos permutam frequentemente criptoativos através de várias plataformas de câmbio com o objetivo de criar uma rede de transacções complexa. Abrindo contas em várias destas empresas, os fundos são transferidos através de diferentes plataformas, o que torna difícil seguir o rasto do dinheiro.

Podem, ainda, ser criadas de empresas de fachada que operem no setor de criptoativos de forma a justificar as transações financeiras ilícitas como transações comerciais legítimas.

Uma outra técnica conhecida é o recurso aos criptoativos de privacidade, como o Monero ou o Zcash, que utilizam técnicas criptográficas avançadas, projetadas especificamente para ocultar endereços de envio, montantes das transações e outras informações identificadoras.

E, talvez a forma mais óbvia, a utilização dos criptoativos na compra de bens e serviços, com posterior venda dos bens de forma a obter moeda fiduciária, tornando os fundos aparentemente legítimos.

[103] Todavia, também é possível utilizar empresas de câmbio legítimas e aplicar várias técnicas para contornar os processos de verificação (através da utilização de documentos de identificação falsos, por exemplo).

Vão, de seguida, explorar-se outras técnicas que, devido à sua maior complexidade, merecem uma explicação mais detalhada.

2.7.1. Serviços de mistura de transações

Um *mixer* (ou misturador) é um serviço *online* que reúne criptoativos detidos por diversos utilizadores, devolvendo, posteriormente, criptoativos "limpos", em diferentes montantes, a fim de que seja ocultado o rasto do dinheiro “sujo”.

Por recurso aos *mixers* ou *tumblers* podem ser quebradas a ligações entre os endereços de envio e os endereços de receção dos criptoativos, obscurecendo, desta forma, o rasto até à fonte original e melhorando simultaneamente o anonimato das transações[104].

Estruturar as transacções desta forma torna mais difícil para as autoridades policiais e para os investigadores o mapeio eficaz do fluxo de fundos oriundos de actividades criminosas[105].

A Europol[106] já reconheceu esta forma de esconder o rasto criminoso dos criptoativos enquanto uma técnica de ofuscação comum, exatamente por aumentar a privacidade das transacções, quebrando as ligações entre o endereço original e o endereço final através da utilização de carteiras intermediárias.

2.7.2. *Coinjoin*

Semelhante aos serviços de mistura analisados no ponto anterior, o recurso a este tipo de tecnologia de ocultação envolve a colaboração de vários

[104] (Cuervo, et al., 2020 p. 6)
[105] (Hudson Inteligence, LLC)
[106] (Europol, 2021 p. 10)

utilizadores, que se juntam para gerar uma transação agregada que inclui múltiplas entradas e saídas, com o objetivo de ofuscar o histórico de transações.

Ao observador externo não é possível criar uma correspondência entre os participantes de uma qualquer transação aleatória com as entradas e saídas dos seus fundos, uma vez que se fundem numa pilha de várias fontes e são posteriormente enviados para outros endereços[107].

Ao contrário de outros serviços de mistura, através da técnica Coinjoin, os utilizadores mantêm a custódia dos seus fundos durante todo o processo.

2.7.3. *Peel Chain*

A *peel chain* é uma técnica utilizada para branquear uma grande quantidade criptoativos através de diversas, mas pequenas, transacções. Aqui, uma pequena porção é "descascada" do endereço do sujeito numa transferência de baixo valor, sendo após direccionada para empresas de câmbio, onde são convertidas em moeda fiduciária ou noutro tipo de activos[108].

Quando bem feitas, estas pequenas quantias transferidas para as empresas de câmbio raramente levantam suspeitas, o que dificulta a sua deteção.

2.7.4. *Smurfing*

A técnica de *smurfing* envolve a divisão de grandes somas de dinheiro em quantias mais pequenas, que são depois enviadas através de várias transações.

[107] (Goriacheva A., 2018 p. 3)
[108] (Hudson Inteligence, LLC)

O *smurfing* acrescenta confusão à cadeia de transacções, tornando mais complexo o rastreio dos fundos[109].

Nesta técnica, o primeiro passo consiste na abertura de contas verificadas em empresas de câmbio, com recurso a "mulas" de dinheiro, que atuam como testas de ferro com documentos falsos que, posteriormente, transferem os criptoativos sujos para as empresas de câmbio através da utilização de *tumblers* ou *mixers* (*vide* ponto 2.7.1. *supra*).

A etapa seguinte compreende a abertura de contas bancárias pelos testas de ferro, com recurso a documentos de identificação estrangeiros falsos, para onde, no final, são transferidos os criptoativos previamente transitados para as empresas de câmbio. E isto é possível porque, nesta fase, o dinheiro do crime já foi separado da sua fonte.

2.7.6. Transações P2P

A realização de transações diretamente para outros indivíduos, evitando empresas de câmbio e serviços intermediários, pode dificultar o rastreamento da origem e do destino dos fundos.

As transações P2P fazem-se com recurso a plataformas *online*, de forma a ser possível às pessoas a compra, venda e troca de criptoativos sem o crivo de qualquer supervisão regulamentar[110][111]. São frequentemente utilizados por pessoas que pretendem maximizar a sua privacidade financeira ou evitar o escrutínio dos reguladores governamentais, das autoridades policiais e dos serviços de informações[112].

As plataformas P2P normalmente requerem poucos, ou nenhuns, passos de verificação da identidade de compradores e vendedores. Os proponentes das

[109] (Financial Crime Academy)
[110] (Conselho Europeu (CE); Conselho da União Europeia (CUE), 2022)
[111] A Binance, uma das maiores corretoras de criptoativos do mundo, providencia uma plataforma P2P - (Binance, 2021)
[112] (Hudson Inteligence, LLC)

plataformas P2P afirmam que não precisam de cumprir os regulamentos KYC ou AML porque estão apenas a "facilitar" as transacções, ligando compradores e vendedores, sem processar quaisquer pagamentos fiduciários ou manter fundos sob a sua custódia.

Embora nem todas as transacções P2P sejam ilícitas, a combinação de pagamentos em numerário e de utilizadores anónimos facilita a prática do branqueamento de capitais.

Haffke, Fromberger, & Zimmermann[113] exemplificaram um ciclo complexo da prática de branqueamento de capitais com recurso a criptoativos, que envolve várias das técnicas *supra* analisadas.

O ciclo inicia, então, com a pessoa “P” que, possuindo dinheiro fiduciário originário de atividades ilícitas, o deposita num país com baixos padrões antibranqueamento de capitais. Querendo comprar *tokens* Monero (que lhe proporcionam um nível elevado de anonimato, mas apenas estão disponíveis em mercados de criptoativos), abre uma conta de utilizador num mercado de criptoativos, que lhe dá acesso a uma carteira (chave pública e chave privada), podendo, agora, transferir um certo montante de dinheiro fiduciário da sua conta bancária para o mercado de criptoativos e, aqui, trocar a moeda fiduciária por Bitcoins. Posteriormente, abre uma conta de utilizador noutro mercado de criptoativos, que lhe dá acesso a outra carteira, e troca as Bitcoin por *tokens* Monero.

A pessoa “P” poderia trocar os *tokens* Monero por “dinheiro branqueado” seguindo os mesmos passos na ordem inversa. Como os *tokens* podem ser transferidos através de fronteiras entre diferentes carteiras, a pessoa “P” poderia fazê-lo em qualquer outro país. Alternativamente, poderia transferir os *tokens* para outras pessoas, que depois conduziriam a troca. Além disso, pode ser utilizado um serviço *mixer* ou *tumbler*.

[113] (2020)

Portanto, face ao exposto, é possível retirar duas características que se mostram determinantes para o sucesso de qualquer esquema de branqueamento de capitais utilizando, para o efeito, criptoativos: por um lado, o véu de anonimidade fornecido por este tipo de ativos, que oculta as identidades do remetente, do destinatário e qualquer outro interveniente; por outro, os esquemas modernos apresentados *supra* (e outros tantos que ainda não são conhecidos ou ainda nem sequer foram inventados) destinados a provocar o afastamento entre a origem e o destino dos fundos, ocultando, assim, o rasto das transações.

São estes dois atributos que, em conjunto, tornam qualquer transação com criptoativos indetetável (e, quando detetável, não rastreável).

PARTE II

ENQUADRAMENTO JURÍDICO

1. O GAFI

Em julho de 1989, os chefes de governo dos países do G-7 decidiram, durante a Cimeira Económica Mundial de Paris (Cimeira de Sommet de l'Arche), reforçar as medidas de combate ao branqueamento de capitais e criar o GAFI[114], uma organização intergovernamental global, cujos membros incluem a maior parte dos principais EM da EU.

O GAFI, que não é um organismo democraticamente eleito, é composto por representantes nomeados pelos seus 39 membros, que trabalham com o intento de desenvolver recomendações sobre a forma como os países devem formular políticas de combate ao branqueamento de capitais e outras políticas de vigilância financeira.

Esta estrutura emitiu o seu primeiro conjunto de 40 recomendações em abril de 1990 (revistas em 1996, em 2001, em 2003 e em 2012)[115], que urgiram os países a criminalizar o branqueamento de capitais na aceção da Convenção de Viena, tendo alcançado uma grande aceitação na comunidade internacional[116].

Foram, ainda, adotadas alterações às recomendações do GAFI em outubro de 2018, de forma a esclarecer explicitamente que se aplicam a atividades financeiras que envolvam criptoativos e, outrossim, aos prestadores de serviços conexos.

---

[114] (Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures, 2021)
[115] Embora não sejam vinculativas, se um membro se recusar a implementá-las, podem ser geradas graves consequências diplomáticas e financeiras.
[116] (Cheniaux, 2021 p. 37)

Além disso, em junho de 2019, foi divulgada uma nota interpretativa à Recomendação n.º 15, que veio estabelecer medidas vinculativas para uma regulamentação e supervisão ou monitorização eficazes dos prestadores de serviços de ativos virtuais, que. Ativos virtuais devem ser considerados como "propriedade", "proventos", "fundos" ou outro "valor correspondente" para fins de aplicação das Recomendações da do GAFI e devem ser aplicadas, pelos países, medidas relevantes relativamente aos ativos virtuais e aos VASP's[117].

Desta nota interpretativa, destaca-se, em síntese, o seguinte:

(i) Devem ser devidamente identificados, avaliados e compreendidos pelos países e pelos VASP's quais os riscos de branqueamento de capitais associados às atividades de ativos virtuais e aos prestadores de serviços de ativos virtuais, e, bem assim, deve ser aplicada uma abordagem baseada no risco de forma a garantir a adoção de medidas adequadas para prevenir ou mitigar tais riscos;
(ii) Os VASP's devem ser obrigados a obter licença ou registo para atuar;
(iii) Devem garantidas pelos países a regulamentação, supervisão e monitoração adequadas dos VASP's para fins de prevenção do branqueamento de capitais e do financiamento do terrorismo, em estrito cumprimento das Recomendações relevantes do GAFI;
(iv) Devem ser garantida pelos países a adoção de sanções (criminais, civis ou administrativas), destinadas aos VASP's, que se afigurem proporcionais e dissuasivas do não cumprimento dos requisitos em matéria de branqueamento de capitais e financiamento do terrorismo;
(v) Devem ser cumpridas pelos VASP's as medidas preventivas descritas nas Recomendações 10 a 21;

[117] O GAFI descreve as empresas prestadoras de serviços de ativos virtuais para ou em nome de outra pessoa como um fornecedor de serviços de ativos virtuais (VASP). Em contrapartida, o Regulamento MiCA, conforme adiante se verá, refere-se a estas empresas como prestadores de serviços de criptoativos (CASP). O termo VASP do GAFI é utilizado mais frequentemente fora da UE e o termo CASP foi adotado na região da UE.

(vi) É necessária cooperação internacional em matéria de ativos virtuais no que diz respeito ao branqueamento de capitais, crimes antecedentes e financiamento do terrorismo.

Em junho de 2019, foram lançadas orientações para uma abordagem baseada no risco relativamente aos ativos virtuais e aos prestadores de serviços de ativos virtuais[118], passando a estar incluídos, no âmbito da Recomendação 16 (também conhecida como "*Travel Rule*" ou "Regra de Viagem"), os prestadores de serviços de ativos virtuais.

Esta *Travel Rule* foi desenvolvida com o objetivo de, por um lado, impedir que os terroristas e outros criminosos tivessem acesso ilimitado a transferências de fundos facilitadas eletronicamente[119] e, por outro, para detetar tal utilização abusiva quando ocorra. Aqui, relevam transferências dentro ou fora do território nacional.

Com o alargamento da Recomendação 16 aos VASP's, os países passaram a dever aplicar tais orientações independentemente de o valor da transferência eletrónica tradicional ou da transferência de ativos virtuais ser expresso em moeda fiduciária ou em ativos virtuais. Desta feita, passou a ser recomendado aos países o asseguramento da obtenção e conservação das informações sobre o ordenante e o beneficiário das operações com VASP's[120].

[118] (Financial Action Task Force (FATF))
[119] A Recomendação 16 define "transferências eletrónicas" como qualquer transação que seja efetuada em nome de um ordenante, através de uma instituição financeira, por meios eletrónicos, com vista a colocar um montante de fundos à disposição de um beneficiário, numa instituição financeira beneficiária, independentemente de o ordenante e o beneficiário serem a mesma pessoa.
[120] Estas informações incluem: o nome do ordenante ou do cliente ordenante; o número da conta ou da carteira VA do ordenante utilizada para processar a transação, no endereço físico (geográfico) do ordenante, o número de identidade nacional, ou número de identificação do cliente que identifique inequivocamente o ordenante perante a instituição ordenante, ou a data e o local de nascimento; o nome do beneficiário; e o número da conta ou da carteira VA do beneficiário utilizada para processar a transação.

Em junho de 2022, o GAFI lançou um relatório sobre a atualização específica da aplicação das suas recomendações sobre ativos virtuais e prestadores de serviços de ativos virtuais[121].

Este relatório foca-se na implementação da *Travel Rule*, da Recomendação 15 e da sua Nota Interpretativa, bem como nos riscos emergentes e desenvolvimentos do mercado que continua a monitorizar, como o fenómeno DeFi, NFT's e carteiras não hospedadas.

O GAFI, neste documento, informou que, embora alguns países tenham adotado medidas significativas para cumprir os requisitos, a aplicação das recomendações continua a ser deficiente a nível mundial, o que conduz à arbitragem jurisdicional.

De acordo com este Relatório, a maioria esmagadora das jurisdições ainda não implementou totalmente os requisitos da Recomendação 15 e da sua Nota Interpretativa (que, como vimos, que estabelecem as normas globais de AML para ativos virtuais e VASP's).

Como resultado: *(i)* das 53 jurisdições que avaliou desde junho de 2021, concluiu que a maioria ainda precisa fazer melhorias significativas ou moderadas quanto à aplicação da Recomendação 15, especialmente em relação à avaliação de riscos de branqueamento de capitais e de financiamento do terrorismo e à aplicação de medidas preventivas; *(ii)* até março de 2022, embora 29 das 98 jurisdições que responderam tenham relatado ter aprovado legislação sobre a *Travel Rule*, apenas 11 jurisdições iniciaram medidas de aplicação e supervisão; e *(iii)* apesar de cerca de um quarto das jurisdições que responderam estar em processo de aprovação da legislação relevante, cerca de um terço (36 das 98) ainda não começou a implementar a *Travel Rule*, o que deixa os ativos virtuais e os VASP's vulneráveis a abusos e demonstra a necessidade urgente de as jurisdições acelerarem a implementação e a aplicação.

[121] (Finantial Action Task Force (FATF))

Assim, neste Relatório, o GAFI apela aos países que tomem medidas no sentido de adotar urgentemente as medidas adequadas em termos de avaliação dos riscos, legislação, registo ou licenciamento, supervisão, aplicação da *Travel Rule*, sanções em conformidade com as decisões políticas, cooperação nacional e internacional e outros requisitos.

Para tanto, insta-os, de forma a garantir o cumprimento das normas AML, a aplicar medidas de identificação dos VASP's, a supervisão e regulamentação dos VASP's, o estabelecimento de diretrizes que ajudem os VASP's a cumprir as normas AML, o cumprimento de sanções, medidas preventivas de luta contra o branqueamento de capitais, incluindo a *Travel Rule*, e o cumprimento das sanções financeiras específicas.

O Relatório menciona várias razões para a fraca aplicação das recomendações do GAFI, nomeadamente as diferenças nos requisitos de jurisdição (o problema sunrise[122]), a questão da diligência devida da contraparte VASP e problemas com as ferramentas de conformidade com a *Travel Rule*.

[122] Este problema refere-se aos atrasos na aplicação da *Travel Rule*. De acordo com o GAFI, a implementação desta regra resultou em diferentes períodos de transição e de aplicação nas
jurisdições.

2. Evolução jurídica do tratamento do branqueamento de capitais na Europa

Passamos, então, a referir sumariamente alguns dos mais importantes mecanismos europeus no âmbito da previsão, prevenção e repressão da prática de branqueamento de capitais e, num momento posterior, aqueles que passaram a prever as transações com criptoativos.

2.1. Recomendação n.º (80) 10

O Comité de Ministros do Conselho da Europa adotou a Recomendação n.º (80) 10 em 27 de junho de 1980 relativa às disposições contra a transferência e a dissimulação de fundos de origem ilícita, o primeiro instrumento internacional contra o branqueamento de capitais.

Esta recomendação, para além de afirmar que o sistema bancário deveria assumir um papel preventivo eficaz na luta contra o branqueamento de capitais "[c]*onsiderando que a transferência de fundos de origem criminal de um país para outro e o processo através do qual os fundos são branqueados por meio da inserção no sistema económico dão origem a problemas sérios, encorajando a perpetração de mais atos criminais e, assim, causar o alargamento deste fenómeno a nível nacional e internacional*"[123], recomendou aos Governos nacionais que providenciassem *(i)* a adoção, por parte dos bancos, de medidas de averiguação e de controlo da identidade dos seus clientes, *(ii)* o estabelecimento de cooperações nacionais e internacionais entre os bancos e as autoridades competentes (no que diz respeito à troca de informações sobre a circulação de notas utilizadas em delitos e no seguimento dos seus movimentos), e *(iii)* a criação de tecnologia que permitisse aos bancos consultar a lista de notas utilizadas em ligação com infrações penais.

[123] Disponível em https://ms.hmb.gov.tr/uploads/sites/2/2019/04/R8010.pdf

2.2. Declaração de Princípios do Comité de Basileia

A Declaração de Princípios do Comité de Basileia sobre as regras e práticas de controlo das operações bancárias[124], de 12 de dezembro de 1988, reconheceu que as instituições bancárias, mesmo que inconscientemente, eram passíveis de serem utilizadas como intermediários das operações de branqueamento e atividades conexas.

Deste modo, impulsionou os bancos a colocar em prática procedimentos eficazes que assegurassem a devida identificação de pessoas que realizassem negócios com as suas instituições, que desencorajassem todas as transações que não parecessem legítimas e que a cooperação com as agências de aplicação da lei fosse alcançada.

2.3. Convenção de Viena das Nações Unidas

A Convenção das Nações Unidas Contra o Tráfico Ilícito de Estupefacientes e de Substâncias Psicotrópicas ("Convenção de Viena das Nações Unidas")[125], de 1988, compeliu, pela primeira vez, os Estados, a criminalizar as atividades de branqueamento de capitais, apesar de se ter limitado aos casos de bens provenientes da prática de crimes relacionados com o tráfico de drogas e de substâncias estupefacientes[126].

Para além de dar ênfase à necessidade da cooperação internacional para o sucesso do combate ao tráfico de drogas e à criminalidade organizada, esta Convenção revelou um esforço no sentido de harmonizar as legislações nacionais, regulou a apreensão e perda dos produtos obtidos e dos instrumentos

[124] Disponível em https://www.bis.org/publ/bcbsc137.pdf
[125] Ratificada pelo Decreto do Presidente da República n.º 45/91, de 06 de junho e publicada no Diário da República I-A, n.º 205, de 06 de junho de 1991
[126] Artigo 3.º da Convenção

utilizados na atividade criminosa e, ainda, sugeriu aos Estados que considerassem a possibilidade de inverter o ónus da prova quanto à origem ilícita dos presumíveis produtos ou bens que pudessem ser objeto de perda.

De acordo com Anabela Miranda Rodrigues[127], "[a] *Convenção de Viena das Nações Unidas contém a primeira definição de branqueamento, sem o nomear expressamente, enunciando os comportamentos que o configuram (artigo 3.º, n.º 1, alínea b)"*, *e que podem descrever-se de acordo com três fases de execução: a primeira, de conversão ou transferência de bens – o chamado placementstage –, em que quem a efetua sabe que estes provêm (de crimes que relevam do âmbito) do tráfico de estupefacientes, com o objetivo de ocultar ou dissimular a origem ilícita dos bens ou de auxiliar qualquer pessoa que esteja implicada no cometimento de um daqueles crimes a eximir-se às consequências jurídicas dos seus atos; a segunda fase é a de ocultação ou dissimulação da natureza, da origem, da localização, disposição, movimentação ou titularidade ou outros direitos respeitantes aos bens – o chamado layeringstage –, sabendo o autor que estes provêm (de crimes que relevam) do âmbito do tráfico de estupefacientes; a terceira e última fase é descrita como a aquisição, detenção ou utilização de bens – o chamado integrationstage – por parte de quem sabe, no momento em que os recebe, que provêm (de crimes que relevam do âmbito) do tráfico de estupefacientes*".

2.4. Convenção Europeia n.º 141 relativa ao branqueamento, deteção, apreensão e perda dos produtos do crime

Em novembro de 1990 foi aprovada, em Estrasburgo, a Convenção Europeia n.º 141, relativa ao branqueamento, deteção, apreensão e perda dos produtos do crime[128], que exigiu aos países signatários *(i)* a implementação de

[127] (2017 p. 116)
[128] Convenção ratificada por Portugal pelo Decreto do Presidente da República n.º 73/97, de 13 de dezembro, e publicada no Diário da República I-A, n.º 287, de 13 de dezembro de 1997 (Resolução da Assembleia da República n.º 70/97), no qual Portugal

legislação e medidas adequadas para combater o branqueamento de capitais, *(ii)* incentivou a cooperação entre as autoridades competentes dos países membros, facilitando a troca de informações, a assistência mútua e a colaboração em investigações relacionadas ao branqueamento de dinheiro e *(iii)* estabeleceu critérios e procedimento para a apreensão e confisco dos produtos do crime, visando privar os criminosos dos lucros ilegais e prevenir que tais bens fossem usados para financiar atividades criminosas futuras.

2.5. Primeira Diretiva antibranqueamento de capitais

Em junho de 1991 foi aprovada, pelo Conselho das Comunidades Europeias, a Diretiva 91/308/CEE (doravante, "AMLD1"), relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais[129], que *(i)* forneceu uma definição de operações que constituem branqueamento de capitais[130], *(ii)* estabeleceu medidas e obrigações para os EM prevenirem a

formulou a seguinte declaração relativamente ao artigo 6.º da Convenção " *o âmbito da punição da infração de branqueamento é restrita aos casos de prática dos crimes de tráfico de droga e outras atividades ilícitas relacionadas, terrorismo, tráfico de armas, extorsão de fundos, rapto, lenocínio, corrupção, peculato e participação económica em negócio, administração danosa em unidade económica do sector público, fraude na obtenção ou desvio de subsídio, subvenção ou crédito, infrações económico-financeiras cometidas de forma organizada com recurso à tecnologia informática e infrações económico-financeiras de dimensão internacional, quando cometidas sob qualquer forma de comparticipação, tal como definidos na sua legislação* [nota: esta reserva foi retirada]."

[129] Transposta em Portugal pelo Decreto-Lei n.º 313/93, de 15 de outubro

[130] "*Conversão ou transferência de bens, com conhecimento por parte daquele que as efectua, de que esses bens provêm de uma actividade criminosa ou da participação numa actividade dessa natureza, com o fim de encobrir ou dissimular a origem ilícita dos mesmos ou de auxiliar quaisquer pessoas implicadas nessa actividade a furtar-se às consequências jurídicas dos seus actos, dissimulação ou encobrimento da verdadeira natureza, origem, localização, utilização, circulação ou posse de determinados bens ou de direitos relativos a esses bens, com conhecimento pelo autor de que tais bens provêm de uma actividade criminosa ou da participação numa actividade dessa natureza, aquisição, detenção ou utilização de bens, com conhecimento, quando da sua recepção, de que provêm de uma actividade criminosa ou da participação numa actividade dessa natureza, a participação num dos actos referidos nos pontos anteriores, a associação para praticar o referido acto, as tentativas de o perpetrar, o facto de ajudar, incitar ou aconselhar alguém a praticá-lo ou o facto de facilitar a sua execução.*"

utilização do sistema financeiro para efeitos de branqueamento de capitais e *(iii)* iniciou o processo de imposição de obrigações específicas em matéria de branqueamento de capitais a elementos do sector privado[131], nomeadamente em matérias de identificação de clientes e transações suspeitas.

Com um pendor essencialmente preventivo, dirigida ao sistema financeiro, impondo obrigações destinadas a prevenir e detetar operações de branqueamento, esta Diretiva instou os EM a proibir o branqueamento de capitais, mas sem exigir a sua incriminação penal[132].

A AMLD1 estabeleceu, ainda, que o crime antecedente do branqueamento de capitais deveria ser compreendido de acordo com o disposto no artigo 3.º, n.º 1, alínea a), da Convenção de Viena (ou seja, no âmbito do tráfico de estupefacientes), mas permitiu a cada EM o alargamento de crimes antecedentes a outras atividades criminosas[133].

2.6. Convenção das Nações Unidas contra o Crime Organizado Transnacional

A Convenção das Nações Unidas contra o Crime Organizado Transnacional, ou "Convenção de Palermo"[134], um tratado internacional adotado pelas Nações Unidas em 2000, entre outras coisas, *(i)* instou a adoção de medidas legislativas (e outras medidas consideradas necessárias) para criminalizar e reprimir o branqueamento de capitais, *(ii)* encorajou a cooperação entre os Estados no rastreamento, apreensão e confisco dos produtos do crime, incluindo os bens provenientes do branqueamento de capitais, *(iii)* incentivou a

[131] Tal como nas 40 Recomendações do GAFI, esta diretiva visava os bancos como as principais entidades obrigadas do sector privado (denominadas como "estabelecimentos de crédito" e "instituições financeiras").
[132] (Viegas, et al., 2022)
[133] (Rodrigues, 2017 p. 118)
[134] Ratificada em Portugal pelo Decreto do Presidente da República n.º 19/2004, de 02 de abril, publicada no Diário da República I-A, n.º 79, de 02 de abril de 2004 (Resolução da Assembleia da República n.º 32/2004) e incorporada no direito interno com o Decreto-Lei n.º 15/93, de 22 de Janeiro.

cooperação na troca de informações financeiras relevantes e na assistência mútua em investigações e processos judiciais relacionados ao branqueamento de capitais, *(iv)* destacou a importância da prevenção do branqueamento de capitais *(v)* e insistiu com a adoção de medidas adequadas a garantir que o setor financeiro fosse regulado e supervisionado de forma eficaz, a fim de prevenir o uso indevido de instituições financeiras para fins de branqueamento de capitais.

2.7. Decisão-Quadro 2001/500/JAI

A Decisão-Quadro 2001/500/JAI[135] do Conselho relativa ao branqueamento de capitais, à identificação, deteção, congelamento, apreensão e perda dos instrumentos e produtos do crime, de 26 de junho de 2001, estabeleceu medidas comuns para combater o branqueamento de capitais e, bem assim, identificar, detetar, congelar, apreender e confiscar os instrumentos e produtos do crime.

Esta Decisão-Quadro incentivou, ainda, a cooperação entre os EM, a Interpol e o GAFI e destacou a importância da prevenção do uso indevido do sistema financeiro para fins de branqueamento de capitais.

2.8. Segunda Diretiva antibranqueamento de capitais

A Diretiva 2001/97/CE do Parlamento Europeu e do Conselho, adotada em dezembro de 2001[136] (doravante, "AMLD2"), teve como objetivo o fortalecimento dos esforços da UE no combate ao branqueamento de capitais, estabelecendo, para o efeito, uma série de requisitos e medidas, que consistiram *(i)* na

[135] Tendo sido posteriormente aprovadas a Decisão-Quadro n.º 2003/577/JAI (que veio permitir a execução, na União Europeia, das decisões de congelamento de bens ou de provas) e a Decisão-Quadro n.º 2005/212/JAI (relativa à perda de produtos, instrumentos e bens relacionados com o crime).
[136] Transposta em Portugal pela Lei n.º 11/2004, de 27 de março

ampliação dos setores abrangidos pela regulamentação antibranqueamento de capitais[137], *(ii)* na introdução da obrigatoriedade de identificar os clientes (o chamado KYC), *(iii)* na manutenção de registos de identificação de clientes, transações e correspondências, *(iv)* no relato de transações suspeitas e *(v)* no reforço da cooperação entre autoridades nacionais e internacionais.

Como vimos, a AMLD1 centrou-se nos fundos provenientes de crimes relacionados com droga, embora dando a cada EM a liberdade para aumentar o leque. Todavia, a presente Diretiva alargou efetivamente o seu âmbito de aplicação, de modo a incluir o crime de corrupção, e tendo, inclusive, introduzido a faculdade de congelar os bens provenientes de atividades criminosas.

2.9. Terceira Diretiva antibranqueamento de capitais

A Diretiva 2005/60/CE do Parlamento Europeu e do Conselho (doravante, "AMLD3"), adotada em 26 de outubro de 2005[138], introduziu o conceito de abordagem baseada no risco e ampliou o escopo dos requisitos de identificação de clientes, dos registos de identificação de clientes, transações e correspondências, dos poderes das unidades nacionais de inteligência financeira e as exigências de cooperação internacional.

Para além do sector financeiro, esta Diretiva aplicou-se também a determinados sectores não financeiros, incluindo advogados, notários, contabilistas, agentes imobiliários, prestadores de serviços de jogos de azar, prestadores de serviços a sociedades e fundos fiduciários e a todos os fornecedores de bens quando os pagamentos fossem efetuados em numerário num montante superior a 15.000.00 € (quinze mil euros).

A AMLD3 teve um impacto muito maior no processo KYC do que as Diretivas anteriores, na medida em que estabeleceu medidas concretas para

[137] Alargamento do âmbito de aplicação às empresas de investimento e empresas de câmbio
[138] Transposta em Portugal pela Lei n.º 25/2008, de 5 de junho

determinar a verdadeira identidade dos clientes, comunicar transações suspeitas e criar sistemas preventivos nas suas organizações.

Em concreto, entre outras coisas, as entidades sujeitas à Diretiva em apreço passaram a ser obrigadas a identificar e verificar a identidade dos seus clientes ("*customer due diligence*") e dos respetivos beneficiários efetivos, a controlar as suas relações comerciais com os clientes e a comunicar suspeitas de branqueamento de capitais ou de financiamento do terrorismo às autoridades públicas, por norma, à unidade nacional de informação financeira.

A Diretiva introduziu, ainda, requisitos e salvaguardas adicionais ("*enhanced due diligence*") para situações que representassem um risco mais elevado de branqueamento de capitais e de financiamento do terrorismo, como sejam, por exemplo, transações com bancos correspondentes situados fora da UE.

Porém, não obstante ser referido no Considerando 41 da Diretiva que "[a] *importância do combate ao branqueamento de capitais e ao financiamento do terrorismo deve levar os Estados-Membros a estabelecerem sanções efectivas, proporcionadas e dissuasivas no direito nacional para o caso de incumprimento das disposições nacionais adoptadas nos termos da presente directiva. Deverão ser previstas sanções para as pessoas singulares e para as pessoas coletivas*", os EM não estavam vinculados a adotar sanções penais[139].

2.10. Quarta Diretiva antibranqueamento de capitais

A Diretiva 2015/849 do Parlamento Europeu e do Conselho, adotada em 2015 e com data de entrada em vigor em junho de 2017[140] (doravante, "AMLD4"), substituiu a anterior Diretiva 2005/60/CE, a AMLD3, e introduziu várias mudanças e atualizações significativas em relação à Diretiva anterior,

[139] (Rodrigues, 2017 p. 115)
[140] Transposta em Portugal pela Lei n.º 83/2017, de 18 de agosto (parcialmente) e pela Lei n.º 89/2017, de 21 de agosto (Capítulo III).

nomeadamente, incluindo uma variedade mais ampla de setores e de profissionais sujeitos às obrigações de prevenção do branqueamento de capitais, estabelecendo requisitos mais rigorosos para a realização de diligências de identificação da identidade de clientes e beneficiários efetivos, reforçando as obrigações de reporte de transações suspeitas, e exigindo a criação de registos centrais de beneficiários efetivos.

Esta Diretiva veio *(i)* reforçar as regras relativas à identificação dos clientes (em particular, dos beneficiários efetivos de empresas e centros de interesses coletivos sem personalidade jurídica), *(ii)* exigir que as informações sobre o proprietário legal das empresas fossem conservadas num registo central em cada EM[141], *(iii)* reforçar a sensibilização e capacidade de resposta relativamente aos riscos de branqueamento de capitais e financiamento do terrorismo, uma vez que, além das avaliações de risco nacionais realizadas pelos Estados-Membros da UE, a CE também passou a efetuar uma avaliação dos riscos de branqueamento de capitais e de financiamento do terrorismo relacionados com atividades transfronteiriças a que estivesse exposto o mercado interno, *(iv)* introduzir uma política coordenada a nível europeu para lidar com a situação dos países não pertencentes à UE e que não dispusessem de regimes eficientes para combater o branqueamento de capitais e o financiamento do terrorismo, a fim de proteger o sistema financeiro da EU[142], e *(iv)* reforçar e melhorar a cooperação entre unidades de informação financeira, os principais agentes na luta contra o branqueamento de capitais e o financiamento do terrorismo[143].

Por outro lado, as entidades sujeitas aos termos da Diretiva[144] deveriam *(i)* comunicar suspeitas de branqueamento de capitais ou de financiamento do

[141] Como, por exemplo, um registo comercial, um registo das sociedades ou registo público.
[142] A primeira lista da UE de «países terceiros de risco elevado» foi adotada através de um ato delegado da Comissão em julho de 2016.
[143] (União Europeia (UE), 2021)
[144] Instituições de crédito, instituições financeiras, empresas e profissões não financeiras designadas (auditores, técnicos de contas externos consultores fiscais, notários e advogados, em determinadas circunstâncias, agentes imobiliários, comerciantes de bens (por exemplo, pedras e metais preciosos quando lidam com pagamentos em

terrorismo às autoridades públicas (regra geral, à unidade de informação financeira), *(ii)* adotar medidas de apoio, tais como assegurar a devida formação do pessoal e a criação de políticas e procedimentos internos de prevenção apropriados e *(iii)* adotar salvaguardas adicionais, medidas de diligência reforçada quanto à clientela para situações de risco mais elevado, como as transações com bancos localizados fora da UE e, nomeadamente, em transações com entidades singulares ou coletivas estabelecidas em países terceiros identificados pela Comissão como países terceiros de risco elevado.

De acordo com Anabela Rodrigues[145], "[o] *que se tornou, assim, claro, com a adoção da quarta Diretiva, é que, no âmbito da vigência das anteriores diretivas, se nada impedia os legisladores nacionais de utilizar o meio penal para assegurar a efetividade da política de prevenção e luta contra o branqueamento decorrente da adoção das diretivas vigentes no âmbito comunitário, o facto é que não estavam aqueles vinculados a fazê-lo*".

2.11. A quinta Diretiva antibranqueamento de capitais

A adoção da Diretiva 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018 (doravante, "AMLD5")[146], alterou a AMLD4 e teve de ser transposta para o direito nacional dos EM até 10 de janeiro de 2020.

Esta Diretiva *(i)* previu o alargamento do âmbito da AMLD4 aos prestadores de serviços de troca entre moedas virtuais e moedas fiduciárias e prestadores de carteiras de custódia, *(ii)* alargou o acesso às informações relativas aos beneficiários efetivos, aumentando a transparência, *(iii)* e reforçou a cooperação entre as unidades de informação financeiras, autorizando-as a partilhar mais informações.

---

numerário de montante igual ou superior a € 10.000,00 – dez mil euros-, prestadores de serviços de jogo).

[145] (2017 p. 115)

[146] Transposta em Portugal pela Lei 58/2020, de 31 de agosto.

Tais alterações à Diretiva anterior tiveram como objetivo reduzir o anonimato e melhorar a rastreabilidade das transações, exigindo às corretoras de criptoativos e aos fornecedores de carteiras virtuais na UE que procedessem à identificação dos clientes e empreendessem as devidas diligências.

A Diretiva em apreço evidenciou o facto de os prestadores de serviços de câmbio entre moedas virtuais e moedas fiduciárias e os prestadores de serviços de custódia de carteiras digitais não se encontrarem obrigados pela UE a identificar atividades suspeitas e que, desse modo, os grupos terroristas tinham à sua inteira disponibilidade a possibilidade de transferir dinheiro para o sistema financeiro da UE ou, no âmbito de redes de moeda virtual, dissimular as transferências ou beneficiar de um certo grau de anonimato nessas plataformas[147].

Daí, foi retirada a conclusão de se afigurar necessário alargar o âmbito de aplicação da AMLD4, de modo a ali incluir os prestadores de serviços cuja atividade consistisse na realização de serviços de câmbio entre moedas virtuais e moedas fiduciárias e os prestadores de serviços de custódia de carteiras digitais. Às autoridades competentes deveria passar a ser possível acompanhar a utilização de moedas virtuais, permitindo, assim, uma abordagem equilibrada e proporcional, salvaguardando o progresso tecnológico e o elevado nível de transparência alcançado em matéria de financiamento alternativo e empreendedorismo social.

A Diretiva reconheceu, ainda, que o fator "anonimidade", típico dos criptoativos, torna possível a sua potencial utilização abusiva para fins criminosos. Admitiu, no entanto, que a inclusão de prestadores de serviços cuja atividade consistisse na realização de serviços de câmbio entre moedas virtuais e moedas fiduciárias e prestadores de serviços de custódia de carteiras digitais não resolveria totalmente a questão do anonimato ligado a transações de moeda virtual, uma vez que grande parte do contexto da moeda virtual permaneceria

[147] Cfr. Considerando 8.

anónimo, já que os utilizadores também poderiam realizar operações sem tais prestadores[148].

Para combater os riscos relacionados com o anonimato, as UIF nacionais deveriam, então, passar a ser capazes de obter informações que lhes permitissem associar endereços de moeda virtual à identidade do detentor de moedas virtuais, sendo, ainda, aberta a possibilidade de os utilizadores se autodeclararem voluntariamente às autoridades designadas.

No artigo 1.º, a AMLD5 começa por elencar as alterações introduzidas à AMLD4, das quais se destacam, porque relevantes em matéria de criptoativos, em concreto:

(i) O aditamento da alínea g) ao ponto 3), do n.º 1, do artigo 2.º da AMLD4, passando a incluir "Prestadores cuja atividade consista em serviços de câmbio entre moedas virtuais e moedas fiduciárias (…)" (*vide* alínea c) do n.º 2 da AMLD5);

(ii) A inclusão, nos pontos 18 e 19 do artigo 3.º da AMLD4, das definições de "moeda virtual"[149] e de "prestador de serviços de custódia de carteiras"[150], respetivamente (*vide* alínea d) do n.º 2 do artigo 1.º da AMLD5);

(iii) A alteração o n.º 1 do artigo 47.º da AMLD4, epigrafado "Supervisão", passando a sujeitar ao círculo regulatório os prestadores de serviços de câmbio entre moedas virtuais e moedas fiduciárias e os prestadores de serviços de custódia de carteiras

[148] Cfr. Considerando 9.

[149] «*"Moeda virtual": 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 aceite por pessoas singulares ou coletivas como meio de troca e que pode possa ser transferida, armazenada e comercializada por via eletrónica*"»

[150] «"*Prestador de serviços de custódia de carteiras": 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*.»

digitais, em concreto, obrigando ao seu registo (vide n.º 29 do n.º 2 do artigo 1.º da AMLD5).

Porém, conforme bem concluem Robby Houben e Alexander Snyers[151] , desde a adoção da AMLD5, o espaço criptográfico não parou, tendo sido gerados novos criptoativos, surgido novos tipos de serviços relacionados com a criptografia e novos prestadores de serviços entraram no mercado de criptografia.

Ao excluir do seu âmbito de aplicação os serviços de câmbio entre criptoativos e, sobretudo, ao excluir também alguns prestadores de serviços de *mixing* ou *tumbling*, esta Diretiva incide a aplicação dos deveres de prevenção e monitorização das transações com criptoativos, de forma seletiva, na etapa da integração. Assim, o agente que queira ocultar vantagem ilícita sob a forma de *Bitcoin*, por exemplo, terá, à partida, maior facilidade no seu câmbio e mistura do que na sua conversão em moeda fiduciária, momento em que enfrentará contacto com (novas) entidades obrigadas, mas em que poderá estar já na posse de uma *Bitcoin* cuja origem foi já dissimulada[152].

2.12. Diretiva relativa ao combate ao branqueamento de capitais através do direito penal

A 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 define as infrações penais e sanções no domínio do branqueamento de capitais, com vista a facilitar a cooperação policial e judiciária entre os EM da UE e evitar que os criminosos tirem partido de sistemas jurídicos mais brandos.

[151] (2020 p. 9).
[152] (Ramalho, et al., 2020 pp. 104 - 105)

Esta Diretiva teve como objetivo criminalizar o branqueamento de capitais quando este seja praticado de forma intencional e com conhecimento de que o produto era proveniente de uma atividade criminosa[153]. Permitiu, também, aos EM criminalizar o branqueamento de capitais caso o autor da infração suspeitasse ou devesse ter sabido que os bens provinham de uma atividade criminosa[154].

No que diz respeito a criptoativos, embora reconheça que "[a] *utilização de moedas virtuais apresenta novos riscos e desafios na perspetiva do combate ao branqueamento de capitais*"[155], a Diretiva em apreço não faz mais nenhuma referência a este tipo de fenómeno.

2.13. Pacote de propostas legislativas destinadas a reforçar as regras da UE em matéria de combate ao branqueamento de capitais e ao financiamento do terrorismo

Em 20 de julho de 2021, a Comissão apresentou o seu pacote de propostas legislativas destinadas a reforçar as regras da UE em matéria de combate ao branqueamento de capitais e ao financiamento do terrorismo[156]. O pacote é constituído pelos seguintes diplomas:

2.13.1. Regulamento relativo à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo

[153] Para tanto, a Diretiva elenca expressamente, no artigo 3.º, quais os comportamentos que são considerados atividade criminosa, e, bem assim, relevantes para o crime de branqueamento de capitais.
[154] Artigo 3.º, n.º 2.
[155] Cfr. considerando 6.
[156] (Conselho Europeu (CE); Conselho da União Europeia (CUE), 2022)

A Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo (COM/2021/420 final) estabeleceu um conjunto único de regras em matéria de luta contra o branqueamento de capitais e o financiamento do terrorismo com maior clareza e orientação para as empresas que têm de cumprir as obrigações em matéria de luta contra o branqueamento de capitais e o financiamento do terrorismo ("entidades obrigadas").

2.13.2. Proposta de Regulamento que cria a Autoridade da UE para o Combate ao Branqueamento de Capitais – a AMLA.

A Comissão Europeia apresentou a Proposta de Regulamento do Parlamento Europeu e do Conselho, que cria a Autoridade para o combate ao branqueamento de capitais e ao financiamento do terrorismo e altera os regulamentos (UE) n.º 1093/2010, (UE) 1094/2010 e (UE) 1095/2010 (COM/2021/421 final). Esta proposta é parte integrante do pacote legislativo destinado a aplicar o plano de ação de 2020 para uma política global da União em matéria de prevenção do branqueamento de capitais e do financiamento do terrorismo.

A AMLA foi desenhada para ser o centro de um sistema integrado composto pela própria autoridade e pelas autoridades nacionais com mandato de supervisão em matérias de branqueamento de capitais e financiamento do terrorismo. A autoridade apoiará, igualmente, as UIF da UE e estabelecerá um mecanismo de cooperação entre elas.

De acordo com esta Proposta, as competências da Autoridade no domínio dos criptoativos estão em consonância com o pacote Finança Digital, publicado pela Comissão em 24 de setembro de 2020[157].

[157] P. 5.

Em junho de 2022 o Conselho[158] adotou a sua posição parcial sobre a proposta, acrescentando poderes à Autoridade para supervisionar diretamente certos tipos de instituições de crédito e financeiras, incluindo prestadores de serviços de criptoativos, se forem considerados de risco.

Dada a natureza transfronteiriça da criminalidade, espera-se que a Autoridade dê um contributo forte e útil para a luta contra o branqueamento de capitais e o financiamento do terrorismo. Entre outras tarefas, contribuirá para a harmonização e coordenação das práticas de supervisão nos sectores financeiro e não financeiro, para a supervisão direta das entidades financeiras de alto risco e transfronteiras e para a coordenação das unidades de informação financeira.

2.13.3. Regulamento que reformula o Regulamento das Transferências de Fundos

A Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às informações que acompanham as transferências de fundos e de determinados criptoativos (reformulação) (COM/2021/422 final), o TFR, reconhece que, até ao momento, as transferências de criptoativos foram "[a]*té agora,* ***as transferências de ativos virtuais têm sido deixadas de fora do âmbito de aplicação da legislação da União em matéria de serviços financeiros, expondo os detentores de criptoativos a riscos de branqueamento de capitais*** *e financiamento do terrorismo, uma vez que* ***o dinheiro ilícito pode circular através de transferências de criptoativos****, prejudicando a integridade, a estabilidade e a reputação do setor financeiro e ameaçando o mercado interno da União, bem como o desenvolvimento internacional das transferências de criptoativos"* (destacado nosso)*.*

Continua*,* afirmando que "*as transferências de ativos virtuais estão sujeitas a riscos de branqueamento de capitais e de financiamento do terrorismo*

[158] (European Council; Council of the European Union, 2022)

semelhantes aos que afetam as transferências eletrónicas de fundos, devem ser sujeitas a requisitos da mesma natureza, pelo que se afigura adequado utilizar o mesmo instrumento legislativo para abordar estas questões comuns" [159].

Assim, este regulamento passa a abranger as alterações aos requisitos de processamento das transações e a inclusão no âmbito de aplicação os prestadores de serviços de criptoativos.

De acordo com o Capítulo III da Proposta de Regulamento, os prestadores de serviços de criptoativos devem assegurar a inclusão de informações de identificação do remetente e do destinatário (como o nome, número de conta, endereços, …) nas transferências de criptoativos.

Estes requisitos são comummente conhecidos como "*Travel Rule*" (ou regra de viagem) e, como vimos no ponto 1 *supra*, foram originalmente concebidos pelo GAFI para combater o branqueamento de capitais e o financiamento do terrorismo, bem como para melhorar a rastreabilidade dos fundos.

2.13.4. Sexta Diretiva antibranqueamento de capitais

A Proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos Mecanismos a criar pelos Estados-Membros para prevenir a utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que revoga a Diretiva (UE) 2015/849 (COM/2021/423 final)

A CE reconhece a existência de vulnerabilidades específicas em matéria de combate ao branqueamento de capitais em matérias de emissão de moeda eletrónica, nos serviços de pagamento e na prestação de serviços de criptoativos e, deste modo, permite aos EM que exijam aos prestadores estabelecidos no seu território, cuja sede social esteja situada noutro EM, a nomeação de um

[159] P. 3.

ponto de contacto central, que deve assegurar o cumprimento das regras de prevenção do branqueamento de capitais e de financiamento do terrorismo desses estabelecimentos[160].

2.14. O Pacote de Financiamento Digital

A CE apresentou o Pacote de Financiamento Digital em 24 de setembro de 2020 com o objetivo de garantir que a UE acolhe a revolução digital e a impulsiona com empresas europeias inovadoras na vanguarda, disponibilizando os benefícios do financiamento digital aos consumidores e empresas europeus[161].

Deste pacote destacam-se dois diplomas legislativos relativos a criptoativos, a saber: a Proposta de Regulamento relativo ao mercado de Criptoativos (o MiCA) e a Proposta de Regulamento relativo a um regime-piloto para infraestruturas de mercado baseadas na tecnologia de registo distribuído (DLT Pilot Regime), o Regulamento (UE) 2022/858.

2.14.1. Regulamento relativo a um regime-piloto para infraestruturas de mercado baseadas na tecnologia de registo distribuído (DLT Pilot Regime)

O Regulamento (UE) 2022/858 do Parlamento Europeu e do Conselho, de 30 de maio de 2022, relativo a um regime-piloto para as infraestruturas de mercado baseadas na tecnologia de registo distribuído e que altera os Regulamentos (UE) n.º 600/2014 e (UE) n.º 909/2014 e a Diretiva 2014/65/UE (doravante, "DLT *Pilot Regime*") foi publicado no Jornal Oficial da União Europeia em 02 de junho de 2022.

[160] Considerando 7 e artigo 5.º, epigrafado "Pontos de Contacto"
[161] (European Commission, 2020)

DLT *Pilot Regime* tem uma abordagem semelhante à de uma *regulatory sandbox* (regime opcional), mas com um foco mais específico: apenas a negociação de criptoativos qualificados enquanto instrumentos financeiros em estruturas de mercados.

Com este regulamento pretende-se reduzir as dúvidas sobre se as regras definidas atualmente para os mercados secundários de instrumentos financeiros se adequam inteiramente à tecnologia de registo distribuído e aos criptoativos, ao mesmo tempo que se garante a proteção dos investidores, bem como da integridade do mercado e da estabilidade financeira.

O DLT Pilot Regime permite que as estruturas de mercado que utilizem tecnologias de registo distribuído sejam temporariamente isentas de alguns requisitos específicos ao abrigo da legislação financeira da União Europeia que, de outra forma, poderiam impedi-los de desenvolver soluções para a negociação e liquidação de transações em criptoativos que se qualifiquem enquanto instrumentos financeiros[162].

As autorizações específicas e as isenções deverão ter natureza temporária, por um período máximo de seis anos a contar da data da concessão da autorização específica, e deverão ser válidas apenas durante a vigência do diploma[163].

2.14.2. A proposta de regulamento relativa aos mercados de criptoativos - MiCA (*markets in cryptoassets*)

A CE publicou, no dia 24 de setembro de 2020, uma proposta de Regulamento do Parlamento Europeu e do Conselho referente aos mercados de criptoativos, o MiCA, inserida no Pacote de Financiamento Digital e mandatada pelo plano de Ação da Comissão sobre *Fintech*.

[162] *Cfr*. Considerando 6.
[163] *Cfr*. Considerando 48.

Em 31 de maio de 2023 foi finalmente publicado o Regulamento (UE) 2023/1114, do Parlamento Europeu e do Conselho, relativo aos mercados de criptoativos[164], que procura estabelecer um quadro próprio e harmonizado a nível da União com regras específicas para os criptoativos e as atividades e serviços conexos, clarificando o enquadramento jurídico aplicável.

Este regulamento reconhece que "[q]*uando utilizados como meio de pagamento, os criptoativos podem proporcionar oportunidades para a realização de pagamentos mais baratos, mais céleres e mais eficientes, em particular no contexto transfronteiriço, ao limitarem o número de intermediários*"[165].

Porém, atenta que "*com exceção das regras aplicáveis à luta contra o branqueamento de capitais,* ***não existem regras que se apliquem à prestação de serviços relacionados com tais criptoativos não regulamentados****, nomeadamente no que se refere à operação de plataformas de negociação de criptoativos, à troca de criptoativos por fundos ou outros criptoativos, e à custódia e administração de criptoativos em nome de clientes. A ausência de tais regras deixa os detentores desses criptoativos expostos a riscos, em particular nos domínios não abrangidos pelas regras de proteção do consumidor. A falta de tais regras pode também dar azo a riscos substanciais para a integridade do mercado, nomeadamente em termos de abuso de mercado, mas também em termos de criminalidade financeira*" (destacado nosso)[166].

De acordo com o Conselho Europeu[167], o objetivo desde regulamento é proteger melhor os investidores e regular os riscos relacionados com os criptoativos, estimulando simultaneamente a inovação e reforçando o papel da UE como norma em matéria de política digital.

O Regulamento MiCA classifica os criptoativos em três categorias[168]:

[164] O Conselho e do Parlamento chegaram a um acordo provisório sobre o Regulamento MiCA em junho de 2022 e o Conselho adotou formalmente as regras em maio de 2023.
[165] Cfr. Considerando 2.
[166] *Cfr*. Considerando 4.
[167] (Council of the European Union and the European Council, 2023)
[168] *Cfr*. considerando 18.

(i) “Criptofichas de moeda eletrónica” (ou *e-money tokens* - EMT) - criptoativos que visem estabilizar o seu valor por referência a uma única moeda oficial[169];

(ii) “Criptofichas referenciadas a ativos” (ou *asset referenced tokens* - ART) - criptoativos que visem estabilizar o seu valor por referência a outro valor ou direito, ou a uma combinação de ambos, incluindo moedas oficiais, abrangendo todos os outros criptoativos (excluindo criptofichas de moeda eletrónica) cujo valor seja garantido por ativos;

(iii) Outros criptoativos - um termo genérico que inclui todos os outros criptoativos que não se enquadrem nas duas categorias anteriores, incluindo as criptofichas de consumo (*utility tokens* ou tokens de utilidade).

E classifica e regula especificamente nove serviços relacionados com criptoativos. São eles[170]:

(i) A custódia e administração de criptoativos (a guarda ou controlo de criptoativos, ou da sua chave criptográfica privada, quando aplicável, em nome de terceiros);

(ii) A operação de plataformas de negociação de criptoativos (a gestão de um ou mais sistemas multilaterais);

(iii) A troca de criptoativos por fundos (a compra ou venda de criptoativos em troca de moedas fiduciárias, por oposição a outros criptoativos);

(iv) A troca de criptoativos por outros criptoativos (a compra ou venda de criptoativos em troca de outros criptoativos, por oposição a moedas fiduciárias);

(v) A execução de ordens relativas a criptoativos (serviços de corretagem ou outros serviços de intermediação, como a celebração de um acordo de compra ou venda de criptoativos em nome de terceiros, ou a aceitação de venda de criptoativos no momento da sua emissão);

[169] Assim denominados para efeito do regulamento por considerar que a função destes criptoativos é idêntica à função da moeda eletrónica, uma vez que ambos podem ser substitutos de moedas e notas e utilizados para fazer pagamentos.
[170] Artigos 75.º a 81.º

(vi) A colocação de criptoativos (comercialização, em nome do oferente ou de um emitente, de criptoativos junto dos compradores);
(vii) A receção e transmissão de ordens por conta de terceiros (a receção de uma ordem de uma pessoa para comprar ou vender criptoativos);
(viii) A consultoria sobre criptoativos e gestão de carteiras de criptoativos (a gestão de carteiras de investimento, incluindo criptoativos, em conformidade com os mandatos acordados com os clientes);
(ix) Prestação de serviços de transferência de criptoativos (a transferência de criptoativos de um endereço ou conta DLT para outro).

O MiCA tem um âmbito de aplicação limitado a criptoativos que não possam ser qualificados como[171] *(i)* instrumentos financeiros, à luz da Diretiva relativa aos mercados de instrumentos financeiros (MIFID2); *(ii)* fundos, à luz da PSD2, exceto se configurarem *e-money tokens*; *(iii)* depósitos, à luz da Diretiva relativa aos sistemas de garantia de depósitos; *(iv)* depósitos estruturados, à luz da MIFID 2; *(v)* titularizações, à luz do Regime Geral para a Titularização; e *(vi)* moeda digital de banco central[172]. E determina que a prestação de serviços de criptoativos é proibida se não for devidamente autorizada[173].

Os objetivos da CE com este Regulamento são a criação de um quadro regulatório que defina as regras a aplicar a todos os criptoativos que não estejam abrangidos pela legislação existente no âmbito dos serviços financeiros, fazer a regulação acompanhar a utilização dos criptoativos e da tecnologia DLT, garantir os direitos dos consumidores e investidores em termos análogos aos que são garantidos para outros serviços já regulados no âmbito do setor financeiro e a estabilidade do sistema financeiro, ao serem estabelecidas regras que permitam mitigar os riscos associados à utilização e comercialização de criptoativos.

O MiCA estabelece requisitos uniformes no que respeita a condições de transparência e divulgação para a emissão e admissão à negociação de criptoativos, à autorização e supervisão de prestadores de serviços de

[171] *Cfr*. Considerando 9.
[172] Cfr. Considerando 13.
[173] Crf. Título V.

criptoativos e supervisão emitentes, à operação, organização e governação dos emitentes de ART, de EMT e dos prestadores de serviços de criptoativos, às regras de proteção do consumidor no que respeita à emissão, negociação, troca e custódia de criptoativos e às medidas de prevenção de abusos de mercado destinadas a assegurar a integridade dos mercados de criptoativos.

Com este regulamento, os prestadores de serviços de criptoativos passam a necessitar de uma autorização para operar na UE, a ter de respeitar requisitos para proteger as carteiras dos consumidores e a ser responsabilizados se perderem os criptoativos dos investidores. Ademais, os prestadores de serviços de criptoativos terão também de declarar informações sobre a sua pegada ambiental e climática.

A Autoridade Europeia dos Valores Mobiliários e dos Mercados (European Securities and Markets Authority – ESMA) deverá criar um registo público para prestadores de serviços de criptoativos que operam na União Europeia sem autorização[174].

O regulamento MiCA representa um marco significativo na regulamentação dos criptoativos na União Europeia, buscando trazer maior transparência, segurança e proteção aos consumidores e investidores nesse setor.

[174] Artigo 110.º.

3. Evolução legislativa nos Estados Unidos da América

De seguida, far-se-á um enquadramento da evolução regulatória dos EUA. Embora o foco da presente dissertação seja a pertinência e evolução da legislação europeia em matéria de branqueamento de capitais e, posteriormente, quando sejam utilizados criptoativos, afigura-se importante fazer um enquadramento jurídico da evolução legislativa americana de forma a melhor fazer uma análise comparativa entre as duas e melhor posicionar a iniciativa europeia.

3.1. Lei de Sigilo Bancário

A Lei relativa à manutenção de registos financeiros e à comunicação de transações em moeda e transações estrangeiras (*Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act*), mais conhecida como Lei de Sigilo Bancário (*Bank Secrecy Act*), aprovada pelo Congresso dos Estados Unidos em 1970, foi um importante marco na legislação dos Estados Unidos[175] e constituiu o primeiro e mais abrangente estatuto federal de combate ao branqueamento de capitais e ao financiamento do terrorismo do país.

A Lei de Sigilo Bancário veio autorizar o Secretário do Departamento do Tesouro dos Estados Unidos a emitir regulamentos que exigissem aos bancos e a outras instituições financeiras a adoção de uma série de precauções contra o crime financeiro, incluindo o estabelecimento de programas AML e a apresentação de relatórios previamente determinados considerados com elevado grau de utilidade em investigações e procedimentos criminais, fiscais e regulamentares, e em determinados assuntos de inteligência e contraterrorismo[176].

[175] (United States Government (USG))
[176] (United States Government (USG))

Foi também este diploma que instituiu o FinCEN, a entidade responsável por recolher e analisar informações sobre atividades financeiras suspeitas, e cuja missão é "*proteger o sistema financeiro contra a utilização ilícita, combater o branqueamento de capitais e os e os crimes conexos, incluindo o terrorismo, e promover a segurança nacional através da utilização estratégica das autoridades financeiras e da recolha, análise e divulgação de informações financeiras*"[177].

3.2. Lei de Controlo do Branqueamento de Capitais

A Lei de Controlo do Branqueamento de Capitais (Money Laundering Control Act) de 1986 alterou o código penal federal americano de forma a instituir o branqueamento de capitais como uma infração federal, estabelecendo coimas e sanções a quem, de forma consciente, *(i)* efetuasse uma transação financeira com bens de origem criminosa, *(ii)* efetuasse uma transação comercial que fosse parte de um esquema para ocultar bens de origem criminosa ou para dissimular a origem ou a propriedade de bens de origem criminosa, *(iii)* ou transportasse (ou tentasse) um instrumento monetário ou fundos de um local nos Estados Unidos para ou através de um local fora dos Estados Unidos, ou vice-versa, como parte de um esquema para ocultar bens de origem criminosa ou para dissimular a origem ou a propriedade de bens de origem criminosa[178].

3.3. Lei contra o abuso de drogas

A Lei contra o abuso de drogas (Anti-Drug Abuse Act) de 1988 alargou a definição de "instituição financeira" de modo a incluir empresas como comerciantes de automóveis e agentes imobiliários, obrigando-os a apresentar relatórios sobre transações de grandes montantes em moeda e exigiu a

[177] (Financial Crimes Enforcement Network (FinCen))
[178] (United States Congress (USC))

verificação da identidade dos compradores de instrumentos monetários superiores a USA 3.000,00 (três mil dólares).[179]

3.4. A Lei de Sigilo Bancário (Annunzio-Wylie *Anti-Money Laundering Act*)

A Lei de Sigilo bancário (Annunzio-Wylie *Anti-Money Laundering Act*) foi implementada em 1994 e alterou a Lei de Sigilo Bancário (*Bank Secrecy Act*).

Com este diploma, *(i)* foram reforçadas sanções por infrações à Lei de Sigilo Bancário, *(ii)* foi fortalecido o papel do Departamento de Tesouraria, que passou a estar autorizado a emitir regulamentos a exigir às instituições financeiras, tal como definidas nos regulamentos do BSA, a manutenção de "padrões mínimos" de um programa AML[180] e *(iii)* foi criado o Grupo Consultivo da Lei do Sigilo Bancário (*Bank Secrecy Act Advisory Group*).

3.5. Lei de Supressão do branqueamento de capitais

A Lei de Supressão do branqueamento de capitais (*Money Laundering Suppression Act*), de 1994, exigiu às agências bancárias que *(i)* analisassem e reforçassem a formação e desenvolvessem procedimentos de exame em matéria de combate ao branqueamento de capitais e *(ii)* revissem e melhorassem os procedimentos de encaminhamento de casos para as agências de aplicação da lei apropriadas[181].

[179] (Financial Crimes Enforcement Network (FinCen))
[180] (Anti-Money Laundering Program Effectiveness, 2020 p. 2)
[181] (Financial Crimes Enforcement Network (FinCen))

3.6. Lei sobre a estratégia em matéria de branqueamento de capitais e crimes financeiros

A Lei sobre a estratégia em matéria de branqueamento de capitais e crimes financeiros (*Money Laundering and Financial Crimes Strategy Act*), de 1998, alterou a lei federal de forma a redefinir o branqueamento de capitais e crimes financeiros conexos como *(i)* o movimento de dinheiro ilícito ou de produtos equivalentes a dinheiro para dentro, fora ou através dos Estados Unidos ou através de certas instituições financeiras dos EUA; ou *(ii)* aquele que é significado dado ao abrigo de estatutos penais estatais e locais relativos ao movimento de dinheiro ilícito ou de produtos equivalentes a dinheiro.

Ademais, *(i)* exigiu às agências bancárias o desenvolvimento de formação contra o branqueamento de capitais para os investigadores, *(ii)* impôs ao Departamento do Tesouro e outras agências desenvolvessem uma Estratégia Nacional de Branqueamento de Capitais, e *(iii)* criou as *task forces* de Alta Intensidade para o Branqueamento de Capitais e Áreas de Crime Financeiro Associado (*High Intensity Money Laundering and Related Financial Crime Area*) de forma a concentrar os esforços de aplicação da lei a nível federal, estatal e local em zonas onde o branqueamento de capitais era predominante[182].

3.7. Lei Patriota dos EUA

A Lei Patriota de 2001 (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism - USA Patriot Act*) foi promulgada como resposta aos ataques terroristas de 11 de setembro e teve como objetivo a dissuasão e punição dos atos terroristas nos Estados Unidos e em todo o mundo, o melhoramento dos instrumentos de investigação da aplicação da lei e outros objetivos, entre os quais se inclui o reforçar as

[182] (Financial Crimes Enforcement Network (FinCen))

medidas dos EUA para prevenir, detetar e processar a lavagem de dinheiro internacional e o financiamento do terrorismo.

Esta Lei *(i)* previu a identificação dos clientes que utilizassem contas de correspondente (secção 311), *(ii)* incentivou uma maior cooperação entre as autoridades policiais, as entidades reguladoras e as instituições financeiras para a partilha de informações sobre as pessoas suspeitas de estarem envolvidas em terrorismo ou branqueamento de capitais (secção 314), *(iii)* facilitou a capacidade do governo para apreender fundos ilícitos de indivíduos e entidades localizados em países estrangeiros e exigiu aos bancos dos EUA a manutenção de registos que identifiquem um agente para a citação ou notificação de processos judiciais relativos às suas contas correspondentes (secção 319) e *(iv)* exigiu às instituições financeiras o estabelecimento de programas de combate ao branqueamento de capitais (secção 352)[183].

3.8. Lei da Reforma da Inteligência e Prevenção do Terrorismo

A Lei da Reforma da Inteligência e a Prevenção do Terrorismo (*Intelligence Reform and Terrorism Prevention Act*), de 2004, alterou a Lei do Sigilo Bancário de forma a exigir ao Secretário do Tesouro a elaboração de regulamentos que exijam que certas instituições financeiras comuniquem transmissões eletrónicas transfronteiriças de fundos, se considerar que essa comunicação é "razoavelmente necessária" na luta contra o branqueamento de capitais e o financiamento do terrorismo[184].

3.9. A Lei de Execução da Lei de Sigilo Bancário

Lei de Execução da Lei de Sigilo Bancário (*Bank Secrecy Act Enforcement Act*) foi adotada em 2010, agravou as penalidades para o não cumprimento dos

[183] (Financial Crimes Enforcement Network (FinCen))
[184] (Financial Crimes Enforcement Network (FinCen))

requisitos da Lei do Sigilo Bancário e fortaleceu a aplicação e fiscalização das regulamentações antibranqueamento de capitais.

3.10. Aplicação dos regulamentos do FinCEN às pessoas que administram, trocam ou utilizam moedas virtuais

Em 2013, o FinCEN emitiu a orientação n.º Fin-2013-G001, "*Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*", que teve um impacto direto em todas as pessoas que "*criam, obtêm, distribuem, trocam, aceitam ou transmitem moedas virtuais*", uma vez que as abrigou sob a aplicabilidade da Lei do Sigilo Bancário.

Em concreto, esta orientação estabeleceu que um administrador ou um operador de câmbio que *(i)* aceite e transmita uma moeda virtual convertível[185] ou *(ii)* compre ou venda moeda virtual convertível por qualquer motivo é um transmissor de dinheiro ao abrigo dos regulamentos do FinCEN, exceto se uma limitação ou isenção da definição se aplicar a essa pessoa.

Deste modo, uma pessoa que cria, obtém, distribui, troca, aceita ou transmite moedas virtuais é definido como um transmissor de dinheiro, devendo, assim, estar registado no FinCEN e ser licenciado em qualquer estado em que opere ou conduza negócios.

Em 2017, o SEC lançou um relatório onde concluiu que as ICO's podem estar sob a alçada dos regulamentos de valores mobiliários, afirmando que os emitentes de valores mobiliários baseados em tecnologias DLT ou blockchain devem registar as ofertas e vendas desses valores mobiliários, a menos que se aplique uma isenção válida.

[185] Para efeitos da orientação do FinCen, moeda virtual "convertível" é um tipo de moeda virtual que ou tem um valor equivalente em "moeda real" ou atua como um substituto da "moeda real".

Para tanto, é aplicado o teste Howey, de forma a determinar se certos ativos são valores mobiliários. Independentemente da forma que assuma, um ativo é um valor mobiliário se representar um investimento numa empresa comum com a expetativa de lucro exclusivamente através dos esforços de outros[186].

3.11. Lei contra o branqueamento de capitais

A Lei contra o Branqueamento de Capitais (*Anti-Money Laundering Act* - AMLA), a mais relevante reforma da legislação AML do país desde a Lei Patriota, foi promulgada pelo Congresso em 1 de janeiro de 2021 como parte da Lei de Autorização da Defesa Nacional os EUA.

De entre os seus objetivos mais importantes, esta Lei contém disposições destinadas a *(i)* estabelecer novos requisitos de transparência e divulgação da propriedade efetiva a nível federal *(ii)* alargar o objetivo do BSA e exigir uma revisão do quadro regulamentar antibranqueamento de capitais, *(iii)* promover parcerias público-privadas e oportunidades de envolvimento em questões de branqueamento de capitais e financiamento do terrorismo; *(iv)* introduzir novas opções de pessoal e programas para melhorar as competências em matéria de branqueamento de capitais e financiamento do terrorismo *(v)* promover a cooperação internacional em matéria de criminalidade financeira, protegendo simultaneamente as informações financeiras contra de uso indevido *(vi)* reforçar os instrumentos de aplicação da lei para impedir o branqueamento de capitais e outras formas de criminalidade financeira *(vii)* revigorar as disposições do BSA em matéria de denúncia de irregularidades *(viii)* alargar o âmbito regulamentar do BSA para incluir empresas que prestem serviços que envolvam "valor que substitui a moeda"[187] [188].

---

[186] (Commissioner Hester M. Peirce, 2019)
[187] (Rosen, et al., 2022 p. 2)
[188] *Cfr*. Secções 5312(a), 5318(a)(2) e 5330(d), todas do Título 31, da Divisão F, do *United States Code*.

Em 2019, em data anterior à promulgação da Lei em apreço, o FinCen[189] emitiu uma orientação, na qual incluiu uma explicação ao termo "valor que substitui a moeda", referindo que abrange situações em que a transmissão de valores não envolve moeda ou fundos, mas envolve algo que as partes numa transação reconhecem ter um valor equivalente ou que pode substituir a moeda.

Assim, com a introdução da expressão "valor que substitui a moeda" (no original "*value that substitutes currency*"), foi alargada a definição de instituições financeiras e de entidades prestadoras de serviços de pagamentos de forma a incluir empresas que prestam serviços com ativos virtuais[190].

3.12. Ordem Executiva de 2022

Em março de 2022, o presidente Biden emitiu uma Ordem Executiva, abrindo as hostes para a criação de uma estrutura para regulamentação dos criptoativos nos EUA.

Esta Ordem Executiva representa a primeira abordagem de todo o governo dos americano destinada lidar com os riscos emergentes e aproveitar os benefícios potenciais dos criptoativos e da tecnologia a estes subjacente.

Para tanto, com esta Ordem Executiva estabeleceu uma política nacional em matéria de criptoativos tendo em vista a proteção dos consumidores e dos investidores, a estabilidade financeira, o financiamento ilícito, a liderança dos EUA no sistema financeiro mundial, a competitividade económica, a inclusão financeira e a inovação responsável.

Em concreto, esta Ordem Executiva exigiu medidas para[191]:

(i) Proteger os consumidores, investidores e empresas através do desenvolvimento de recomendações políticas que abordem as

[189] (Financial Crimes Enforcement Network (FinCen), 2019 p. 4)
[190] (Rosen, et al., 2022 p. 7)
[191] (The White House, 2022)

implicações do crescente sector de ativos digitais e incentivar os reguladores a garantir uma supervisão suficiente e a salvaguardar quaisquer riscos financeiros sistémicos colocados pelos ativos digitais;

(ii) Proteger a estabilidade financeira global e dos EUA e mitigar o risco sistémico, encorajando a identificação e mitigação dos riscos financeiros sistémicos colocados pelos ativos virtuais e desenvolvendo recomendações políticas adequadas para colmatar eventuais lacunas regulamentares;

(iii) Mitigar os riscos financeiros ilícitos e de segurança nacional colocados pela utilização ilícita de ativos digitais, orientando um enfoque sem precedentes de ação coordenada em todas as agências governamentais relevantes dos EUA e instruindo as agências a cooperarem de forma garantir que os quadros, capacidades e parcerias internacionais estejam alinhados e respondam às necessidades dos cidadãos;

(iv) Promover a Liderança dos EUA em Tecnologia e Competitividade Económica para Reforçar a Liderança dos EUA no Sistema Financeiro Global, estimulando o estabelecimento de um quadro de investigação, desenvolvimento e abordagens operacionais aos criptoativos;

(v) Promover o acesso equitativo a serviços financeiros seguros e acessíveis, através da elaboração de um relatório sobre o futuro do dinheiro e dos sistemas de pagamento, incluindo as implicações para o crescimento económico, o crescimento financeiro e a inclusão, a segurança nacional e a medida em que a inovação tecnológica pode influenciar esse futuro;

(vi) Apoiar os avanços tecnológicos e assegurar o desenvolvimento e a utilização responsáveis dos ativos virtuais, dando instruções ao Governo dos EUA para tomar medidas concretas para estudar e apoiar os avanços tecnológicos no desenvolvimento, conceção e implementação responsáveis dos sistemas de criptoativos, dando

simultaneamente prioridade à privacidade, à segurança, ao combate à exploração ilícita e à redução dos impactos climáticos negativos;

(vii) Explorar uma Moeda Digital do Banco Central dos EUA, atribuindo urgência à investigação e desenvolvimento a mesma, caso a emissão seja considerada de interesse nacional.

3.13. Proposta Lei de Inovação Financeira Responsável

Em junho de 2022, os EUA emitiram sua proposta mais abrangente sobre a regulamentação de ativos criptográficos, a Proposta de Lei de Inovação Financeira Responsável (ou Lummis-Gillibrand Bill), que contempla uma estrutura regulatória abrangente para criptoativos.

Esta Proposta de Lei possui uma norma clara para determinar quais os ativos digitais que são mercadorias e quais são valores mobiliários, analisando a finalidade do ativo e os direitos ou poderes que transmite ao consumidor, dando às empresas de ativos digitais a capacidade de determinar quais serão as suas obrigações regulamentares e dando aos reguladores a clareza de que necessitam para aplicar as leis existentes em matéria de comércio de valores mobiliários e mercadorias.

Na aceção deste documento, os criptoativos são ativos nativamente eletrónicos, que conferem direitos ou poderes económicos, de propriedade ou de acesso e que são registados através de tecnologia DLT criptograficamente segura (ou qualquer tecnologia semelhante)[192].

Ainda, prevê a atribuição de autoridade regulamentar em matéria de criptoativos à CFTC, de acordo com o pressuposto de que a maioria dos criptoativos são muito mais semelhantes a mercadorias do que a valores mobiliários. Os criptoativos que, de acordo com este diploma, correspondam à definição de mercadoria (como a Bitcoin e o Ether, que representam mais de

[192] Secção 9801, parágrafo 3.º.

metade da capitalização do mercado de criptoativos), serão regulados pela CFTC.

No que à previsão de normas sobre branqueamento de capitais diz respeito, este Projeto Lei propõe[193] *(i)* a adoção, pelo Departamento do Tesouro, a CFTC e o SEC *standards* de avaliação das instituições financeiras relacionados com a prevenção do branqueamento de capitais e da evasão às sanções, *(ii)* o registo, junto do FinCen, dos endereços dos operadores de quiosques e de ATM's criptoativos, *(iii)* o aditamento, pelo FinCEN, de regras relativas à verificação das identidades dos clientes dos quiosques de criptoativos e *(iv)* a imposição de novas sanções em caso de violação intencional das leis AML.

3.14. Proposta de Lei de Combate ao Branqueamento de Capitais e Criptoativos

Em 15 de dezembro de 2022 os senadores Elizabeth Warren e Roger Marshall apresentaram o Projeto de Lei de Combate ao Branqueamento de Capitais com Ativos Digitais com a intenção de mitigar os riscos que os criptoativos representam para a segurança nacional dos EUA, de fechar lacunas na estrutura existente de combate ao branqueamento de capitais e ao combate ao financiamento do terrorismo, e de trazer o ecossistema de ativos digitais em maior conformidade com as regras que regem o resto do sistema financeiro.

Para tanto, este Projeto de Lei prevê[194] *(i)* o alargamento as responsabilidades da Lei do Sigilo Bancário, em particular os requisitos de KYC, a fornecedores de carteiras de ativos digitais, a *miners*, validadores e outros participantes da rede que possam atuar para validar, proteger ou facilitar transações de criptoativos, dando instruções ao FinCEN para designar estes intervenientes como empresas de serviços financeiros, *(ii)* a abordagem à

[193] (Gillibrand, 2023)
[194] (Warren, et al., 2022)

questão das carteiras digitais "não hospedadas"[195], que permitem aos indivíduos o contorno de verificações de AML, instruindo o FinCEN a finalizar e implementar sua regra proposta em dezembro de 2020, que exigiria que aos bancos e às empresas de serviços financeiros a verificação das identidades de clientes e contrapartes, *(iii)* a intenção de proibir as instituições financeiras de utilizarem ou efetuarem transações com *mixers* de criptoativos e outras tecnologias que aumentem o anonimato, bem como de manipularem, utilizarem ou efetuarem transações com criptoativos que tivessem sido tornados anónimos através de tais tecnologias, *(iv)* o reforço da aplicação de conformidade com a Lei de Sigilo Bancário, instruindo o Departamento do Tesouro a estabelecer um processo de análise e revisão da conformidade AML/CFT para os empresas de serviços financeiros e instruindo a Securities and Exchange Commission e a Commodity Futures Trading Commission a estabelecer processos de análise e revisão da conformidade AML para as entidades supervisionadas e *(v)* o alargamento das regras da BSA relativas à comunicação de contas bancárias estrangeiras para incluir criptoativos.

[195] Tipo de carteira que permite ao utilizador manter os seus criptoativos fora de qualquer bolsa, como se mantivesse notas no seu próprio bolso.

PARTE III

Tomada de Posição

Face a todo o exposto, conclui-se que, em matéria de branqueamento de capitais com recurso a criptoativos, o mecanismo americano de referência é a Lei de Sigilo Bancário, encontrando-se ainda em fase preliminar a adoção de normativos específicos e direcionados para o fenómeno dos criptoativos.

Desta feita, é evidente que a UE se encontra na vanguarda no que a esta temática diz respeito, com a aprovação de normativos especificamente concebidos para regular este fenómeno. A questão que, então, se coloca, é a de saber se, porventura, serão suficientes para prevenir e reprimir a prática do crime objeto de estudo.

Mas, antes de avançarmos, importa fazer um parêntesis e sublinhar que os normativos europeus comportam limitações.

O facto de a UE ser composta por 27 Estados-Membros, cada um com seu próprio sistema legal e tradições jurídicas, dificulta a harmonização e aplicação uniforme da legislação em todo o território. Estes EM são soberanos em matéria de legislação, o que significa que certos assuntos podem ser deixados à sua decisão, resultando em diferenças nas leis entre os países.

Depois, o facto de, de um modo geral, os seus normativos primarem pela elevada complexidade e ou, até, o facto de as Diretivas precisarem de ser transpostas, implica que nem sempre todos os países implementam a legislação da mesma forma, o que pode levar a discrepâncias na sua aplicação e enfraquecer a eficácia da legislação.

Com as necessárias adaptações, a legislação americana padece dos mesmos problemas.

Como analisamos ao longo da presente dissertação, os criptoativos surgiram em 2009 com o lançamento da primeira criptomoeda, a *Bitcoin*, e

incorporaram a tecnologia DLT, que, antes de 2017, era considerada uma tecnologia imatura e, bem assim, o seu potencial impacto nos mercados financeiros e possível adoção da tecnologia nos serviços financeiros era tido como pouco claro, pelo que qualquer regulamentação específica era entendida como sendo precipitada[196].

Só a partir de 2017 é que os reguladores começaram a perceber o potencial desta tecnologia para os mercados financeiros, assim como a escala dos riscos envolvidos[197].

A natureza revolucionária dos criptoativos não permitiu uma resposta legislativa e de aplicação imediata. Os processos AML e KYC não foram originalmente concebidos para atender a este fenómeno, no entanto, alguns processos legislativos mais recentes começam a dar conta deste panorama[198].

O MiCA não foi construído com o fito do combate ao branqueamento de capitais com criptoativos, mas estabelece certas regras que, até certo ponto, ajudam a mitigar os riscos neste setor, como a exigência destinada à EBA de que mantenha um registo público de empresas na área dos criptoativos que não sejam conformes, facilitando, assim, o rastreamento de qualquer violação das leis de combate ao branqueamento de capitais.

Este regulamento abrange criptoativos e prestadores de serviços de criptoativos, exigindo a estes últimos a obtenção de autorização para atuar em território europeu, o que tornará mais fácil às autoridades a supervisão das empresas em matéria de AML.

Os prestadores de serviços de criptoativos, cuja empresa-mãe esteja localizada em países que constam da lista da UE de países terceiros considerados de alto risco para atividades de combate ao branqueamento de capitais, bem como da lista da UE de jurisdições não cooperantes para efeitos

[196] (Ferreira, et al., 2021 pp. 4, 5)
[197] (Ferreira, et al., 2021 p. 5)
[198] (Europol, 2021)

fiscais, serão obrigados a implementar controlos reforçados em conformidade com o quadro da UE em matéria de combate ao branqueamento de capitais.

Subsistem, porém, alguns desafios, como a exclusão do âmbito do regulamento dos serviços que sejam totalmente descentralizados, o que impõe riscos aos utilizadores de criptoativos, aumentando os riscos sistémicos e dificultando a aplicação da regulamentação financeira da UE.

Já no que diz respeito à AMLD5 e ao TFR, qualquer plataforma que não corresponda à definição de CASP's encontra-se de fora do âmbito destes normativos. Para além das carteiras sem custódia, por exemplo, um serviço de mistura (um *mixer*) não é considerado um CASP quando consiga asseverar que é totalmente descentralizado, o que será o caso quando prosseguir transações P2P.

Como vimos, através da utilização de serviços mistura de criptoativos na ocultação dos criptoativos (utilizando qualquer uma das técnicas analisadas no ponto 2.7 da Parte I), torna-se impossível rastrear a cadeia de transações, uma vez que, após a mistura, deixam de ser conhecidas as partes de uma transação. Por sua vez, não saberemos para quem os fundos são encaminhados após a utilização do protocolo de mistura e, do ponto de vista do destinatário, não sabemos de onde vêm os fundos, exceto de que são originários de um serviço de mistura.

Futuros regulamentos e diretivas até poderiam classificar quaisquer fundos rastreáveis a serviços de mistura como sendo de alto risco e exigir aos prestadores de serviços de criptoativos o bloqueio da conta de tais utilizadores. No entanto, isso só resolve um problema e cria um novo, uma vez que ao utilizador seria sempre possível "quebrar a ligação" com o serviço de mistura[199] (*vide*, uma vez mais, as técnicas analisadas no ponto 2.7 da Parte I).

Se considerarmos o que realmente torna o setor de criptoativos menos propenso à prática de branqueamento de captais na Europa, não podemos

[199] (Zetzsche, et al., 2023 p. 95)

deixar de destacar o Regulamento da Transferência de Fundos, por meio da adoção da famosa *Travel Rule*, que exige aos prestadores de serviços de criptoativos que compartilhem os detalhes dos clientes no caso de uma transação que envolva criptoativos. O requisito de que as informações da pessoa devam viajar ao longo da transação torna mais difícil aos criminosos a exploração do recurso ao anonimato no comércio de criptoativos para efeitos de branqueamento de capitais.

Como o crescimento da utilização de criptoativos, o TFR revelou-se um passo importante para uma maior transparência e responsabilidade no sistema financeiro em toda a UE.

Embora na indústria dos criptoativos este Regulamento possa ser havido como oneroso, o seu objetivo, em última análise, é a prevenção de atividades ilícitas através da utilização de criptoativos, como sejam o branqueamento de capitais e o financiamento do terrorismo.

Posto isto, a obrigatoriedade de identificação das partes envolvidas em transações de criptoativos é um tema controverso que levanta questões sobre a privacidade e a natureza descentralizada dessas moedas digitais. Embora seja importante combater atividades ilegais, como o branqueamento de capitais, é válido considerar as possíveis consequências de tais medidas para o futuro dos criptoativos e para a própria ideia que impulsionou o surgimento dessa tecnologia.

Como é já por demais evidente, a característica mais aliciante dos criptoativos para prática criminal é a sua capacidade de realizar transações de forma anónima, permitindo aos indivíduos a preservação da sua privacidade e e a proteção das suas informações pessoais.

Mas o fator anonimidade não é atrativo apenas para pessoas com intuito criminoso. Esta característica tem o potencial por muitos valorizado de permitir confidencialidade e sigilo nas transações financeiras, sobretudo num mundo cada vez mais digital onde os dados pessoais estão sujeitos a violações de segurança.

Assim, a imposição da identificação das partes envolvidas em transações de criptoativos pode desencadear uma série de efeitos negativos. Primeiramente, tal obrigatoriedade pode afastar os indivíduos que procuram utilizar criptoativos como uma forma de preservar a sua privacidade e fugir à vigilância excessiva de instituições financeiras ou governamentais. Tal pode gerar uma perda de confiança e de interesse nos criptoativos, tornando-os menos atraentes para muitos usuários.

Além disso, a exigência de identificação também pode criar barreiras significativas para a adoção generalizada dos criptoativos. Nem todos os utilizadores estão dispostos ou se sentem confortáveis em compartilhar as suas informações pessoais num ambiente digital, mesmo que isso seja necessário para o estrito cumprimento de regulamentações e leis.

Destarte, é importante reconhecer que o avanço tecnológico e a inovação estão intrinsecamente ligados à liberdade de explorar novas possibilidades e abordagens. Impor excessivas restrições à identificação das partes em transações com criptoativos pode limitar esse avanço, inibindo a criatividade e a experimentação, elementos-chave no impulsionamento da evolução tecnológica.

Embora certos países tenham implementado regulamentações que preveem o fenómeno dos criptoativos, a velocidade do avanço tecnológico muitas vezes supera a capacidade dos órgãos reguladores de adaptar-se e controlar todas as nuances deste ambiente.

Além disso, existem jurisdições com regulamentações mais flexíveis (ou mesmo sem regulamentações), o que possibilita que indivíduos e organizações mal-intencionados busquem refúgio nesses locais de forma a realizar a suas transações criminosas sem enfrentar as mesmas restrições que encontrariam em países mais rigorosos.

Tecnologias emergentes, como a análise de dados, a inteligência artificial e o *machine learning*, comportam o potencial de serem aplicadas de forma a melhorar a deteção de atividades suspeitas e identificar padrões que possam indiciar práticas ilegais, como o branqueamento de capitais. A colaboração entre

países e instituições financeiras também é fundamental para combater o branqueamento de capitais no contexto dos criptoativos.

No entanto, é preciso reconhecer que a evolução tecnológica é constante e, consequentemente, novas brechas e desafios podem surgir. A velocidade com que essas mudanças ocorrem muitas vezes supera a capacidade das regulamentações e controlos existentes. Para tanto, é essencial que haja uma constante atualização das regulamentações e o aprimoramento dos mecanismos de fiscalização para acompanhar esse cenário em constante evolução. Apenas por meio de um esforço contínuo e colaborativo será possível minimizar os riscos e assegurar a integridade do sistema financeiro no contexto dos criptoativos.

Assim, é crucial encontrar um equilíbrio entre a privacidade e a necessidade de combater atividades ilícitas. As regulamentações podem ser aprimoradas para buscar soluções mais equilibradas, como a implementação de mecanismos de verificação de identidade que protejam a privacidade dos usuários, ao mesmo tempo que permitam a deteção de transações suspeitas.

Uma abordagem mais aberta e colaborativa, envolvendo governos, instituições financeiras e especialistas em tecnologia e em criptoativos pode ajudar a encontrar soluções que preservem os princípios fundamentais dos criptoativos, como a descentralização e a privacidade, sem comprometer a segurança e a integridade do sistema financeiro.

Em última análise, é essencial reconhecer que a evolução dos criptoativos e a regulamentação adequada são desafios complexos e multifacetados. A busca por um equilíbrio entre a privacidade e a segurança é um processo contínuo, que exige reflexão, diálogo e adaptação constante para garantir que as inovações tecnológicas possam prosperar, mantendo-se alinhadas aos princípios e valores que impulsionaram o surgimento dos criptoativos.

Conclusão

À medida que nos encontramos imersos na era digital, é cada vez mais difícil acompanhar e prever todas as situações decorrentes desses avanços. Um exemplo concreto desse cenário é a utilização dos criptoativos no branqueamento de capitais, mesmo diante das novas legislações.

É inegável o potencial positivo das novas tecnologias e dos instrumentos monetários na modernização do panorama financeiro. No entanto, os setores não regulamentados e os intervenientes que operam no espaço virtual, relativamente aos quais pouco se conhece o *modus operandi* e o impacto nas atividades AML, utilizam meios eficazes de ocultação da identidade das pessoas envolvidas nas transações financeiras. Para fazer face a esta nova realidade, os países devem compreender estes fatores e o seu impacto nos futuros fluxos financeiros.

A questão sobre se a legislação atual é suficiente para impedir a prática de branqueamento de capitais utilizando criptoativos é objeto de debate e contínua avaliação. Embora tenham sido adotadas medidas regulatórias significativas em várias jurisdições, existem desafios específicos relacionados aos criptoativos que dificultam sua regulação eficaz.

Os criptoativos surgiram como uma alternativa descentralizada e anónima para a realização de transações financeiras. Essa característica, que inicialmente era vista como uma vantagem, também se demonstrou como sendo uma brecha para a prática de atividades ilegais, como o branqueamento de capitais, sobretudo devido à característica do anonimato, que tem permitido que indivíduos e organizações desonestas sejam bem-sucedidos nas ocultação da origem ilícita dos seus recursos.

Como vimos, a EU tem trabalhado ativamente para fortalecer as suas leis e regulamentos no sentido de combater o branqueamento de capitais relacionado aos criptoativos. Em particular, o TFR, o mais relevante diploma na matéria, exige às empresas que prestam serviços de criptoativos a

implementação de medidas de conformidade, como a identificação dos clientes, monitorização de transações e relatórios de atividades suspeitas.

Depois, as exigências de KYC dos remetentes e destinatários dos criptoativos pode levantar problemas, uma vez que nem toda a gente procura o fator anonimidade deste tipo de ativos para contornar a lei, mas apenas por motivo de privacidade em relação à partilha das suas informações pessoais em ambiente digital.

Portanto, embora a legislação atual tenha feito avanços significativos na prevenção e repressão ao branqueamento de capitais utilizando criptoativos, é uma questão em constante evolução e que requer esforços contínuos para adaptar e fortalecer as medidas regulatórias à medida que surgem novos desafios. A colaboração internacional, a supervisão efetiva e a educação são componentes cruciais para enfrentar essa questão complexa e em constante mutação.

Embora as alterações à legislação AML tenham sido substanciais nas últimas décadas, a mudança do panorama global e a inovação tecnológica significam que os reguladores e as instituições financeiras devem ser proactivos em relação às ameaças criminosas e terroristas de branqueamento de capitais.

Para que essa resposta seja eficaz, será vital uma parceria contínua e inovadora entre legisladores, instituições financeiras e tecnologias emergentes, que, em conjunto, podem chegar a soluções inovadoras na deteção de atividades suspeitas e identificação de padrões que possam indiciar práticas de branqueamento de capitais.

Referências Bibliográficas

Alcarva, Paulo. 2018. *Banca 4.0 - Revolução Digital: Fintechs, Blockchain, Criptomoedas, Robo-advisers e Crowdfunding.* s.l. : Conjuntura Actual Editora, 2018. 978-989-694-301-1.

—. 2021. *Bitcoin e Blockchain - Guia prático para perceber, gerar e investir em criptomoedas.* s.l. : Conjuntura Actual Editora, 2021. 978-989-69-4300-4.

Anderson, David L. e Ault, Kirstin M. 2019. *United States of America v. BTC-e, a/k/a Canton Business Corp., and Alexander Vinnik.* 4:19-cv-04281-KAW, s.l. : United States District Court, Northern District of California, San Francisco Division, 2019.

Anti-Money Laundering Program Effectiveness. **(FinCen), Financial Crimes Enforcement Network. 2020.** 181, 17 de september de 2020, Federal Register - The Daily Journal of the United States Government, Vol. 85, pp. 58023-58029.

Banco de Portugal. 2020. Criptoativos, stablecoins e euro digital? Descubra as diferenças. *Banco de Portuga Eurosistema.* [Online] 2020. [Citação: 2022 de abril de 20.] https://www.bportugal.pt/page/criptoativos-stablecoins-e-euro-digital-descubra-diferencas-1.

—. Criptoativos, stablecoins e euro digital? Descubra as diferenças. [Online] https://www.bportugal.pt/page/criptoativos-stablecoins-e-euro-digital-descubra-diferencas-1.

Banco de Portugal working group on crypto-assets. 2020. *Occasional Paper on Crypto-Assets.* Lisboa : s.n., 2020. 978-989-678-757-8.

BankInfoSecurity. 2020. *$90 Million Seized in Fraud Case Tied to BTC-e Exchange.* 23 de june de 2020.

BBC News. 2016. *Liberty Reserve digital cash chief jailed for 20 years.* 09 de may de 2016.

Binance. 2021. Intro to Peer-to-Peer Trading: What is P2P Trading and How Does a Local Bitcoin Exchange Work? [Online] 25 de março de 2021. [Citação: 2023 de junho de 19.] https://www.binance.com/en/blog/p2p/intro-to-peertopeer-trading-what-is-p2p-trading-and-how-does-a-local-bitcoin-exchange-work-421499824684901839.

Braguês, José Luís. 2009. *O Processo de Branqueamento de Capitais.* Observatório de Economia e Gestão de Fraude. s.l. : Edições Húmus, 2009. Working Papers Nº 2/2009. 978-989-8139-09-2.

Bullmann, Dirk, Klemm, Jonas e Pinna, Andrea. 2019. *European Central Bank Occasional Paper Series No. 230- In search for stability in crypto assets: are stablecoins de solution?* Frankfurt : s.n., 2019. 978-92-899-3871-6.

Cheniaux, Rafael. 2021. A incriminação do branqueamento em Portugal à luz do direito comunitário - A questão das vantagens licitamente adquiridas no estrangeiro. *ULP Law Review | Revista de Direito da ULP.* 2021, Vol. 15, 1.

Comissão Europeia. 2018. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Banco Central Europeu, ao Comité Económico e Social Europeu e ao Comité das Regiões.* Bruxelas : s.n., 2018.

Commissioner Hester M. Peirce. 2019. How we Howey. *U. S. Securities and Exchange Commission.* [Online] 9 de may de 2019. [Citação: 29 de junho de 2023.] https://www.sec.gov/news/speech/peirce-how-we-howey-050919.

Conselho Europeu (CE); Conselho da União Europeia (CUE). 2022. Combate ao branqueamento de capitais: Conselho define a sua posição sobre um conjunto reforçado de regras. [Online] 7 de dezembro de 2022. [Citação: 2 de abril de 2023.] https://www.consilium.europa.eu/pt/press/press-releases/2022/12/07/anti-money-laundering-council-agrees-its-position-on-a-strengthened-rulebook/.

Consulta de Tratados Internacionais - Convenção Relativa ao Branqueamento, Detecção, Apreensão e Perda dos Produtos do Crime. *Ministério Público Portugal.* [Online] [Citação: 30 de abril de 2023.]

https://www.ministeriopublico.pt/instrumento/convencao-relativa-ao-branqueamento-deteccao-apreensao-e-perda-dos-produtos-do-crime-5.

Council of the European Union and the European Council. 2023. Digital Finance. [Online] 6 de june de 2023. [Citação: 15 de june de 2023.] https://www.consilium.europa.eu/en/policies/digital-finance/?utm_source=linkedin.com&utm_medium=social&utm_campaign=20230516-crypto&utm_content=visual-carousel.

CreditDonkey. 2022. Crypto Friendly Banks. [Online] 5 de april de 2022. [Citação: 23 de june de 2023.] https://www.creditdonkey.com/crypto-friendly-banks.html.

Crypto Tokens and Token Systems. **Schwiderowski, Jan, Pedersen, Asger Balle e Beck, Roman. 2023.** 17 de march de 2023, Information Systems Frontiers.

crypto.bi. What is Turing completeness and how does it relate to cryptocurrencies? [Online] https://crypto.bi/turing/.

Cryptocurrencies and fiat money: The end of a public good? **Kourmpetis, Stavros e Gazis, Alexandros. 2022.** Sakhir, Bahrain : IEEE, 2022. 978-1-6654-9060-3.

Cryptocurrencies and future financial crime. **Trozze, Arianna, et al. 2022.** 1, Crime Science : s.n., 05 de Janeiro de 2022, Vol. 11.

Cuervo, Cristina, Morozova, Anastasiia e Sugimoto, Nobuyasu. 2020. *Regulation of Cryptoassets.* 2020. 9781513520315.

Darknetlive. 2019. *Alphabay Vendor "DailyFix" Ordered to Forfeit 64 Bitcoins.* 10 de dezembro de 2019.

Debus, Julian. 2017. *Consensus Methods in Blockchain Systems.* Frankfurt School Blockchain Center. 2017.

Diário de Notícias. 2019. *Darknet, bitcoins, haxixe e canábis. Pedro e Rita fizeram tráfico real com moedas virtuais.* 10 de dezembro de 2019.

Ethereum. 2023. Ethereum Whitepaper. [Online] 30 de june de 2023. [Citação: 30 de june de 2023.] https://ethereum.org/en/whitepaper/.

EUR-Lex. Branqueamento de capitais. [Online] [Citação: 21 de 03 de 2023.] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Amoney_laundering&lang1=PT&from=EN&lang3=choose&lang2=choose&_csrf=84f7b596-dd7b-43fd-99b8-a1e22e9248d1.

European Banking Authority (EBA). 2019. EBA reports on crypto-assets. *European Banking Authority.* [Online] 9 de Janeiro de 2019. [Citação: 11 de dezembro de 2022.] https://www.eba.europa.eu/eba-reports-on-crypto-assets.

European Central Bank. 2019. *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures.* ECB Crypto-Assets Task Force. Frankfurt : s.n., 2019. p. 40, Occasional Pappers. 1725-6534.

European Commission. 2020. Digital finance package. [Online] 24 de september de 2020. [Citação: 3 de may de 2023.] https://finance.ec.europa.eu/publications/digital-finance-package_en.

European Council; Council of the European Union. 2022. New EU Authority for Anti-money laundering: Council agrees its partial position. [Online] 29 de june de 2022. [Citação: 20 de junho de 2023.] https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/new-eu-authority-for-anti-money-laundering-council-agrees-its-partial-position/.

European Parliament. 2020. *Key Developments, regulatory concerns and responses.* Policy Department for Economic, Scientific and Quality of Life Policies. 2020. 978-92-846-6502-0.

European Union (EU). 2020. *The EU's anti-money laundering policy in the banking sector.* s.l. : Curia Rationium, 2020.

Europol. 2020. *20 arrests in QQAAZZ multi-million money laundering case.* 15 de outubro de 2020.

—. 2021. *Cryptocurrencies: tracing the evolution of criminal finances.* Luxembourg : Publicatioons Office of the European Union, 2021. 978-92-95220-37-9.

—. 2021. *Europol Spotlight - Cryptocurrencies: Tracing the Evolution of Criminal Finances.* Luxemburgo : Publications Office of the European Union, 2021. 978-92-95220-37-9.

Exploring the links between AML, digital currencies and blockchain technology. **Naheem, Mohammed Ahmad. 2019.** 3, 2019, Journal of Money Laundering Control, Vol. 22, pp. 515 - 526.

Ferreira, Agata e Sandner, Philipp. 2021. Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. *Computer Law & Security Review.* novembro de 2021, Vol. 42.

Financial Action Task Force (FAFT). 2013 - 2021. *Methodology for assessing technical compliance with the FAFT Recommendations and the effectiveness of AML/CFT Systems.* Paris : s.n., 2013 - 2021.

—. 2020. *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets.* Paris : s.n., 2020.

—. 2014. Virtual Currencies - Key definitions and potencial AML/CFT risks. [Online] 2014. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

Financial Action Task Force (FATF). 2019. *Guidance for a risk-based approach - Virtual Assets and Virtual Asset Service Providers.* Paris : s.n., 2019.

—. 2018. *Professional Money Laundering.* Paris : s.n., 2018.

Financial Action Task Force. 2019. *Guidance for a Risk-Based Approach - Virtual Assets and Virtual Asset Service Providers.* 2019.

—. 2018. Professional Money Laundering. [Online] 26 de july de 2018. [Citação: 12 de april de 2023.] https://www.fatf-

gafi.org/en/publications/methodsandtrends/documents/professional-money-laundering.html.

Financial Conduct Authority. 2019. *Guidance on Cryptoassets.* 2019.

Financial Crime Academy. Cryptocurrency Money Laundering Methods: The Key To Cryptocurrency Crime. [Online] [Citação: 12 de may de 2023.] https://financialcrimeacademy.org/cryptocurrency-money-laundering-methods/.

Financial Crimes Enforcement Network (FinCen). 2019. *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies.* FinCen. 2019. FinCen Guidance. FIN-2019-G001.

—. History of Anti-Money Laundering Laws. [Online] [Citação: 21 de april de 2023.] https://www.fincen.gov/history-anti-money-laundering-laws.

—. Mission. [Online] https://www.fincen.gov/about/mission.

—. USA PATRIOT Act. [Online] [Citação: 19 de junho de 2023.] https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act.

Finantial Action Task Force (FATF). 2022. *Targeted Update On Implementation Of The Fatf Standards On Virtual Assets And Virtual Asset Service Providers.* Paris : s.n., 2022.

Garcia, Pedro Carreira. 2022. Expresso. [Online] 9 de dezembro de 2022. https://expresso.pt/economia/2022-12-09-Negocios-com-criptomoedas-movimentam-30-mil-milhoes-em-Portugal-48736bac.

Gillibrand, Kirsten. 2023. Lummis, Gillibrand Reintroduce Comprehensive Legislation To Create Regulatory Framework For Crypto Assets. *Press Release.* [Online] 12 de july de 2023. https://www.gillibrand.senate.gov/news/press/release/lummis-gillibrand-reintroduce-comprehensive-legislation-to-create-regulatory-framework-for-crypto-assets/.

Goriacheva A., Jakubenko N., Pogodina O., Silnov D. 2018. *Anonymization Technologies of Cryptocurrency Transactions as Money Laundering Instrument.* 2018. pp. 46 - 53.

Haffke, Lars, Fromberger, Mathias e Zimmermann, Patrick. 2020. Virtual Currencies and Anti-Money Laundering - The shortcomings of the 5th AML Directive (EU) and how to adress them. *Journal of Banking Regulation.* 2020, Vol. 21, 2.

Haig, Samuel. 2019. BTC-e's Vinnik Case Drags on as New Accusations Continue Emerging. *Coin Telegraph.* [Online] 2019. [Citação: 17 de 05 de 2023.] https://cointelegraph.com/news/btc-es-vinnik-case-drags-on-as-new-accusations-continue-emerging.

Haynes, Andrew e Yeoh, Peter. 2020. *Regulatory and Legal Issues.* Informa Law from Routledge : s.n., 2020. 978-0-367-48636-5.

Houben, Robby e Snyers, Alexander. 2020. *Crypto-assets - Key developments, regulatory concerns and responses.* European Parliament : Policy Department for Economic, Scientific and Quality of Life Policies, 2020. 978-92-846-6502-0.

—. 2018. *Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion.* Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament. 2018. 978-92-846-3200-8.

Hudson Inteligence, LLC. Mixers and Coinjoin. *Cryptocurrency.* [Online] [Citação: 02 de july de 2023.] https://www.fraudinvestigation.net/cryptocurrency/tracing/mixers-and-coinjoin.

Jake Frankenfield. 2022. Criptographic Hash Funtions: Definitions and Examples. *Investopedia.* [Online] maio de 2022. https://www.investopedia.com/news/cryptographic-hash-functions/.

Jersey Financial Services Commission. 2022. Money Laundering. [Online] 27 de july de 2022. [Citação: 27 de february de 2023.] https://www.jerseyfsc.org/industry/guidance-and-policy/money-laundering/.

Jornal de Negócios. 2023. Uma ponte perfeita entre ativos digitais e tradicionais. [Online] 21 de junho de 2023. [Citação: 23 de junho de 2023.] https://www.jornaldenegocios.pt/negocios-em-rede/detalhe/uma-ponte-perfeita-entre-ativos-digitais-e-tradicionais.

Lepore, Cristian, et al. 2020. A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. *Mathematics.* 2020, Vol. 8, 1782.

Malaquias, Pedro Ferreira. 2021. *Criptoativos - Uma realidade de hoje.* Uría Menéndez – Proença de Carvalho. 2021.

Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures. **Wronka, Christoph. 2021.** 2021, Journal of Money Laundering Control, pp. 79 - 93. 1368-5201.

Mulig, Elizabeth Vallery e Smith, L. Murphy. 2008. *Understanding and Preventing Money Laundering.* 2008.

Nakamoto, Satoshi. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. [Online] 2008. https://bitcoin.org/bitcoin.pdf.

Ordóñez, Miguel. 2018. El futuro de la banca: dinero seguro y desregulación del sistema financiero. *Revista Procesos de Mercado.* 2018, pp. 321-336.

Polícia Judiciária. 2017. *Operação BIT.* 5 de julho de 2017.

Ramalho, David Silva e Matos, Nuno Igreja. 2020. Branqueamento e Bitcoin: uma introdução. *Revista do Ministério Público.* abr.-jun. de 2020, 162, pp. 77-115.

Rodrigues, Anabela Miranda. 2017. O Crime de Branqueamento de Capitais à Luz do Direito Penal Internacional e da União Europeia - Bem Jurídico e

Configuração Típica em Portugal, no Brasil e em Macau. *Revista Brasileira de Estudos Jurídicos.* jul - dez de 2017, Vol. 12, 2.

Rosen, Liana W. e Miller, Rena S. 2022. *The Financial Crimes Enforcement Network (FinCEN): Anti-Money Laundering Act of 2020 Implementation and Beyond.* Congressional Research Service, United States Congress (USC). s.l. : R47255, 2022.

Sanction Scanner. 2019. *Liberty Reserve Money Laundering Scandal.* 2019.

Santos, João Vieira dos. 2021. *Regulação dos Criptoativos (Regulation of Crypto-assets).* 2021.

2022. The United States Department of Justice (DOJ). [Online] 5 de agosto de 2022. [Citação: 22 de janeiro de 2023.] https://www.justice.gov/opa/pr/alleged-russian-cryptocurrency-money-launderer-extradited-united-states.

The White House. 2022. FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets. *Statements and Releases.* [Online] 09 de march de 2022. [Citação: 2 de may de 2023.] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/.

União Europeia (UE). 2021. Prevenir a utilização abusiva do sistema financeiro para efeitos de branqueamento de capitais e terrorismo. *EUR-Lex.* [Online] 27 de 10 de 2021. [Citação: 02 de 04 de 2023.] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:230804_1.

United States Attorney's Office, Northern District of Californa. 2017. [Online] 26 de Julho de 2017. [Citação: 25 de 10 de 2022.] https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.

United States Congress (USC). H.R.5077 - Money Laundering Control Act of 1986. *Congress.gov.* [Online] [Citação: 12 de 05 de 2023.] https://www.congress.gov/bill/99th-congress/house-bill/5077.

United States Department of State (USDS). 2001. Money Laundering and Financial Crimes. [Online] 1 de March de 2001. [Citação: 10 de may de 2023.] https://2009-2017.state.gov/j/inl/rls/nrcrpt/2000/959.htm.

United States Government (USG). Financial Crimes Enforcement Network. *What we do.* [Online] [Citação: 13 de 05 de 2023.] https://www.fincen.gov/what-we-do.

—. The Bank Secrecy Act. *Financial Crimes Enforcement Network.* [Online] [Citação: 02 de 05 de 2023.] https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act.

Vasconcelos, Miguel Pestana de. 2021. *Direito Bancário - 3.ª ed.* s.l. : Edições Almedina, 2021. 978-972-40-9763-3.

Viegas, Miguel e Sarmento, Carlos. 2022. *O Branqueamento de Capitais e o Financiamento do Terrorismo.* s.l. : Grupo Editorial Vida Económica, 2022. 9789897689772.

Warren, Elizabeth e Marshall, Roger. 2022. *The Digital Asset Anti-Money Laundering Act of 2022.* US Senate. 2022.

Zetzsche, Dirk A., et al. 2023. *Remaining regulatory challenges in digital finance and cryptoassets after MiCA.* Policy Department for Economic, Scientific and Quality of Life Policies . s.l. : European Parliament, 2023. 978-92-848-0564-8.