ACADEMIA MILITAR

Investigação Económico-Financeira — Implicações do Recurso a Ativos Virtuais

Autor: Aspirante de GNR Infantaria Paulo Alcobia Carvalho

Orientador: Professor Catedrático Doutor José Fontes

Coorientador: Capitão GNR Infantaria Gabriel Oliveira

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Dissertação de Mestrado

Lisboa, maio de 2023

ACADEMIA MILITAR

Investigação Económico-Financeira — Implicações do Recurso a Ativos Virtuais

Autor: Aspirante de GNR Infantaria Paulo Alcobia Carvalho

Orientador: Professor Catedrático Doutor José Fontes

Coorientador: Capitão GNR Infantaria Gabriel Oliveira

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Dissertação de Mestrado

Lisboa, maio de 2023

EPÍGRAFE

“Se não acredita ou não entende, não tenho tempo para o convencer, desculpe.”
(Satoshi Nakamoto, 2008)

DEDICATÓRIA

À minha família, LORD e XXVIII CFO da GNR.

Sem o vosso apoio nada seria concretizável.

AGRADECIMENTOS

Tendo em conta o cariz individual deste Trabalho de Investigação Aplicada, não seria justo assumir todos os louros da realização desta investigação sem salientar a presença e o apoio de algumas pessoas, absolutamente, fundamentais na conclusão desta análise investigatória.

Com um papel de destaque no que toca ao apoio e à disponibilidade demonstrada ao longo da realização do meu Trabalho de Investigação Aplicada, tenho a agradecer ao meu Orientador o Exmo. Professor Catedrático José Fontes, sem a sua ajuda não teria sido possível a concretização deste estudo.

Ao meu Coorientador Exmo. Capitão Gabriel Oliveira, sem a sua presença e dedicação, a realização deste trabalho não seria, de todo, possível, o meu mais sincero obrigado.

Gostaria de expressar a minha profunda gratidão aos Exmos. entrevistados no âmbito deste trabalho sendo os mesmos o Tenente Coronel Diogo Dores, Diretor de Investigação Criminal do Comando Operacional da GNR, o Capitão Hélder Fernandes, chefe da SIC da UAF da GNR, o Dr. Pedro Verdelho, Diretor do Gabinete Cibercrime da Procuradoria-Geral da República, o Dr. Carlos Casimiro, Procurador da República, coordenador da SIATID – DCIAP, o Dr. José Braguês, Chefe da Secção de Informação da UIF, o Dr. Afonso Sales, Coordenador da PJ – UNCC, o Dr. Fernando Ramos, responsável pela Secção de Investigação da Criminalidade Informática contra o Património e Vida em Sociedade e o Dr. Pedro Felício, *Head of Unit - European Financial and Economic Crime Centre (EFECC)* obrigado pela disponibilidade e celeridade com que responderam às entrevistas para o meu Trabalho de Investigação Aplicada. O vosso contributo foi de valor inestimável e permitiu-me obter perspetivas valiosas sobre o tema em questão. Agradeço a todos por terem dedicado o seu tempo e partilhado o seu conhecimento, o que me permitiu enriquecer o meu trabalho.

Uma homenagem especial aos homens e mulheres que me acompanharam ao longo destes cinco anos de formação e de muitas memórias, o XXVIII CFO da Guarda Nacional Republicana que me tornaram na pessoa que sou hoje.

A todos os intervenientes, mais uma vez, o meu mais sincero agradecimento pela ajuda e colaboração.

RESUMO

Este Trabalho de Investigação Aplicada aborda as implicações do recurso a ativos virtuais na investigação económico-financeira, analisando a sua origem e história, bem como a sua regulamentação. É apresentada uma visão geral dos *atores* envolvidos no combate à criminalidade económico-financeira, destacando-se a Guarda Nacional Republicana - Unidade de Ação Fiscal, a Polícia Judiciária - Unidade Nacional de Combate à Corrupção e Unidade Nacional Combate ao Cibercrime e à Criminalidade Tecnológico, a Autoridade Tributária e as entidades europeias, como o Grupo de Ação Financeira Internacional e a *Financial Action Task Force*.

São discutidos os crimes com recurso a ativos virtuais, como o branqueamento de capitais e os crimes conexos, bem como as formas necessárias e possíveis de apreensão desses ativos. É também analisada a regulamentação dos ativos virtuais, como a *Markets in Crypto Assets Regulation* (MiCAR), e as vantagens e desvantagens do seu uso.

Outro resultado importante deste estudo é a constatação de que os crimes relacionados com ativos virtuais não se limitam à lavagem de dinheiro, mas incluem também outros crimes, como extorsão, roubo e fraude, entre outros. O estudo destaca, também, que as investigação e combate aos crimes relacionados com ativos virtuais exige a colaboração entre diferentes *atores*, incluindo a polícia, o setor privado e organizações internacionais.

Conclui-se que o recurso a ativos virtuais pode trazer benefícios, mas também desafios significativos para a investigação económico-financeira. É necessária uma maior colaboração entre os *atores* envolvidos e a atualização da regulamentação existente para garantir uma investigação eficaz e a prevenção da consumação de ilícitos criminais com recurso a esses ativos. A apreensão dos ativos virtuais é também um desafio, sendo necessário encontrar formas de superar essas dificuldades, como a formação dos investigadores e a cooperação internacional.

Em suma, este estudo destaca que o recurso a ativos virtuais representa um desafio para a investigação económico-financeira, mas que a colaboração entre diferentes instituições e a regulamentação adequada podem contribuir para reduzir o uso destes ativos em atividades criminosas e facilitar a investigação e combate aos crimes económico-financeiros.

Palavras-chave: Ativos Virtuais; Investigação Financeira; Criptomoedas; *Blockchain*; Apreensão de Ativos.

ABSTRACT

This article addresses the implications of the use of virtual assets in economic and financial investigations, analyzing their origin and history, as well as their regulation. An overview is presented of the actors involved in fighting economic and financial crime, highlighting the Portuguese National Guard - Fiscal Action Unit, the Judicial Police - National Unit for Combating Corruption and National Unit for Combating Cybercrime and Technological Crime, the Tax Authority, and European actors such as the International Financial Action Task Force and the Financial Action Task Force.

Crimes involving virtual assets, such as money laundering and associated crimes, as well as the necessary and possible means of seizing such assets, are discussed. The regulation of virtual assets, such as the Markets in Crypto Assets Regulation (MiCAR), is also analyzed, as are the advantages and disadvantages of its use.

Another important result of this study is the finding that crimes associateds to virtual assets are not limited to money laundering, but also include other crimes such as extortion, theft, fraud among others. The study also highlights that investigating and fighting crimes related to virtual assets requires collaboration between different actors, including the police, the private sector and international organizations.

It is concluded that the use of virtual assets can bring benefits but also significant challenges to economic and financial investigations. Greater collaboration between the actors involved and the updating of existing regulations is necessary to ensure effective investigation and prevention of the commission of criminal offenses involving these assets. Seizing virtual assets is also a challenge, and it is necessary to find ways to overcome these difficulties, such as training investigators and international cooperation.

In summary, this study highlights that the use of virtual assets represents a challenge for economic and financial investigation, but that collaboration between different actors and appropriate regulation can contribute to reducing the use of these assets in criminal activities and aid investigation as well as fighting economic and financial crimes.

Keywords: Virtual Assets; Financial Investigation; Cryptocurrencies; Blockchain; Asset Seizure.

ÍNDICE GERAL

ÍNDICE DE QUADROS

LISTA DE APÊNDICES

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AJ	Autoridade Judicial
APA	*American Psychological Association*
AT	Autoridade Tributária
AV	Ativos Virtuais
BC-FT	Branqueamento de Capitais e Financiamento de Terrorismo
B2B	*Business-to-business*
CeFi	Sistemas Financeiros Centralizados
Cfr.	Conforme
CGD	Caixa Geral de Depósitos
CP	Código Penal
DCIAP	Departamento Central de Investigação e Ação Penal
DCICCEF	Direção Central de Investigação da Corrupção e Criminalidade Económico-Financeira
DeFi	Sistemas Financeiros Descentralizados
DGAIEC	Direção Geral das Alfândegas e dos Impostos Especiais sobre o Consumo
DGCI	Direção Geral dos Impostos
DGITA	Direção Geral de Informática e Apoio aos Serviços Tributários e Aduaneiros
DL	Decreto-Lei
DSAFA	Direção de Serviços Antifraude Aduaneira
DSIFAE	Direção de Serviços de Investigação da Fraude e de Ações Especiais
EFECC	*European Financial and Economic Crime Center*
FATF	*Finantial Action Task Force*
GAB	Gabinete de Administração de Bens
GAFI	Grupo de Ação Financeira Internacional
GNR	Guarda Nacional Republicana
GRA	Gabinete de Recuperação de Ativos
LOIC	Lei de Organização da Investigação Criminal
MiCAR	*Markets in Crypt Assets Regulation*

MP	Ministério Público
NFT	*Non Fungible-token*
OPC	Órgãos de Polícia Criminal
PGR	Procuradoria Geral da República
PJ	Polícia Judiciária
PREMAC	Plano de Redução e Melhoria da Administração Central
P2P	*Peer-to-peer*
QC	Questão Central
QD	Questões Derivadas
RGIT	Regime Geral das Infrações Tributárias
TIA	Trabalho de Investigação Aplicada
UAF	Unidade de Ação Fiscal
UE	União Europeia
UIF	Unidade de Informação Financeira
UNCC	Unidade Nacional de Combate à Corrupção
UNC3T	Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica
VASP	*Virtual Assets Service Providers*

INTRODUÇÃO

A Guarda Nacional Republicana (GNR), como força de segurança e órgão de polícia criminal (OPC), tem como principal função a maximização do sentimento de segurança por parte da população, que por sua vez se obtém, entre outros métodos, através do policiamento com o intuito da prevenção criminal (Mota, 2021).

Admitindo que a prevenção dos comportamentos criminosos é considerada, cada vez mais, uma atividade basilar para o bem-estar da sociedade, o fenómeno dos ativos virtuais (AV) é uma novidade no âmbito da ação fiscal por parte da GNR que leva à necessidade da criação de procedimentos e métodos de combate aos crimes tributários cometidos através desta inovação tecnológica no panorama económico nacional.

A tecnologia utilizada neste tipo de transações acaba por se tornar o foco principal deste estudo. Os AV utilizam, maioritariamente, uma tecnologia denominada de *blockchain* que veio descentralizar as transações financeiras mantendo a celeridade e privacidade das mesmas.

Helbig (2022) refere que, esta tecnologia "elimina" a forma como o paradigma dos bancos é visto e ainda a sua importância e necessidade como terceiro membro de uma transação. Surge então o problema da fuga ao fisco e dos incumprimentos legais ao nível da tributação.

A *blockchain* permite a descentralização das transações de AV através da rede *peer-to-peer* (P2P). Esta rede é composta por todos os possuidores do AV e funciona apenas entre pessoas, ou seja, para funcionar basta existirem um "vendedor e um comprador". As transações efetuadas são lançadas para a *blockchain* criando assim um documento texto denominado de *hash* que vai tornar válida a transferência assim que mais de metade dos detentores desta criptomoeda confirme a transação. Este consenso é demasiado importante para o bom funcionamento destes sistemas e para que estes se mantenham seguros e confiáveis. "Mecanismos de criptografia são empregues de forma a garantir a autoridade, autenticidade, não-repúdio, integridade das transações, bem como os requisitos de segurança de todo o sistema" (Sampaio et al., 2018).

Segundo Europol (2021), o uso dos AV como parte de esquemas criminais tem vindo a aumentar, apesar de que o número de transações feitas na consumação de ilícitos criminais serem bastante baixos em comparação com as outras transações efetuadas.

Nos últimos anos têm existido e aumentado o número de processos onde se verificam o uso de AV como parte de atividades criminais e branqueamento de capitais. Os casos que

envolvem financiamento a forças terroristas através destes AV têm se mantido baixos embora que os crimes cometidos através do recurso de forma errada a este tipo de ativos tenham deixado de estar apenas relacionados com o cibercrime e passado a estar relacionados com todos os tipos de crimes que envolvam transações financeiras pois, utilizando este meio de transação, o rastreio da transferência torna-se mais complicado (V. Costa, 2022).

É difícil perceber a escala e a quantidade dos ilícitos criminais que utilizam os AV devido à enorme dificuldade de aceder ao rastreio das transações. Tendo em conta os AV estudados os ilícitos mais predominantes são a fraude e o branqueamento de capitais.

Nem tudo neste "mundo virtual" é errado ou de mau fundamento, e os normativos de uso destes ativos estão cada vez mais efetivos e melhorados de forma a que no ambiente das criptomoedas sejam requeridos serviços e plataformas de forma a armazenar mais informações sobre os usuários e as transações efetuadas nas contas das corretoras financeiras tendo um consequente impacto positivo na atuação das Forças e Serviços de Segurança.

Desta forma, torna-se urgente e atual tratar desta problemática que tem tendência a causar problemas na ação fiscal realizada pela GNR num futuro próximo e iminente (Europol, 2021).

PARTE I – ENQUADRAMENTO TEÓRICO

CAPÍTULO 1 – ATIVOS VIRTUAIS: ORIGEM E HISTÓRIA

1.1. Dos Ativos Virtuais

Os AV, de acordo com a Lei n.º 83/2017 de 18 de agosto[1], Medidas de Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo são

> "uma representação digital de valor que não esteja necessariamente ligada a uma moeda legalmente estabelecida e que não possua o estatuto jurídico de moeda fiduciária, mas que é aceite por pessoas singulares ou coletivas como meio de troca ou de investimento e que pode ser transferida, armazenada e comercializada por via eletrónica".

Por ativos, entendemos, que se tratam de um conjunto de bens tangíveis ou intangíveis, com um determinado valor monetário que estão na posse de uma pessoa singular ou coletiva. A palavra virtual remete para o lado deste tipo de ativos que têm de ser tratados de forma digital ou eletrónica (Kafteranis & Turksen, 2022).

Sendo os AV intangíveis, por existirem, apenas, no ambiente digital são criados e armazenados em redes descentralizadas, na maioria das vezes, com recurso a tecnologia *blockchain* e podendo ser, ainda, comprados, negociados, vendidos, e utilizados com diversas finalidades sejam elas investimentos ou simples transações financeiras.

Segundo Brody & Couture (2021) a maioria dos AV é baseada em criptografia e tecnologia *blockchain*, que garante a segurança e a transparência das transações e torna os ativos praticamente impossíveis de serem falsificados ou duplicados.

Os AV surgiram como uma alternativa às moedas e investimentos tradicionais, permitindo que as pessoas possam investir e negociar sem a necessidade de intermediários financeiros e com maior liberdade e autonomia. No entanto, os AV também apresentam riscos, como volatilidade, falta de regulamentação e possibilidade de fraudes, o que requer cuidado e conhecimento antes de investir (Brody & Couture, 2021).

Existem diversos tipos de AV, sendo os mais conhecidos as criptomoedas, os *tokens* e, mais recentemente, os non fungible tokens (NFT). Este tipo de mercados tem vindo a crescer num nível astronómico, com grande inovação na criação de novos produtos e classes de ativos. O mercado dos NFT, apresenta um crescimento fora do comum quando equiparado

[1] Cfr art.º 2º, n.º 1 al. ll) da Lei nº 83/2017 de 18 de agosto, Medidas de Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo.

com a sua perspetiva inicial, tendo já criado adeptos por todo o mundo e de forma regular (Peter, 2021).

Alguns exemplos de AV, na ótica de Brody & Couture (2021) são criptomoedas como *Bitcoin* e *Ethereum*, *tokens* de utilidade e *tokens* de segurança. As criptomoedas são uma forma de dinheiro digital que usa criptografia para garantir transações seguras e para controlar a criação de novas unidades. Os *tokens* de utilidade são emitidos por empresas para dar aos usuários acesso a um produto ou serviço específico, enquanto os *tokens* de segurança representam a propriedade de um ativo, como uma ação ou uma obrigação. Além disso, existem outras formas de AV, como jogos online, artigos digitais colecionáveis e outros tipos de tokens e moedas digitais.

As empresas que tratam da conexão do cliente com os AV são denominadas de *Virtual Assets Service Providers* (VASP) e a principal missão deste tipo de empresas é a persecução e sustentação do crescimento. Desse modo, acabam por procurar estimular o mercado financeiro junto das empresas que trabalham na forma de business-to-business (B2B) para que estas sejam correspondidas com a rapidez e agilidade do sistema utilizado pelos AV (Hardjono et al., 2020).

Na opinião de Riegelnig & Suisse, 2019, embora os AV sejam relativamente novos e ainda estejam a ser desenvolvidos, muitas empresas e indivíduos já os usam como forma de investimento e pagamento. No entanto, a regulação em torno destes, ainda está em desenvolvimento, e muitos governos e agências reguladoras estão a trabalhar de forma a criar um quadro legal para a sua utilização.

1.2. Da *Blockchain*

Nos primórdios da era digital, foram criadas bases de dados para guardar as informações mais valiosas de modo a mantê-las em segurança, por necessidade, das grandes empresas, sendo assim, o acontecimento que desencadeou o aparecimento da *blockchain* (Fassano, 2020).

Após serem identificadas algumas necessidades nestas bases de dados e a aquisição de uma rede que se "autogerisse", em 1998 *Wei Dai* tornou-se o pioneiro na procura e estudo de uma rede descentralizada com o propósito de se gerir através dos seus utilizadores, deixando de ser necessária uma entidade externa à rede para a administrar. Vários autores trabalharam no aperfeiçoamento e estudo desta modalidade até que em 2008 surgiu um

"cidadão(os) desconhecido(s)" com o pseudónimo de Satoshi Nakamoto que veio com uma ideia inovadora, a *Bitcoin* (Evans, 2012).

Esta moeda virtual, atualmente a mais valiosa e famosa do mundo, utiliza a tecnologia *blockchain* de forma a registar nas cadeias de blocos todas as alterações, movimentos e transações na rede P2P. O protocolo *Bitcoin* entrou em vigor no dia 3 de janeiro de 2009 e veio revolucionar todo o tipo de pagamentos, transações e movimentos de ativos derivado ao seu sistema descentralizado (Pacheco, 2018).

A tecnologia *blockchain* é a principal razão pela qual os AV estão, cada vez mais, a tornar-se presentes e capazes de substituir os sistemas atualmente utilizados que começam a ser questionados tendo em conta as potencialidades desta nova tecnologia. Esta tecnologia torna-se disruptiva devido ao facto de criar, de forma totalmente digital, um laço de confiança com os utilizadores, deixando de parte, qualquer tipo de mediador de transação como forma de confiança para acontecer a mesma (Sampaio et al., 2018).

Desta forma, tendo em conta Pacheco (2018), a entidade externa numa transação, como por exemplo os bancos, acaba por ser dispensada pois a tecnologia *blockchain* acaba por, através da sua rede P2P, transformar todos os utilizadores como os próprios mediadores desta transação. A rede P2P funciona conectada ao princípio "pessoa para pessoa" tornando todas as modificações feitas na cadeia de blocos confirmadas pelos seus utilizadores.

Esta rede, através da sua alta tecnologia, guarda e mantém sempre disponível uma cópia do registo de todas as transações efetuadas presentes num livro razão denominado de *ledger* que torna toda a informação nele presente não alterável, de modo a tornar todas as transações fidedignas e credíveis (Gonçalves, 2021). Todas as informações fornecidas e presentes neste livro são validadas e acordadas por todos os intervenientes da rede *blockchain* utilizando um protocolo de segurança. Através deste método novas transações e alterações podem ser realizadas pelos seus utilizadores nunca alterando as informações já presentes nele. Podem ser, ainda, revertidas as informações anteriores partindo do pressuposto que tanto a informação alterada como as alterações feitas ficarão presentes no livro razão de forma a garantir a auditoria e a integridade da rede (Fassano, 2020).

De forma a perceber-se a tecnologia *blockchain*, é importante a abordagem de alguns aspetos como o *hashing*, a prova de trabalho e o sistema P2P.

Deste modo, o *hashing* funciona como o bilhete de identidade de um bloco presente na *blockchain*. Cada bloco tem a sua própria identidade, sendo que, todas as informações presentes nesse bloco geram a criação do *hashing*. A simples alteração de um caráter desse bloco irá transformar o *hashing* num código totalmente diferente. Este processo de criação

funciona como uma função num sentido único, em que o que está presente no bloco gera um *hashing* mas a partir desse mesmo *hashing* não é possível calcular o que se encontra no bloco, mantendo assim, identidades, montantes, transações, entre outros elementos completamente seguros (Helbig, 2022).

De acordo com Vieira (2019), a *blockchain*, em português, cadeia de blocos, na admissão de novos blocos, tem um mecanismo denominado de prova de trabalho (*proof of work*) com o objetivo de gerar dificuldade na criação de um novo bloco e de tornar esse bloco fidedigno de estar presente na cadeia de blocos. Para a alteração de um bloco, tendo acesso o poder de cálculo da rede demoraria cerca de 10 minutos, mas, tendo em conta que cada bloco tem presente em si o *hashing* do anterior, este cálculo teria de ser multiplicado pelo número de blocos presentes nessa cadeia.

Por último a rede P2P e os registos partilhados são o que gere os registos da *blockchain*. Deste modo, todos os participantes da rede *blockchain*, têm acesso a todos os registos que, num sistema financeiro centralizado estaria ao encargo de uma entidade bancária. Utilizando o exemplo anterior da alteração de um bloco, para tornar essa alteração ainda mais segura e fidedigna, apenas será introduzida na rede após, pelo menos, 50% dos participantes da rede P2P estarem convencidos de que a alteração ao bloco é legitima (Gouveia, 2021).

1.3. Das Criptomoedas

As criptomoedas tiveram o seu início na última década do século XX quando David Chaum, famoso criptógrafo norte-americano, através da sua genialidade, criou a *DigiCash* que se tornou na primeira forma de dinheiro "não físico". Esta tecnologia desenvolvida por David gerou um enorme mediatismo em torno do criptografo e do seu produto *eCash* (Narayanan et al., 2016).

Esta, que foi a primeira moeda virtual conhecida e a tornar-se mediática, foi alvo de uma proposta de compra por parte da *Microsft Corporation* no incrível valor de 180 milhões de dólares americanos. Esta proposta, aparentemente irrecusável, viria a ser recusada por parte da empresa de Chaum que viria a aceitar uma proposta similar por parte do *De Nederlandsche Bank*, que se tratava do maior banco de autoridade monetária do pais (Banco Central Holandês). Este passo tomado por David Chaum viria a ser crucial para a falência da sua empresa e ao desaparecimento da *DigiCash*. Apesar do aparente, erro esta criação foi

crucial para o aparecimento das criptomoedas, sendo que as gerações seguintes de moedas virtuais utilizaram a tecnologia de Chaum (Fassano, 2020).

Das empresas que utilizaram a tecnologia base da *DigiCash* a empresa *PayPal* foi a que mais se destacou, estando, ainda, nos dias de hoje em utilização a nível global (Perset, 2010).

O que a *PayPal* veio trazer, que a sua concorrência não conseguiu fornecer, foi a capacidade de efetuar pagamentos online e a realização de transferências entre duas entidades de forma célere e segura sem a tradicional burocracia e morosidade do processo bancário, transformando este processo numa situação quase descentralizada e P2P.

Alguns anos mais tarde surgiu, em 2008, um "cidadão(os) desconhecido(s)" com o pseudónimo de Satoshi Nakamoto que publicou um documento com a informação de que seria lançada uma tecnologia com o intuito de revolucionar o mundo financeiro e que, de certa forma, teria por base a *blockchain* (Evans, 2012). Esta tecnologia revolucionária, denominada de *Bitcoin,* viria a tornar-se a primeira e mais valiosa moeda virtual do mundo e também a "avó" de todas as criptomoedas (Griffith, 2014).

O ecossistema *Bitcoin* inclui a rede principal para propagar transações, a *blockchain* e muitos intermediários, *pools* de mineração e processadores de pagamento que facilitam o comércio (Gandal et al., 2018).

Dado o recente aumento meteórico da *Bitcoin* para níveis além do pico de 2013 (e o enorme aumento nos preços de outras criptomoedas), tendo em conta Vasconcelos (2022), é importante que as bolsas garantam que não existem negociações fraudulentas. O potencial de manipulação cresceu apesar do aumento da capitalização de mercado total porque houve um aumento muito grande no número de criptomoedas. Atualmente, são mais de 300 criptomoedas com capitalização de mercado entre 1 milhão e 100 milhões. Em janeiro de 2014, havia menos de 30 moedas com capitalização de mercado entre os mesmos valores. Assim, existem muitos mais mercados com capitalização de mercado relativamente menor do que havia em 2014.

Como o ecossistema *Bitcoin* atualmente não é regulamentado, o "autopoliciamento" pelos principais utilizadores e organizações é essencial. Além disso, à medida que a *Bitcoin* vai entrando nos sistemas internacionais de finanças e pagamentos, os reguladores podem querer reavaliar as políticas que a deixam não regulamentada e assumir, assim, um papel ativo de supervisão (Antonoulos, 2017).

Devido à sua natureza relativamente "sem lei", as criptomoedas estão sob constante ameaça de ataque. Inúmeros investigadores realizaram estudos para documentar e combater

ameaças como esquemas *Ponzi* (Vasek et al., 2016), lavagem de dinheiro (Toguchi, 2021), *botnets* de mineração e o roubo de "*brain wallets*" (Vasek et al., 2016). Estes autores vinculam com sucesso as transações aos provedores mais populares de serviços *Bitcoin*, como por exemplo, as corretoras de transações. Nenhum desses papéis pode associar transações individuais com usuários específicos em corretoras (Gandal et al., 2018).

Atualmente existem mais de 300 criptomoedas e *altcoins* tornando o mercado cada vez mais estável e avançado tecnologicamente sendo as principais moedas virtuais a *Bitcoin*, a *Ethereum*, a *Cardano*, a *Solana*, a *Tether* e a *DodgeCoin* entre outras. Este crescimento tem trazido, também, avanços astronómicos ao nível da tecnologia *blockchain* (Kushwaha et al., 2022).

Importa referir também a manipulação de preço da criptomoeda *DogeCoin*, que foi alvo de comentários na rede social Twitter por parte do multimilionário Elon Musk no ano de 2021. Esta manipulação de valor feita "apenas" numa rede social trouxe para o top 10 de criptomoedas mais valiosas este AV. Desta forma consegue-se demonstrar a enorme volatilidade deste tipo de AV (Aguiar, 2021).

1.4. Dos *Non Fungible Tokens*

Os NFT são um conceito de AV criado recentemente que se formam ao passar uma matéria digital por um *hash* de forma a criar um código que torna único esse ativo. Desta forma, este tipo de AV são considerados o avanço da arte ou arte digital. O facto que gerou todo o mediatismo em torno deste AV aconteceu em 2021, quando a obra *"Everydays – The First 5000 Days"* de Mike Winklemann foi vendida por cerca de 70 milhões de dólares na casa de leilões "Christie's" (Kafteranis & Turksen, 2022).

O aparecimento dos NFT está ligado, também, ao facto das regras contra o branqueamento de capitais terem sido atualizadas, a nível europeu, ficando mais severas no âmbito dos mercados da arte tradicional (Conselho da União Europeia & Parlamento Europeu, 2018). Esta atualização legislativa levou a que os criminosos tentassem descobrir formas de continuar a cometer ilícitos.

Os NFT podem ser variadíssimos tipos de AV, sendo os mais comuns, objetos em mundos virtuais, caracteres digitalizados do mundo da música, desporto e outras atividades artísticas e também, como seria de esperar, obras de arte de forma virtual (Dowling, 2022). Estes AV são utilizadores da tecnologia *blockchain* o que garante ao seu portador a exclusividade do item que tem bem como os seus direitos de propriedade.

Os NFT dependem diretamente de uma rede *Ethereum* que tem a função de executar programas, como se tratasse de um computador, de forma a virtualizar essa rede através de outros computadores. Esta dependência funciona, na medida em que, os direitos de propriedade destes AV estão registados nessa rede *Ethereum* e, onde à semelhança da arte convencional nos museus e galerias, o seu proprietário pode expor a sua "obra" de forma segura sem perder o seu direito de propriedade ou correr o risco de ser furtado (Ante, 2021).

A grande diferença entre os ativos NFT e os restantes (e.g. *Bitcoin*) prende-se com a capacidade de fundir e unir estes ativos. Enquanto que não existem elementos que diferenciem duas bitcoins tornando-as, iguais na sua composição, o mesmo não se pode dizer dos NFT que, como o nome indica são algo que não tem a possibilidade de ser fundido ou unido a um outro elemento (Kafteranis & Turksen, 2022). Através da compra de NFT o proprietário garante um certificado de autenticidade que não pode ser modificado, perdido ou destruído tornando assim estes AV únicos (Carron, 2021).

1.5. Dos *Virtual Assets Service Providers*

Os VASP são prestadores de serviços de AV que podem ser definidos por uma pessoa física ou jurídica não estando, esta, coberta pelas recomendações das condutas e normas dos negócios que fornecem um serviço para outras pessoas dentro das seguintes áreas (GAFI, 2021):

- Trocas de AV por moeda fiduciária;
- Trocas entre AV;
- Transferências de AV;
- Guarda e/ou administração de AV;
- Cedência de instrumentos que permitam o controlo dos AV;
- Prestação de serviços financeiros relacionados com a oferta e/ou venda de AV.

A definição de VASP deveria ser elucidada e adotada a nível internacional, coisa que não acontece, de modo a que os países soubessem como controlar estas empresas e/ou pessoas prestadoras de serviços. Este tipo de prestação de serviços, muitas vezes tenta utilizar definições que os favorecem nos termos legais de forma a não serem vistos como VASP recorrendo ao método de trabalho que utilizam ou à tecnologia que promovem (Broby & Quimbayo, 2021).

1.6. Dos Sistemas Financeiros Centralizados vs. Descentralizados

À primeira vista, os sistemas centralizados, em comparação com os sistemas descentralizados, podem parecer muito distintos e dispares, mas à medida que vamos dissecando estes dois tipos de sistemas financeiros conclui-se que as maiores diferenças estão conectadas às questões quem controla os ativos, quão transparente é o sistema (seja ele Centralizado ou Descentralizado) e quais os tipos de proteções e privacidade que estes sistemas promovem junto do consumidor final (Qin et al., 2021).

Começando por analisar os sistemas financeiros descentralizados, de agora em diante denominados de DeFi. Kalodner et al. (2015) observam uma completa otimização por parte destes protocolos em relação aos sistemas financeiros centralizados (CeFi), recorrendo às funcionalidades e tecnologia fornecidas pelas propriedades exclusivas da *blockchain.*

Recorrendo a um exemplo prático, de acordo com Carapella et al. (2022) e Zarrin et al. (2021), nos sistemas CeFi existe um modelo, por parte da entidade reguladora da transferência, de livro de ordens que no sistema DeFi é substituído e otimizado, em comparação aos sistemas CeFi por um *Automated Market Maker* que se trata de um contrato inteligente que limita as negociações à existência de apenas duas entidades, excluindo, desta forma, a terceira que seria a entidade reguladora. Este processo, para além de ser inovador por reduzir o número de partes envolvidas reduz, também, os custos das transações.

Por outro lado, nas finanças tradicionais ou os sistemas CeFi, existem diversos intermediários tais como instituições financeiras, bancos, provedores de mercado, bolsas de valores, etc. A função primordial destes intermediários é reunir a maior quantidade de pessoas para utilizarem os seus serviços, sejam pessoas com recursos financeiros ou pessoas que procuram recursos financeiros. Existe o pensamento de que, os sistemas CeFi são o ponto central que separa os sistemas financeiros baseados no mercado nos seus setores tradicionais de pagamentos, transações valores mobiliários, seguros e dinheiro numa forma geral. Deste modo, os sistemas CeFi são caracterizados por serem grandes intermediários onde estão centralizadas as funções e os recursos financeiros (Zetzsche et al., 2020).

1.7. Das Vantagens e Desvantagens do Recurso a Ativos Virtuais

As vantagens dos sistemas DeFi são, muitas vezes, tidas como “promessas” em relação aos sistemas CeFi por ainda não terem a consistência e aderência destes sistemas. As principais vantagens resultantes da tecnologia *blockchain* são a alta transparência em todas as ações efetuadas nesta rede por ficar tudo registado e acessível aos seus usuários de forma

rápida e segura, a confiança e a imutabilidade que faz com que se torne impraticável a tentativa de alteração dos blocos gerados na *blockchain.* Neste sistema existe o termo "pseudotransparencia" que se aplica pelo facto dos usuários não revelarem na totalidade a sua identidade mas apenas a sua chave pública permanecendo, assim, em anonimato (Wieandt & Heppding, 2022).

Segundo Helbig (2022) torna o sistema dependente da tecnologia *ledger* que vem deste modo substituir a entidade central (e.g. Bancos) nos sistemas CeFi. Apesar do grande escrutinio nestas redes, existe o pressuposto de que os seus participantes, na sua grande maioria, sejam bem intencionados e que confiem nos sistemas de deteção e eliminação de comportamentos maliciosos por parte de utilizadores fraudulentos.

Existe, de acordo com Qin et al. (2021), também, o conceito de autosoberania que se trata do acesso democrático e sem permissão a produtos financeiros. Este conceito, no sistema DeFi permite que os utilizadores tenham a capacidade de gerir os seus dados pessoais e os seus fundos. Deste modo não existe uma dependência por parte das entidades centrais o que leva à menor possibilidade de ocorrência de erros e perdas de valores por más condutas ou comportamentos maliciosos por parte das entidades reguladoras e centrais.

A inclusão financeira faz parte do dicionário dos sistemas DeFi que, ao contrário dos sistemas CeFi, não cria barreiras ao acesso aos seus serviços. Esta inclusão é maximizada através das baixas taxas de transações por não ter de existir um pagamento a uma entidade externa (Carapella et al., 2022).

Relativamente às desvantagens do recurso aos AV, tendo em conta a ótica de Zarrin et al. (2021), estão conectadas com os sistemas DeFi em relação aos CeFi onde existem desafios, economicos e técnicos que, por alguns autores, são tidas como desvantagens. Estes desafios são vistos como vulnerabilidades de contratos inteligentes no sistema DeFi, preocupações ao nível da privacidade e ceticismo ligado à tecnologia *blockchain*.

É importante referir também que os altos níveis de alavancagem, a incerteza regulatória e as possíveis barreiras de entrada para novos usuários com menos capacidade financeira que realizam transações de baixo valor são, também, algumas das desvantagens e riscos económicos ao recurso a AV em relação aos sistemas CeFi. A alta alavancagem pode ser provocada pelos usuários fazendo com que os ativos ganhem um valor especulativo e bastante variável. Por outro lado, a incerteza regulatória está interligada com o facto do uso destes ativos não ser regulado por nenhuma entidade e sim por uma tecnologia, sendo que não existe, também, um quadro regulatório de impostos para este tipo de sistema tornando-

o assim imprevisível, arriscado e desvantajoso, em certos aspetos, economicamente (Zetzsche et al., 2020).

Tendo em conta que o sistema DeFi, alimentado maioritariamente pela *blockchain*, foi implementado de forma embrionária e em larga escala, estando, constantemente, a sofrer alterações, existem diversos aspetos que divergem do sistema CeFi e consequentemente vêm introduzir alguns desafios a superar.

Deste modo, o primeiro desafio abordado será a volatilidade financeira que, tendo em conta um passado recente, pode-se concluir que o sistema DeFi, recorrendo aos AV, oferece uma volatilidade mais acentuada. Segundo Wieandt & Heppding (2022), "Ether, uma das criptomoedas mais importantes no sistema DeFi, flutuou cerca de 73% em média entre 2018 e 2021, enquanto o Standard & Poor's 500 (S&P 500)[2] flutuou cerca de 13% em média no mesmo período." No sistema CeFi existem 43 bancos centrais com a função de garantir a estabilidade dos preços, coisa que não acontece no sistema DeFi.

Em segundo lugar surge o desafio da proteção do consumidor que, com o recurso ao exemplo do sistema CeFi, onde existem entidades reguladoras com tarefas de supervisão, não deixam de ocorrer escândalos económico-financeiros. Por outro lado, os sistemas DeFi não têm nenhuma autoridade central que proceda a este controlo e supervisão. Deste modo a proteção dos consumidores é alcançada tecnicamente e com o recurso à boa fé dos utilizadores (Li et al., 2020).

Em terceiro lugar o pseudoanonimato conseguido através dos protocolos de segurança da rede *blockchain*, onde apenas é demonstrado a chave pública dos intermediários de modo a existir apenas as ações de forma pública e não quem as praticou. Deste modo, no sistema CeFi existe a necessidade de autenticação dos intervenientes devido às regras e regulamentações legais de cada Estado (Carapella et al., 2022; Qin et al., 2021).

Em quarto lugar, a falta de regulamentação e a incerteza legal deixam o sistema DeFi com um grau de incerteza associado. Esta lacuna não pode ser colmatada tendo em conta as normas do sistema CeFi pois estas acabam por ser o resultado de anos de trabalho por parte das entidades reguladoras (Li et al., 2020; Zarrin et al., 2021).

Por último, é importante referir a visão das instituições em comparação com a funcionalidade deste tipo de sistema. No sistema DeFi não existe necessidade de uma

[2] O S&P 500 é um índice de ações que representa as 500 maiores empresas negociadas nas bolsas de valores dos Estados Unidos. É calculado pela Standard & Poor's, uma das principais empresas de análise financeira do mundo, e é amplamente utilizado como indicador da saúde e do desempenho do mercado acionista americano.

entidade ou intermediário pois todas as funcionalidades financeiras são implementadas por contratos inteligentes. Por outro lado o sistema CeFi acaba por ser o oposto pois tem entidades que exercem um papel fulcral em função da confiança e fidedignidade do sistema e de forma a reduzir assimetrias de informação (Zetzsche et al., 2020).

CAPÍTULO 2 – INVESTIGAÇÃO ECONÓMICO FINANCEIRA

2.1. Da Criminalidade Económico-Financeira

A criminalidade económico-financeira é muitas vezes associada a crimes cometidos por entidades com poder seja ele político, social e ou económico que, por norma, pertencem às elites das classes mais abastadas financeiramente sendo este tipo de crimes comummente conhecidos por crimes de colarinho branco. Estes crimes têm como objetivo principal a obtenção de lucros ilimitados recorrendo a atividades legais, tornando a sua deteção e a consequente aplicação da lei bastante complexas. São exemplos de crimes económico-financeiros os "Crimes Tributários (fiscais, aduaneiros e contra a segurança social); Crimes de burla e abuso de confiança contra o Estado e setor bancário; Crimes de corrupção, participação económica em negócio; Administração Danosa; Crimes do mercado de valores mobiliários; Branqueamento de capitais." (E. Dias, 2011).

A criminalidade económico-financeira foi caracterizada pelo Conselho da Europa como ações praticadas por duas ou mais pessoas num projeto criminal com o objetivo de obter poder e lucro através de negócios ilegais, usando violência, intimidação e influência nos pontos estratégicos da política, da economia, do mediatismo, do governo e da atividade judicial (Filipe, 2018).

Enquanto que, por parte de Hassemer, surge uma definição mais restrita e operacional, onde este tipo de criminalidade se torna num conjunto de comportamentos com elevada relevância penal, com o objetivo de somar ganhos ilícitos, sendo que, os bens e os interesses financeiros do Estado saem lesados nesse processo (Hassemer citado in Bravo, 2013).

Tendo em conta a legislação portuguesa, de acordo com a Lei n.º 36/ 1994 de 29 de setembro, fazendo realçar a criminalidade organizada com recurso a tecnologia informática sendo de dimensão internacional ou transnacional, tal como a corrupção, fraude e administração danosa.

Segundo Lobão (2019) o conceito é muito mais amplo, nos dias de hoje, abrangendo todos os tipos de crimes, violentos ou não violentos, com resultados de subtração económica ou financeira. Apesar de todas as definições suprarreferidas, a Comunidade Europeia continua sem atingir um consenso quanto ao catálogo de crimes que se enquadram neste conceito.

Por outro lado, Bravo (2013) refere que, a criminalidade organizada e a económico-financeira não se tratam de conceitos puramente jurídicos sendo também operacionais e/ou instrumentais. Estes acabam por ser associados a algumas especificidades de criminalidade já recorrentes nos processos penais portugueses. Acabam por consumar crimes contra pessoas, património, exercício de funções públicas, economia, através da tecnologia da informação, mercado de valores mobiliários, corrupção e branqueamento de capitais.

Esta tipologia criminal, na ótica de Figueiredo (2021), tendo em conta as movimentações ilícitas de capitais, rendimentos e bens que, por sua vez, são angariados através de práticas ilícitas que podem ser consideradas a nível nacional, mas também internacional, é denominada de economia do crime.

Tendo em conta o 11º Congresso das Nações Unidas sobre a Prevenção do Crime e Justiça Penal, que teve lugar em Banguecoque no mês de abril do ano de 2005. A definição de crime económico foi estabelecida como “toda a forma de crime não-violento que tem como consequência uma perda financeira. Este crime engloba uma vasta gama de atividades ilegais, como a fraude, a evasão fiscal e o branqueamento de capitais " (ONU, 2005, p. 1 citado por Cruz, 2018).

2.2. Das Medidas de Combate à Criminalidade Económico-Financeira (*SOFT LAW*)

O desenvolvimento tecnológico associado aos AV tem sido uma plataforma de grande inovação, permitindo não só uma forma de pagamento enquanto transmissão de valor, mas também um meio de financiamento para novos projetos. No entanto, a presença de fraudes evidencia a necessidade de uma estruturação e organização adequadas (R. Ferreira, 2022).

Tendo em conta o suprarreferido, na opinião de Santos (2018), o sistema descentralizado da *blockchain* deve basear-se em princípios fundamentais, como a descentralização, democratização e transparência. O estado atual do mercado dos AV, que tem negligenciado o controlo e não prevê sanções, preocupa diversas entidades da EU, sendo que, algumas dessas entidades caminham na direção de alguns projetos do Parlamento Europeu, embora, neste momento, sejam apenas instrumentos de S*oft Law* e autorregulação, como os "códigos de boa governança".

Desta forma, o Parlamento Europeu não negligencia a importância da *Soft Law*, que é um assunto analisado e estudado pela Comissão dos Assuntos Jurídicos desse mesmo organismo. Por definição, a *Soft Law* pode ser considerada como "normas de conduta que,

em princípio, não têm força jurídica obrigatória *per si*, mas que ainda assim podem produzir alguns efeitos jurídicos" (Snyder, 1993, p. 32 citado in Almeida, 2022).

Assim, os efeitos jurídicos da *Soft Law*, por não serem obrigatórios, são indiretos e visam produzir efeitos práticos. Esses instrumentos são geralmente usados para preencher lacunas na legislação, já que nem sempre é possível legislar sobre questões que afetam todos os países membros de forma geral (Dawson, 2016).

Segundo Antunes (2018) são os "códigos de boa governança" mencionados anteriormente, que fornecem orientações não vinculativas para os setores e organizações a fim de promover a transparência e a responsabilidade. Outros exemplos incluem os Livros Brancos da Comissão Europeia, que contêm propostas de ação da UE em áreas específicas e são usados para lançar debates públicos e obter consensos políticos entre partes interessadas, o Conselho e o Parlamento Europeu.

A S*oft Law* na UE também pode incluir outras formas de instrumentos, como declarações comuns, resoluções do Conselho, códigos de conduta, conclusões do Conselho, orientações, comunicações e recomendações. Esses instrumentos também podem abranger o fenômeno da corregulação, que é uma forma de colaboração entre setores privados e públicos para estabelecer padrões e regulamentações para uma determinada área (Maia, 2018).

Dessa forma, segundo Melkevik & Melkevik (2017), mesmo sendo um instrumento informal e flexível, a *Soft Law* pode acabar a assumir um papel jurídico importante ao condicionar a atuação de um determinado sujeito. Esta questão, verifica-se quando os destinatários das orientações e diretrizes passam a ter uma confiança legítima na sua aplicação, o que pode levar a uma autolimitação da conduta do regulador. Caso haja um desvio dessas linhas diretrizes, pode haver violação dos princípios da igualdade de tratamento, segurança jurídica e proteção da confiança, o que pode ser sancionado jurisdicionalmente.

Podemos abordar, também, a figura dos Códigos de Conduta, que são exemplos de instrumentos de *Soft Law* utilizados em diversos setores, tais como o setor bancário, o setor da publicidade e o setor da comunicação social. Estes códigos não têm valor jurídico obrigatório, mas visam orientar a conduta dos profissionais destes setores, promovendo a autorregulação e a melhoria da qualidade do serviço prestado. Ainda assim, em caso de violação destes códigos, as entidades reguladoras podem utilizar tais violações como fundamento para a aplicação de sanções, desde que existam normas legais que as prevejam (R. Ferreira, 2022). De acordo com Almeida (2022) “pode-se associar ao instrumento da *Soft*

Law à Lei-quadro das Entidades Reguladoras, em específico a norma relativa aos poderes destas entidades em emitirem recomendações e diretivas genéricas, não assumindo valor vinculativo[3].”

A regulação dos criptoativos ainda é um tema em evolução e incerto no âmbito da UE, havendo um reconhecimento de que a tecnologia subjacente aos criptoativos traz oportunidades e desafios ao setor financeiro e à proteção dos consumidores (Maia, 2018). Nesse sentido, a utilização de instrumentos de *Soft Law* permite uma abordagem mais flexível e adaptável a um contexto em constante mudança, permitindo aos reguladores alertar para os riscos e incentivar a adoção de boas práticas sem a rigidez de uma regulamentação formal. No entanto, segundo Catarino (2022), é importante notar que a *Soft Law* não é capaz de conferir força vinculativa e que uma regulação mais estruturada e formal poderá ser necessária no futuro para garantir a estabilidade e segurança do mercado de criptoativos.

A complexidade técnica associada aos criptoativos e à sua diversidade funcional torna a regulamentação um desafio significativo. Posto isto, a natureza transnacional do mercado de AV significa que a regulamentação precisa de ser coordenada internacionalmente, para evitar fragmentação regulatória e riscos para a integridade do mercado.

A *Soft Law*, neste contexto, pode ser uma ferramenta útil para os reguladores comunicarem as suas intenções e expectativas em relação ao mercado de criptoativos, incentivando o desenvolvimento de melhores práticas e normas voluntárias de autorregulação. No entanto, é importante lembrar que a *Soft Law* não pode substituir a necessidade de legislação clara e vinculativa, especialmente quando se trata de proteger os consumidores e investidores contra fraudes e riscos financeiros (Almeida, 2022).

Em suma, existem dois grandes obstáculos à regulação deste tipo de mercados. O primeiro prende-se com a regulamentação de alguns setores, nomeadamente o financeiro, que para além de extremamente exigente pode trazer algum tipo de dificuldade à inovação do mesmo. O segundo aborda a globalidade dos mercados de AV ultrapassando fronteiras e tornando-se internacionais entre os seus intervenientes o que traz diversos obstáculos à regulamentação pois tem de ser o máximo abrangente possível de modo a enquadrar todos os intervenientes.

Já o parâmetro da autorregulação poderá ser uma solução eficiente no mercado dos AV, onde as partes interessadas são capazes de definir as suas próprias regras de conduta e procedimentos de governança, sem depender exclusivamente de regulamentação

[3] Cfr. alínea b), do n.º 2, do art.º 40.º, da Lei n.º 67/2013, de 28 de Agosto.

governamental. Esta abordagem é comummente utilizada em vários setores de atividade, incluindo o financeiro, mas requer um compromisso e uma adesão voluntária por parte dos intervenientes do mercado (Santos, 2018).

No contexto dos criptoativos, Ferreira (2022) refere que, a autorregulação poderia ser realizada através de iniciativas da indústria, tais como a criação de códigos de conduta ou de melhores práticas, que estabelecessem normas de transparência, segurança, privacidade e prevenção de fraude. Estas normas poderiam ser implementadas por entidades como associações de empresas ou organizações de autorregulação, que poderiam ter um papel ativo na definição e aplicação de normas de conduta.

Embora a autorregulação possa apresentar algumas vantagens, como a flexibilidade e rapidez na resposta às mudanças do mercado, é importante notar que a sua eficácia depende da capacidade e vontade dos intervenientes do mercado para cumprir as normas acordadas. A autorregulação não deve ser vista como uma alternativa à regulamentação governamental, mas como um complemento que pode ajudar a preencher as lacunas da regulamentação em situações de incerteza ou mudança rápida (Comité Económico e Social Europeu, 2012).

2.3. Das Estruturas de Combate à Criminalidade Económico-Financeira

As estruturas de combate à criminalidade Económico-Financeira portuguesas, na atualidade, que serão abordadas nesta investigação serão a Comissão de Coordenação das Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, o Gabinete de Recuperação de Ativos (GRA) e a Unidade de Informação Financeira (UIF), ambos da Polícia Judiciária (PJ) e o Gabinete de Cibercrime da Procuradoria Geral da República (PGR). Estas têm como, principal, missão o combate à criminalidade económico-financeira e a cooperação e coordenação nacional e internacional no âmbito deste tipo de ilícitos de modo a que todos os elementos confluam num esforço e trabalho único na persecução da criminalidade.

2.3.1. Da Comissão de Coordenação das Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo

A Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo (BC/FT) criada pela Resolução do Conselho de Ministros n.º 88/2015[4], de 1 de outubro, e funciona na

[4] Cfr. n.º 1.º, da Resolução do Conselho de Ministros n.º 88/2015.

dependência direta do Ministério das Finanças (Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, 2015).

Esta tem "como principal missão acompanhar e coordenar a identificação, avaliação e resposta aos riscos Branqueamento de Capitais e Financiamento de Terrorismo (BC-FT) a que Portugal está ou venha a estar exposto, contribuindo para a melhoria contínua da conformidade técnica e da eficácia do sistema nacional de combate BC-FT." (Nunes, 2018 citado em V. Costa, 2022).

Esta comissão veio a sofrer alguns aditamentos às suas competências específicas com a criação da Lei 83/2017 de 18 agosto. Tem assim como missão geral "acompanhar e coordenar a identificação, avaliação e resposta aos riscos de BC-FT a que Portugal está ou venha a estar exposto, contribuindo para a melhoria contínua da conformidade técnica e da eficácia do sistema nacional de combate ao BC-FT" (Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, 2015).

Tem como principais atribuições[5] as seguintes:

- Avaliar e propor a adoção de políticas necessárias ao prosseguimento da estratégia nacional de prevenção e combate ao BC/FT[6];
- Assegurar, numa base contínua, a atualização da avaliação nacional de riscos de branqueamento de capitais e de financiamento do terrorismo, desenvolvendo os instrumentos, procedimentos e mecanismos necessários[7];
- Avaliar a conformidade técnica e a eficácia do sistema nacional de prevenção e combate ao BC/FT[8];
- Propor medidas legislativas, regulamentares e operacionais[9];
- Promover a coordenação e a cooperação entre todas as autoridades com responsabilidades no domínio da prevenção e combate ao BC/FT[10];
- Preparar avaliações do sistema nacional de prevenção e combate ao BC/FT solicitadas por organismos supranacionais com competência na matéria[11];

[5] Cfr. n.º 3, da Resolução do Conselho de Ministros n.º 88/2015.
[6] Cfr. n.º 3, alínea a) da Resolução do Conselho de Ministros n.º 88/2015.
[7] Cfr. n.º 3, alínea b), da Resolução do Conselho de Ministros n.º 88/2015.
[8] Cfr. n.º 3, alínea c), da Resolução do Conselho de Ministros n.º 88/2015.
[9] Cfr. n.º 3, alínea e), da Resolução do Conselho de Ministros n.º 88/2015.
[10] Cfr. n.º 3, alínea i) e j), da Resolução do Conselho de Ministros n.º 88/2015.
[11] Cfr. n.º 3, alínea m), da Resolução do Conselho de Ministros n.º 88/2015.

- Prestar colaboração às autoridades competentes, no âmbito da aplicação, em território nacional, de medidas restritivas adotadas pelas Nações Unidas, pela União Europeia (UE) ou por outras organizações internacionais[12] (Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, 2015).

2.3.2. Do Gabinete de Recuperação de Ativos

O GRA, na dependência da Polícia Judiciaria[13] e criado através da Lei 45/2011, de 24 de junho e a sua missão[14] é identificar, localizar e confiscar bens ou produtos relacionados a crimes, tanto em âmbito nacional quanto internacional, cooperar com outros Estados que tenham gabinetes de recuperação de ativos e exercer outras competências que lhe sejam legalmente atribuídas. Além disso, o GRA é responsável por coletar, analisar e processar estatísticas anonimizadas resultantes da sua atividade ou aquelas que a lei exige que sejam comunicadas, incluindo informações sobre apreensões e aplicação de medidas de garantia patrimonial em processos criminais, bem como o destino final dos bens apreendidos, como restituição, envio para autoridades de outros estados em cumprimento de pedidos de cooperação judicial internacional ou declaração de perda a favor do Estado (Polícia Judiciária, 2011).

Segundo o website da PJ e o art.º 5.º da Lei 45/2011, de 24 de junho, o GRA "tem composição multidisciplinar, integrando elementos da Polícia Judiciária, do Instituto dos Registo e Notariado e da Autoridade Tributária e Aduaneira. Está sediado em Lisboa e tem Delegações no Porto, em Coimbra e em Faro."(Polícia Judiciária, 2011).

2.3.3. Da Unidade de Informação Financeira

A UIF, foi incorporada na estrutura da PJ por meio do Decreto-Lei (DL) n.º 304/2002, de 13 de dezembro, e é atualmente definida como um serviço da Direção Nacional pela nova orgânica da PJ aprovada pelo DL n.º 137/2019, de 13 de setembro. As competências da UIF estão estabelecidas no artigo 27.º do DL n.º 137/2019 e no artigo 82.º da Lei n.º 83/2017, de 18 de agosto (Polícia Judiciária, 2017).

A UIF, tem como responsabilidade a recolha, centralização, tratamento e disseminação de informações relacionadas à prevenção e investigação de crimes como o

[12] Cfr. n.º 3, alínea q), da Resolução do Conselho de Ministros n.º 88/2015.
[13] Cfr. art.º 2.º, da Lei 45/2011, de 24 de junho.
[14] Cfr. art.º 3.º, da Lei 45/2011, de 24 de junho.

branqueamento de vantagens de origem ilícita, financiamento do terrorismo e crimes tributários em âmbito nacional. Além disso, esta unidade está encarregue de cooperar com a autoridade judicial (AJ), as autoridades de supervisão e fiscalização, entidades financeiras e não financeiras previstas na Lei n.º 83/2017, de 18 de agosto. No âmbito internacional, a UIF colabora com outras unidades de informação financeira ou estruturas similares[15] (Polícia Judiciária, 2017).

Compete[16] à UIF:

- Receber, centralizar, tratar e analisar as comunicações de operações suspeitas efetuadas no exercício do dever de comunicação[17];
- É responsável por recolher, centralizar, tratar e analisar informações provenientes de outras fontes, relacionadas à prevenção e investigação de atividades criminosas que envolvam fundos ou outros bens decorrentes do branqueamento de capitais ou do financiamento do terrorismo[18];
- Difundir informações relevantes, incluindo análises e resultados, no âmbito nacional[19];
- Cooperar com outras autoridades nacionais que tenham funções relevantes na prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo. Essa cooperação pode incluir a partilha de informação, a realização de ações conjuntas ou outras formas de colaboração que sejam consideradas necessárias e adequadas[20];
- Cooperar no plano internacional com unidades congéneres, nos termos previstos na lei e nos instrumentos de cooperação internacional aplicáveis. Esta cooperação pode envolver a partilha de informações, a realização de investigações conjuntas e o intercâmbio de boas práticas no âmbito da prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo[21] (Polícia Judiciária, 2017).

[15] Cfr. n.º 1, do art.º 27.º, da DL n.º 137/2019, de 13 de setembro.
[16] Cfr. n.º 1, do art.º 82.º, da Lei n.º 83/2017, de 18 de agosto.
[17] Cfr. n.º 1, alínea a), do art.º 82.º, da Lei n.º 83/2017, de 18 de agosto.
[18] Cfr. n.º 1, alínea b), do art.º 82.º, da Lei n.º 83/2017, de 18 de agosto.
[19] Cfr. n.º 1, alínea c) do art.º 82.º, da Lei n.º 83/2017, de 18 de agosto.
[20] Cfr. n.º 1, alínea d) do art.º 82.º, da Lei n.º 83/2017, de 18 de agosto.
[21] Cfr. n.º 1, alínea e), do art.º 82.º, da Lei n.º 83/2017, de 18 de agosto.

2.3.4. Do Gabinete de Coordenação da Atividade do Ministério Público na Área da Cibercriminalidade (Gabinete Cibercrime)

O Gabinete de Coordenação da Atividade do Ministério Público (MP) na área da Cibercriminalidade, na continuação deste trabalho referido como Gabinete Cibercrime, é uma entidade diretamente subordinada à Procuradoria-Geral da República. Criado por Despacho do Procurador-Geral da República, a 7 de dezembro de 2011 e liderado por um Procurador da República, a sua finalidade primordial é coordenar internamente, no âmbito do MP, as atividades relacionadas à cibercriminalidade, além de promover a capacitação especializada nessa área e estabelecer canais de comunicação eficazes com prestadores de serviços de acesso às redes de comunicação, a fim de facilitar a sua colaboração em investigações criminais (Procuradoria-Geral Da República - Despacho de Criação Gabinete Cibercrime, de 7 de Dezembro de 2011, 2011).

O Gabinete Cibercrime tem como objetivo coordenar as atividades do MP na área da cibercriminalidade e estabelecer canais de comunicação com fornecedores de serviços de acesso às redes de comunicação. Além disso, mantém uma rede de pontos de contato em todo o país, que tem como responsabilidade partilhar questões relativas ao cibercrime e à obtenção de prova digital que surjam em processos concretos, bem como o resultado dos debates que ocorram na rede (Ministério Público, 2009b).

A criminalidade praticada no meio digital, também conhecida como cibercriminalidade, não se limita às disposições da Lei do Cibercrime (Lei nº 109/2009 de 15 de setembro), uma vez que diariamente surgem novos tipos de crimes convencionais que são cometidos em ambiente digital (Ministério Público, 2009a).

Os magistrados do MP têm tido diferentes pontos de vista sobre a legislação relativa à cibercriminalidade e à obtenção de provas digitais, o que tem levado a soluções distintas em casos similares. Uma das tarefas do Gabinete Cibercrime é a coordenação que possibilite uma abordagem mais uniforme e coerente do MP em relação aos mesmos crimes relevantes do ponto de vista criminal (Ministério Público, 2009a).

A contínua e ininterrupta progressão das tecnologias e sua consequente influência nas atividades criminosas demandam uma busca incessante por atualização e adaptação, sendo que, a emergência desta nova realidade suscitou a necessidade de interação entre as autoridades encarregadas de investigar crimes e entidades privadas. O Gabinete Cibercrime tem como objetivo facilitar o contato dos magistrados responsáveis pela investigação com terceiros, garantindo uma colaboração eficaz e rápida, além de criar canais ágeis de comunicação com entidades responsáveis pela segurança informática, para garantir pronta

capacidade de resposta quando forem solicitadas a cumprir as suas obrigações legais (Ministério Público, 2009a).

Os objetivos principais do Gabinete Cibercrime estão relacionados com a resolução efetiva de investigações criminais que ocorrem nas redes de comunicação. Para alcançar esses objetivos, é necessário conhecer as tendências e práticas criminais associadas a essa área. Isso pode incluir o acompanhamento de processos em andamento, tanto de uma forma geral quanto de maneira mais direta e próxima, conforme previsto no Estatuto do MP. O objetivo final é garantir a resolução eficaz de crimes cibernéticos e colaboração eficiente entre autoridades e entidades privadas para alcançar esse objetivo (Ministério Público, 2009a).

2.4. Dos *Atores* no Combate à Criminalidade Económico-Financeira

Existe a necessidade de dissecar os *atores* preponderantes no combate à criminalidade económico-financeira. Com esse efeito, o subcapítulo 2.4 vem detalhar cada um deles de modo a que se perceba qual o papel, tendo em conta a problemática investigada e as suas funções no panorama nacional e internacional.

2.4.1. Da Guarda Nacional Republicana – Unidade de Ação Fiscal

É interessante observar que a evolução da estruturação das forças e serviços de segurança em Portugal está intimamente ligada à evolução do panorama nacional e internacional, bem como à necessidade de modernização da administração pública. A Guarda Fiscal, criada em 1885, foi uma importante força de fiscalização dos impostos e rendimentos públicos, mas foi extinta em 1992 devido à necessidade de adaptação ao contexto pós-integração de Portugal na UE. A sua integração na GNR deu origem à Brigada Fiscal, que mais tarde viria a ser transformada na atual Unidade de Ação Fiscal (UAF), com competência específica de investigação para a missão tributária, fiscal e aduaneira (V. Costa, 2022).

A GNR passou por uma reorganização que levou à aprovação de uma nova Lei Orgânica (LOGNR) em vigor desde 6 de dezembro de 2007. De acordo com o artigo 41º desta Lei, foi criada a UAF, uma unidade especializada a nível nacional responsável pela investigação no âmbito das áreas tributária, fiscal e aduaneira da Guarda. (Garção, 2008) A criação da UAF dentro da GNR de acordo com Lourenço (2017) é uma resposta do Estado português ao aumento da criminalidade fiscal e tributária, bem como ao incremento da

economia paralela. Esta unidade especializada tem como missão investigar e fiscalizar ações relacionadas com a tributação, fiscalização e aduaneira, bem como prevenir e combater a evasão fiscal, o BC/FT.

O Regulamento Geral do Serviço da GNR, por sua vez, estabelece que as missões de prevenção e investigação da atividade tributária, fiscal e aduaneira são da responsabilidade da UAF em todo o território nacional. O Despacho n.º 62/09-Ordem à Guarda, de 30 de dezembro, atribui à unidade diversas funções, tais como executar ações de investigação criminal e fiscalização tributária em todo o país, apoiar operacionalmente e tecnologicamente as atividades de investigação e coordenar a fiscalização da circulação de mercadorias (V. Costa, 2022; Garção, 2008).

A UAF é responsável pela investigação das infrações tributárias, fiscais e aduaneiras, enquanto o restante dispositivo territorial da GNR é responsável pela fiscalização e controlo da circulação de mercadorias sujeitas à ação tributária, fiscal ou aduaneira. A missão da UAF é prevenir, descobrir e investigar os crimes e contraordenações consignados no Regime Geral das Infrações Tributárias (RGIT) (R. Costa, 2013; Lourenço, 2017).

Para compreender como a UAF realiza ações de fiscalização, é necessário entender o processo penal tributário descrito no Capítulo I da Parte II do RGIT. Este diploma prevê infrações tributárias, e é responsabilidade da UAF, como OPC, adquirir informações sobre crimes tributários e proceder de acordo com o artigo 243.º do CPP, que se refere ao auto de notícia. Além disso, Lopes (2022) refere que, a competência da UAF inclui processos de contraordenação tributária, já que o artigo 59.º do RGIT estipula que os OPC são responsáveis pela fiscalização tributária. O artigo 67.º do RGIT também menciona a UAF como competente para instruir processos de contraordenação resultantes dos autos produzidos pelos seus membros.

O artigo 7.º, n.º4, alínea a) da Lei de Organização da Investigação Criminal (LOIC) estabelece a competência concorrencial da UAF na investigação de crimes tributários de valor superior a 500 000€, juntamente com a PJ. Essa previsão é considerada segundo Assunção (2010) um "capital de enorme confiança" para a UAF e afasta qualquer dúvida sobre a sua competência para investigar crimes tributários além dos crimes aduaneiros previstos no RGIT (artigo 41.º) (Cardoso, 2020).

Segundo P. Dias (2017) a proatividade na recolha de informações é, de facto, essencial para o sucesso da investigação de crimes tributários. A utilização de técnicas de inteligência e análise de informação permite à UAF desenvolver uma visão global dos fenómenos criminais e identificar os seus padrões e tendências. Desta forma, é possível

antecipar e prevenir a prática de crimes tributários, bem como identificar e responsabilizar os seus autores.

2.4.2. Da Polícia Judiciária – Unidade Nacional de Combate à Corrupção e Unidade Nacional Combate ao Cibercrime e à Criminalidade Tecnológica

A PJ, no âmbito do combate à criminalidade económico-financeira, indo de encontro ao propósito deste trabalho, tem duas unidades que devem ser alvo de estudo, sendo elas a Unidade Nacional de Combate à Corrupção (UNCC) e a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T).

Deste modo e segundo o DL n.º 137/2019, de 13 de setembro a UNC3T é uma unidade especializada da PJ que atua na prevenção e repressão do cibercrime e de outros crimes tecnológicos[22]. Foi criada em 2014, no âmbito da reforma da PJ, e tem como missão principal combater a criminalidade informática em todas as suas vertentes e é composta por uma equipa multidisciplinar de investigadores, peritos informáticos e analistas de dados, que trabalham em estreita colaboração com outras unidades da PJ e com outras agências nacionais e internacionais. A sua atuação inclui a investigação de crimes informáticos, a prevenção e a sensibilização da sociedade civil para as questões de segurança na internet, a cooperação com outras unidades de combate ao cibercrime a nível internacional e a produção de conhecimento especializado na área (Polícia Judiciária, 2020).

A UNCC é uma unidade da PJ que foi criada após a nova Lei Orgânica da Polícia Judiciária, Lei nº37/2008 de 6 de agosto, ter sido aprovada, o que resultou na extinção da Direção Central de Investigação da Corrupção e Criminalidade Económica e Financeira (DCICCEF) (R. Costa, 2013).

A sua missão está descrita no DL n.º 42/2009, de 12 de fevereiro, que lhe atribui a competência de prevenção, deteção, investigação criminal e colaboração com as autoridades judiciais em relação aos crimes de corrupção, peculato, tráfico de influências e participação económica em negócio. Além disso, as suas competências no combate à criminalidade fiscal e aduaneira foram definidas no seu artigo 2.º, incluindo os crimes económico-financeiros, branqueamento de capitais e crimes tributários de valor superior a 500.000 euros. A UNCC possui competências concorrentes com a UIF após a introdução da LOIC (Meireles, 2011 in R. Costa, 2013).

[22] Cfr. n.º 1, do art.º 33.º, do DL n.º 137/2019, de 13 de setembro.

2.4.3. Da Autoridade Tributária

A Autoridade Tributária (AT), constituída pelo DL nº 118/2011 de 15 de dezembro, como parte do Plano de Redução e Melhoria da Administração Central (PREMAC). O objetivo desse plano, de acordo com P. Costa (2014) foi reestruturar a Administração Pública e criar a AT como um serviço da administração direta do Estado, que incorpora a Direção-Geral dos Impostos (DGCI), a Direção-Geral das Alfândegas e dos Impostos Especiais sobre o Consumo (DGAIEC) e a Direção-Geral da Informática e Apoio aos Serviços Tributários e Aduaneiros (DGITA). Essa reorganização centralizou a gestão e reduziu os custos, simplificando a estrutura organizacional.

De acordo com o n.º 1 do artigo 1.º deste DL, a AT tem como atribuições suceder às competências da DGCI, DGAIEC e DGITA. Além disso, a AT é responsável pela investigação de crimes tributários e aduaneiros, através de dois órgãos inseridos na Inspeção Tributária da AT, a Direção de Serviços de Investigação de Fraude e de Ações Especiais (DSIFAE) e a Direção de Serviços Antifraude Aduaneira (DSAFA) (R. Costa, 2013).

A DSAFA, que faz parte da DGAIEC, tem como missão, de acordo com o Artigo 20º, nº 1, da Portaria nº 320-A/2011 de 30 de dezembro, a preparação e desenvolvimento de ações estratégicas de combate à fraude tributária e aduaneira, assegurando a articulação e colaboração com outras entidades com competências inspetivas.

Segundo Seiça (2019) as suas competências incluem, de acordo com as alíneas a), b) e k)[23], a centralização e tratamento integrado de dados aduaneiros e fiscais de natureza estratégica e tático-operacional, bem como a promoção e coordenação dos contatos necessários com entidades competentes no âmbito de assistência mútua.

No que se refere à investigação, de acordo com a alínea j), a DSAFA deve assegurar a execução de diligências no âmbito do artigo 40º e 41º do RGIT (V. Costa, 2022).

Já a DSIFAE, inserida na Inspeção Tributária da AT, tem como missão preparar e desenvolver ações estratégicas de combate à fraude e evasão tributárias, promovendo a cooperação com entidades públicas e privadas e outros serviços com competências inspetivas ou de investigação criminal.

Segundo a Portaria nº320-A/2011 de 30 de dezembro, compete-lhe centralizar e tratar integradamente dados aduaneiros e fiscais de natureza estratégica e tático-operacional, bem como obter provas relativamente a eventuais crimes tributários quando existam indícios do mesmo. Além disso, deve garantir a cooperação com a PJ no acesso e tratamento de

[23] Cfr. o art.º 20.º, n.º 1, da Portaria n.º 320-A/2011, de 30 de dezembro.

informação tributária e aduaneira, cooperar administrativamente e prestar assistência mútua entre os Estados membros da UE e enviar à Comissão Europeia informações que esta solicite (Pereira, 2012).

2.4.4. Dos *Atores* Europeus – Grupo de Ação Financeira Internacional e *Finantial Action Task Force*

Devido à crescente preocupação com o branqueamento de capitais, em 1989, o G-7, reuniu em Paris, e criou o GAFI (Grupo de Ação Financeira Internacional) e a FATF (*Financial Action Task Force)*, que atua como um organismo intergovernamental independente, responsável por desenvolver e promover políticas internacionais para proteger o sistema financeiro global contra o BC/FT e a proliferação de armas de destruição em massa. (Financial Action Task Force - GAFI, 2020) Para alcançar esse objetivo, o GAFI emite recomendações que estabelecem um conjunto de medidas que os países devem implementar para combater o BC e são reconhecidas como o padrão de referência internacional (ibid.), além de serem suficientemente flexíveis e adaptáveis aos sistemas jurídicos dos seus membros (Nunes, 2018).

As recomendações do GAFI, atualmente com quarenta medidas relacionadas ao BC e nove medidas relacionadas ao FT, foram apresentadas pela primeira vez em 1990 e que foram revistas em 1996, 2003 e 2012 (Financial Action Task Force - GAFI, 2020). Elas têm como objetivo combater o uso dos sistemas financeiros para fins de branqueamento de capitais provenientes do tráfico ilícito de drogas (Nunes, 2018). Após a publicação das recomendações, elas são revisadas periodicamente após a conclusão de um ciclo de avaliação da implementação em cada país membro (V. Costa, 2022).

O sistema português já passou por avaliações em 1994, 1999, 2006 e 2017, e foi considerado pelo GAFI como robusto. Como resultado, Portugal está sujeito apenas a um processo de acompanhamento regular, que consiste num monitorização menos intensa aplicada a países com um sistema altamente robusto (Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, 2015).

O FATF (2014) é um organismo intergovernamental independente que desenvolve e promove políticas para proteger o sistema financeiro global contra o branqueamento de capitais, o financiamento do terrorismo e a proliferação de armas de destruição em massa. As recomendações do FATF são reconhecidas como o padrão global de combate a estes ilícitos.

Apesar das diversas preocupações, a FATF mantem-se como uma organização importante neste âmbito e a nível de regulamentação internacional. O branqueamento de capitais, o financiamento ao terrorismo e a corrupção continuam a ser alvo de foco pelas autoridades(Nance, 2018). A FATF, geralmente, é vista como uma organização bem-sucedida, com capacidade adaptativa de forma a ajustar a sua atuação e recomendações as mudanças criminais constantes (Roberge, 2011).

2.5. Dos *Markets in Crypto Assets Regulation* (MiCAR)

Atualmente, a UE está em processo de desenvolvimento de regras que procuram maximizar o potencial das criptomoedas e, ao mesmo tempo, mitigar as ameaças para os intervenientes europeus, por meio da proposta *Markets in Crypto Assets Regulation* (MiCAR). Em março de 2022, foram iniciadas negociações com os países da UE no Conselho Europeu para discutir a versão final do documento conclusivo (Almeida, 2022).

MiCAR tem como objetivo estabelecer regras para a oferta pública de criptoativos, a admissão de criptoativos em plataformas de negociação, a licença de provedores de serviços de criptoativos e a implementação de regras de abuso de mercado para negócios de criptoativos. Existem três categorias principais de *tokens* na proposta do MiCAR sendo eles os *tokens* referenciados a ativos, *tokens* de dinheiro eletrónico e outros criptoativos, cada um com requisitos diferentes em relação à licença e emissão (Kafteranis & Turksen, 2022).

A intenção da regulação, segundo Gortsos (2021) é estimular o desenvolvimento e uso destas tecnologias, ao mesmo tempo em que garante segurança jurídica, fomenta a inovação e protege consumidores e investidores, além de promover a estabilidade financeira. Em geral, o MiCAR concentra-se em aspetos como transparência, divulgação, autorização e supervisão de transações, com o objetivo de supervisionar a emissão de criptomoedas pela Autoridade Europeia dos Valores Mobiliários (*European Securities and Markets Authority*) e pela Autoridade Bancária Europeia (*European Banking Authority*).

Com base nessa regulamentação, as empresas que prestam serviços relacionados a criptomoedas terão que fornecer informações aos clientes sobre os riscos, custos e encargos envolvidos. Além disso, a regulamentação das ofertas públicas de criptomoedas (como ofertas iniciais de aquisição e aumento de capital) tem como objetivo garantir a estabilidade financeira, bem como evitar a manipulação do mercado, lavagem de dinheiro, financiamento do terrorismo e outras atividades criminosas (Guillot, 2022).

Essas regras fazem parte de um pacote mais amplo de medidas relacionadas às "Finanças Digitais" que têm como objetivo apoiar a transição digital da UE, incentivando a

inovação e garantindo a proteção dos usuários. (ibid) Nesse sentido, em março de 2022, o Parlamento aprovou novas regras para apoiar o teste da tecnologia de registo distribuído (um termo amplo que se aproxima de *blockchain*) em infraestruturas de mercado por um período de 3 anos (Parlamento Europeu, 2022).

Em seguida, de acordo com Florysiak (2022) em abril de 2022, o Parlamento concordou em iniciar negociações com os países da UE para estabelecer regras que permitam o rastreio e a identificação de transferências de criptomoedas e dos seus detentores, a fim de evitar o uso dessas moedas para atividades criminosas.

CAPÍTULO 3 – IMPLICAÇÕES DO RECURSO A ATIVOS VIRTUAIS

3.1. Dos Crimes com Recurso a Ativos Virtuais

3.1.1. Do Branqueamento de Capitais

De acordo com o art.º 368º - A do CP, o branqueamento verifica-se quando existe uma conversão, transferência, auxílio ou um facilitar de uma operação de conversão ou transferência de vantagens financeiras obtidas de forma ilícita, com o objetivo de dissimular a sua origem ou evitar que o autor ou participante dessas infrações seja processado criminalmente[24].

Para além de converter, transferir, auxiliar ou facilitar a operação de vantagens financeiras obtidas de forma ilícita, também incorre no mesmo crime quem ocultar ou dissimular a verdadeira natureza, origem, localização, disposição, movimentação ou titularidade dessas vantagens, ou dos direitos a ela relacionados. Isso significa que, além de participar diretamente da operação criminosa, também é considerado crime ocultar ou esconder as informações sobre as vantagens financeiras obtidas ilegalmente. Essa prática é muitas vezes utilizada para dificultar a investigação e a punição dos responsáveis pelo crime original que gerou essas vantagens financeiras[25].

Segundo Teixeira (2022) **"**O conceito de branqueamento não é pacífico na doutrina, tanto a nível nacional como internacional, surgindo várias conceções elaboradas na tentativa de descrever a sua total amplitude."

É correto afirmar que o branqueamento de capitais, também conhecido como lavagem de dinheiro, consiste num conjunto de processos e práticas utilizados para ocultar a origem ilícita de vantagens financeiras provenientes da prática de crimes. Este fenômeno é considerado um dos maiores desafios para a segurança financeira internacional, já que a movimentação de dinheiro sujo pode financiar atividades criminosas e terroristas, além de corromper instituições e afetar a integridade do sistema financeiro global (Martins et al., 2021).

O termo "branqueamento de capitais" tem origem na década de 1920, quando o notório chefe de máfia *Al Capone* usava as suas lavandarias como fachada para ocultar a origem dos seus lucros ilícitos. Desde então que este conceito se expandiu para abranger uma ampla gama de práticas financeiras, incluindo o uso de empresas falsas, transferências

[24] Cfr. n.º 3, do art.º 368.º - A do CP.
[25] Cfr. n.º 4, do art.º 368.º - A do CP.

internacionais de dinheiro, investimentos em setores ilegais, entre outras estratégias (Fontes, 2022).

De facto, durante a "era da proibição" nos Estados Unidos da América, o branqueamento de capitais emergiu como uma prática comum entre organizações criminosas que obtinham lucros com atividades ilegais, como o tráfico de álcool e drogas.

Segundo Fontes (2022) como resultado, o objeto de branqueamento expandiu-se para além dos capitais, incluindo outros ativos financeiros, como imóveis, veículos de luxo e obras de arte. Atualmente, o branqueamento de capitais é um problema global que afeta a segurança e a estabilidade do sistema financeiro internacional, exigindo esforços constantes para combater e prevenir esse tipo de atividade criminosa.

Em suma, a expressão "branqueamento", na ótica de Teixeira (2022) é geralmente utilizada no CP para descrever uma prática criminosa ampla que envolve todas as vantagens além dos capitais, enquanto o termo "branqueamento de capitais" é utilizado para se referir especificamente à ocultação de vantagens financeiras e ao sistema preventivo utilizado pelas instituições que auxiliam na transação de bens monetários.

3.1.2. Dos Crimes Conexos

As infrações tributárias encontram-se previstas no art.º 2.º, n.º 1 do RGIT, deste modo, sendo, todo o facto típico, ilícito, culposo e declarado punível por lei anterior (Azevedo, 2017).

Segundo o n.º 2 do mesmo artigo do RGIT estas infrações podem ser divididas em dois tipos de ilícitos sendo eles o ilícito criminal e o ilícito contraordenacional. Associado ao tipo de ilícito, seja ele criminal ou contraordenacional, as penas ou sanções, respetivamente, são adaptáveis à situação, assim representando penas para os ilícitos criminais a pena de prisão e/ou pena de multa e para os ilícitos contraordenacionais a sanção de coima. A forma de distinguir estes ilícitos está, intimamente, ligada com a gravidade da infração.

De acordo com B. Ferreira (2018), nas infrações que consumarem, simultaneamente, a prática de um crime e de uma contraordenação o agente terá de responder criminalmente perante o seu ato nunca abandonando a possibilidade de lhe serem impostas as consequências (sanção acessória) da prática da contraordenação[26]. Deverá ainda ser punido da forma mais severa respeitando e defendendo, assim, o interesse público.

[26] Cfr. o art.º 2.º, n.º 3, do RGIT.

As obrigações fiscais atribuídas aos contribuintes, quando não são cumpridas, levam à prática de ilícitos fiscais que podem ser consumados de várias formas. Estes ilícitos são condenados através do Direito Fiscal que, com a legislação em vigor, formaliza a criminalização de certos comportamentos que, de certa forma, têm como objetivo lesar as receitas tributárias do Estado (Marques, 2009).

Os ilícitos fiscais, tendo em conta a opinião de Dziura et al. (2020), são compreendidos como um tipo de incumprimento por parte dos contribuintes em relação às suas obrigações do âmbito fiscal, e podem assumir diversas formas. Estas formas podem ser a fraude fiscal, a evasão fiscal e a elisão fiscal, entre outras e, maioritariamente, este tipo de ilícitos está intimamente conectado com a falta de pagamento ou omissão de certos rendimentos, por parte do contribuinte, ao Estado.

Existem duas formas de sanções por parte das autoridades fiscalizadoras, uma está ligada aos comportamentos subsumíveis a situações de evasão fiscal que assumem quatro caminhos distintos sendo eles sanções de natureza preventiva, sanções de natureza reconstitutiva, sanções de natureza compulsória e sanções de natureza compensatória.

Por outro lado, existem ainda as sanções de natureza punitiva que são associadas aos comportamentos culposos e ilícitos por parte dos contribuintes. Estas condutas são decididas tendo em conta a gravidade das infrações cometidas (Campos, 1999).

Tendo em conta a necessidade de definir o comportamento por parte do contribuinte em relação à usurpação de contributos ao Estado existem dois conceitos que são de elevada importância e esclarecimento. Estes conceitos, seguindo a doutrina anglo-saxónica, são a "*tax avoidance*" e a "*tax evasion*" (Azevedo, 2017).

Abordando inicialmente a "*tax avoidance*" pode-se concluir que, tendo em conta a questão temporal, retrata o planeamento fiscal que o contribuinte realiza de forma a conseguir, sem cometer qualquer tipo de ilegalidade, evitar ou diminuir a obrigação fiscal que a sua atividade exija. Deste modo o contribuinte, com o seu comportamento evasivo, não comete nenhum tipo de ilícito por se reger por meios técnicos legalmente admissíveis, sendo que, estes tipos de comportamentos são "permitidos pelo princípio da tipicidade taxativa das normas tributárias" (Marques, 2009, p. 5).

Por outro lado, a expressão "*tax evasion*", remete-nos para o tipo de ilícito que, quando consumado, se retrata, à luz do Direito Fiscal Português, como a evasão fiscal, onde o contribuinte, de forma intencional, tenta enganar, de forma dolosa, o fisco indo contra os preceitos legais.

A fraude fiscal é consumada quando "o contribuinte realiza atos ou negócios jurídicos tendo em vista fugir ao pagamento dos tributos ou a obtenção de proveitos fiscais" usando métodos fraudulentos para o efeito (Marques, 2009, p. 6).

Por outro lado, a evasão fiscal só é retratada após a consumação do facto tributário de forma a obter o não pagamento do imposto devido. Por fim, o crime de fraude fiscal existe quando acontece uma omissão ou ação de forma a tornar mais proveitosa a situação tributária em questão (Campos, 1999).

O conceito de elisão fiscal está, relacionado com a estruturação das atividades exercidas pela pessoa singular ou coletiva e com a tentativa de reger as declarações tributárias pelo mínimo contributo fiscal possível. A elisão fiscal trata-se de um processo lícito de forma a tentar eliminar ou adiar a obrigação contributiva ou reduzir, ao mínimo possível, o montante tributável. Este ato ocorre na precedência do facto gerador de imposto de forma a concretizar esta diminuição do tributo devido (Oliveira, 2009).

Este tipo de atuação tem em vista a escolha do "regime tributário mais vantajoso para as empresas" (Teive & Petri, 2022). Este tipo de atuação pode ser considerado legal tendo em conta as imunidades contributivas, ou lacunas na lei colmatadas com um bom planeamento tributário por parte do agente contributivo (Pellizarri, 1990).

O ponto fulcral que vai diferir e distinguir a elisão da evasão fiscal será o momento temporal do facto gerador de imposto sendo que a elisão ocorrerá quando existe uma preparação prévia da tributação, enquanto que, a evasão ocorrerá após o facto gerador de imposto ser consumado e houver uma tentativa de diminuição de contribuição fiscal (Abrahão, 2011).

As diferenças, de notar, entre a elisão e a evasão fiscal regem-se por dois aspetos, segundo Yamashita (2005, p.28): "critério de licitude ou ilicitude: de acordo com o qual os atos ilícitos se configuram como evasão fiscal, enquanto que os atos lícitos se configuram como elisão" e também o "critério temporal: onde o praticado antes do fato gerador se constituirá em elisão fiscal e, os que ocorrerem após a criação do fato gerador, se constituirá em evasão fiscal."

Por outro lado, Souza (1998) defende que a cronologia será a única forma de distinguir, de forma segura, a fraude da elisão. "Pois, a elisão trata-se de práticas adotadas pelo contribuinte, antes do fato gerador, para evitar, adiar ou diminuir o recolhimento dos tributos, já a fraude fiscal se refere a prática adotada após o respetivo fato gerador" (Teive & Petri, 2022, p.3).

3.2. Da Forma Necessária e Possível de Apreensão de Ativos Virtuais

De acordo com o Relatório Anual da Europol sobre a Situação do Crime Organizado na UE, referente ao ano de 2020, a percentagem de receitas do crime confiscadas ou congeladas e efetivamente recuperadas na UE foi de cerca de 2.2% e 2.4 mil milhões de euros, enquanto a percentagem de receitas do crime recuperadas foi de cerca de 1.1% e 1.1 mil milhões de euros (R. Costa, 2020).

No que diz respeito ao vocabulário utilizado na recuperação de ativos, de acordo com Fraga et al. (2016) o processo começa com a identificação dos bens e a sua localização, que é conhecido como "*identifying*". Em seguida, é realizado o "*tracing*", que consiste em rastrear a origem dos bens e seguir o seu percurso. Depois, é feito o "*freezing*", que envolve o congelamento dos bens, de forma a impedir que sejam movimentados ou utilizados pelo seu proprietário. Posteriormente, é efetuado o "*seizing*", que corresponde à apreensão dos bens por parte das autoridades competentes. Por fim, é realizado o "*confiscating*", que consiste na tomada definitiva dos bens pelas autoridades, após um processo judicial.

A ordem correta dos termos utilizados na recuperação de bens, de acordo com Correia (2015), é *Investigation (Tracing and Identifying)*, *Prosecution (Freezing and Seizing*) e *Enforcement (Confiscating).* A diferença entre "*Freezing*" e "*Seizing*" é que no congelamento (*Freezing*), os bens continuam a ser administrados pela instituição financeira ou outras situações anteriormente ao início de utilização de um mecanismo de congelamento. Ou seja, a instituição financeira ou outra entidade responsável por esses bens é notificada de que os mesmos foram congelados e não podem ser movimentados sem autorização da autoridade competente.

Já na apreensão (*Seizing*), a AJ competente toma posse ou administração dos fundos financeiros ou bens, ou seja, a AJ assume o controle físico desses bens.

O confisco refere-se à privação não efémera de fundos ou ativos por ordem de uma autoridade competente ou tribunal, através de procedimentos judiciais ou administrativos que transferem a propriedade do fundo ou ativo para o Estado. Isso pode ser feito de duas maneiras: confisco com base no valor e confisco com base no objeto.

O confisco com base no valor ocorre quando uma pessoa condenada é ordenada a pagar um valor equivalente ao benefício criminoso obtido. Isso permite a determinação do valor dos proventos e instrumentos do crime, e aplica a confiscação de um valor equivalente. O confisco com base no objeto, por outro lado, é a apreensão da propriedade física

encontrada como produto ou instrumento do crime. Isso significa que o bem em si é apreendido e transferido para o Estado, em vez do seu valor ser determinado e confiscado.

O confisco alargado refere-se aos bens que não estão relacionados com a acusação em julgamento. Neste caso, o confisco é "alargado" a bens que não são instrumentos, frutos diretos ou indiretos do crime em questão. O confisco alargado aplica-se não apenas ao benefício específico do crime pelo qual uma pessoa foi condenada, mas estende-se a todo o benefício recebido por atividade criminal em geral.

O confisco não baseado em condenação não requer a condenação de qualquer pessoa em particular. Numa ação *in-rem* (poder que um tribunal pode exercer sobre a propriedade) que requer prova de que o bem é um instrumento do crime ou provento criminal, mas não requer a comprovação da culpa individual (R. Costa, 2020).

O termo "*cryptocurrency tumbler*" refere-se a um método para garantir o anonimato na utilização de criptomoedas. Após a crise económica de 2008, uma pessoa chamada Satoshi Nakamoto (possivelmente um pseudônimo) desenvolveu a primeira criptomoeda, o *Bitcoin*, bem como o *software* para utilizá-lo. Como resultado da crise, muitas pessoas perderam a confiança no sistema financeiro e nas instituições, e começaram a utilizar criptomoedas como um substituto ao dinheiro tradicional (moedas fiduciárias) (Griffith, 2014).

Todas as transações com criptomoedas são registadas numa base de dados pública chamada *blockchain*. O objetivo principal do *blockchain* é garantir a transparência dessas transações e impedir que sejam alteradas, permitindo a identificação de esquemas de corrupção através de fluxos de financiamento ilegal (Helbig, 2022).

Coelho (2013) refere que, com o avanço das criptomoedas, surgiram serviços e tecnologias anónimas para dissimular proveitos de crimes, tais como o TOR (*Darknet*), *DarkWallet* (*Darknet*), *Bitcoin Laundry (Mixer), Coinjoin* ou *Coinshuffle*. O princípio geral desses instrumentos é criar transações coletivas numa das etapas da transação, eliminando a possibilidade de fixar a transação real entre a moeda e o seu remetente.

O uso de criptomoedas em serviços de anonimato, segundo Nogueira (2020) como o *cryptocurrency tumbler*, permite a realização de atividades ilegais, como o branqueamento de capitais. O objetivo desses serviços é ocultar a cadeia de transações no *blockchain*, dificultando a identificação de remetentes e destinatários das criptomoedas. *Softwares* como *mixers* e serviços como *BitMix, SharedCoin, BitcoinLaundery*, *BitLaunder* e *Easycoin* são exemplos de ferramentas utilizadas para esse fim. No entanto, mesmo com esses serviços, as autoridades podem solicitar registos e mapear transações suspeitas, reduzindo o número

de possíveis suspeitos envolvidos em atividades criminosas. É importante ressalvar que nenhum serviço de anonimato pode garantir uma total ausência de registos e rastreamento.

Torna-se importante destacar que a utilização de criptomoedas para fins ilegais, como o branqueamento de capitais, é uma prática criminosa que deve ser combatida pelas autoridades competentes. Além disso, é importante ressaltar que a tecnologia *blockchain* não é intrinsecamente ligada a atividades ilícitas, sendo utilizada em diversos setores para garantir transparência e segurança em transações financeiras e outras operações (Helbig, 2022).

Ao realizar uma investigação que envolva criptomoedas, é fundamental que as autoridades estejam devidamente capacitadas e atualizadas sobre as estratégias e ferramentas necessárias para rastrear e apreender os ativos financeiros envolvidos.

É importante, por exemplo, considerar a utilização de serviços de *mixers* e outros instrumentos de anonimato de forma a estar preparado para lidar com situações em que a recuperação dos ativos pode ser mais difícil. Por fim, é fundamental que as autoridades trabalhem em conjunto com as comunidades de criptomoedas e com empresas especializadas na área para desenvolver novas ferramentas e estratégias de combate a atividades ilícitas envolvendo criptomoedas. A transparência e a cooperação são fundamentais para garantir que a tecnologia *blockchain* seja utilizada de forma ética e responsável (Pacheco, 2018).

As técnicas utilizadas para análise do *blockchain,* de acordo com Aguiar (2021), incluem a utilização de ferramentas como o *Bitcoin Core*, que é um *software* que permite a análise da cadeia de blocos e a obtenção de informações detalhadas sobre as transações realizadas. É possível analisar as entradas e saídas de cada transação, o montante envolvido, o endereço das carteiras envolvidas e o momento em que a transação foi realizada. Outras ferramentas importantes na análise de transações incluem as *block explorers*, que são sites que permitem a visualização de informações sobre as transações em tempo real, e as ferramentas de análise de gráficos de transações, que permitem a visualização de relações entre diferentes endereços de carteiras e a identificação de padrões de uso.

Além disso, a análise de criptomoedas envolve também a utilização de técnicas de análise de dados, como a análise de redes sociais e a análise de padrões de uso, para identificar possíveis ligações entre diferentes usuários de criptomoedas e entender melhor como essas moedas são utilizadas na economia (Griffith, 2014).

É correto afirmar que o objetivo principal do *blockchain* é garantir a transparência das transações realizadas com criptomoedas e evitar a possibilidade de alteração dessas informações. Além disso, Nogueira (2020) afirma que, o *blockchain* também oferece outras

vantagens, como a descentralização, a segurança e a privacidade dos usuários. O *clustering* é uma técnica utilizada para agrupar endereços de criptomoedas, transações e carteiras virtuais com o objetivo de identificar indivíduos e suas transações financeiras. O *cryptocurrency tumbler* é uma ferramenta utilizada para aumentar o anonimato nas transações com criptomoedas, dificultando a identificação dos usuários envolvidos.

É importante salientar que, de acordo com R. Costa (2020) o uso de tecnologias anónimas como o TOR (*Darknet*), *DarkWallet (Darknet), Bitcoin Laundry (Mixer), Coinjoin*, ou *Coinshuffle* para dissimular a origem de proveitos criminosos configura um crime em si mesmo, conhecido como branqueamento de capitais. Além disso, as autoridades têm trabalhado em medidas para rastrear transações de criptomoedas e identificar possíveis atividades criminosas, como a obrigatoriedade de licenciamento de corretoras de criptomoedas e a implementação de ferramentas de análise de *blockchain* forense. Ainda assim, é importante que as pessoas que operam com criptomoedas estejam cientes dos riscos e se informem sobre as melhores práticas de segurança.

Os *Mixers*, por sua vez, são programas que oferecem anonimato ao obscurecer a cadeia de transações em um *blockchain*, interligando todas as transações na mesma carteira de criptomoedas e enviando-as para parecer que foram enviadas de outra carteira, incluindo transações falsas para dificultar a rastreabilidade da origem, remetente e destinatário. Alguns exemplos de serviços de *mixing* são *BitMix, SharedCoin, BitcoinLaundry, BitLaunder e Easycoin*, sendo o *Bitmix* o mais popular e cobrando comissão de 0,8 a 3%. No entanto, nenhum serviço de anonimato pode garantir a ausência total de registos, podendo ser solicitados pelas autoridades competentes. Além disso, é possível levantar o anonimato mapeando todas as transações com determinados parâmetros registados no *blockchain*, como o número de moedas enviadas pelo criminoso, o que pode ajudar a reduzir o número de suspeitos (Aguiar, 2021).

Para um correto procedimento de apreensão de AV existem algumas sugestões que incluem a criação de uma nova carteira de criptomoedas usando uma carteira HD[27] para armazenar geradores em vez de chaves e o algoritmo de geração. Também é importante documentar cada movimento, usar sistemas ao vivo, usar carteiras com diversas assinaturas,

[27] As Carteiras Hierárquicas Determinísticas (HD), amplamente conhecidas como Carteiras HD, são uma forma de carteira de criptomoedas que utilizam uma única sequência de 12, 18 ou 24 palavras-chave para gerar uma quantidade ilimitada de endereços. Esse processo ocorre de forma automática, hierárquica e sequencial. Para facilitar esse processo, são utilizados códigos mnemônicos, que transformam a sequência em palavras compreensíveis para nós. Dessa forma, realizar o backup da sequência torna-se mais simples e prático.

testar transferências de entrada e saída, e imprimir/salvar/armazenar as chaves em algum lugar e depois destruir as cópias locais (Checco & Rossetti, 2020).

Para mover as criptomoedas para o novo endereço, é recomendado, por Checco & Rossetti (2020), que o suspeito faça a transferência sob observação, para minimizar o risco de roubo ou transferência remota. Também é possível criar transações numa máquina e transmiti-las noutra, ou preparar a transação *offline*. É importante verificar a transação descodificando a sua versão em bruto e ter o suspeito a assinar a transação antes de a transmitir.

Algumas das escolhas de criptomoedas e requisitos mencionados incluem o uso de *Trezor, Ledger*, ou *OpenDime* como opções de armazenamento seguro de criptomoedas. Também é importante considerar onde armazenar as 24 palavras mnemônicas, se houver uma chave/frase de *backup*, e o que acontece se o *hardware* for destruído. A ideia de dividir o valor em quantias menores e muitas chaves também pode ser uma boa opção. Além disso, é importante considerar se a carteira ou VASP é fidedigna e o que acontece se for *hackeada* ou fechada. E, finalmente, é preciso lembrar que, se as chaves privadas puderem ser exportadas, o problema de "quem guarda/vê as chaves privadas" ainda é um risco a considerar (B. Ferreira, 2018).

PARTE II – ENQUADRAMENTO METODOLÓGICO E TRABALHO DE CAMPO

CAPÍTULO 4 – METODOLOGIA, MÉTODOS E MATERIAIS

4.1. Da Metodologia e Procedimentos

Este Trabalho de Investigação Aplicada (TIA) tem como finalidade a "especialização, de natureza académica, com recurso à atividade de investigação, de inovação ou de aprofundamento de competências profissionais"[28], para obtenção do grau de mestre nos ciclos de estudos integrados da Academia Militar mais concretamente no mestrado integrado em Ciências Militares na especialidade de Segurança (Academia Militar, 2015).

A metodologia torna-se, no âmbito dos trabalhos de investigação, um dos fatores cruciais para alcançar objetivos propostos e conclusão destes mesmos trabalhos do foro académico, sendo o método científico um meio para atingir um fim, com o propósito de produzir conhecimento através de certos procedimentos (Sarmento, 2013a).

A metodologia envolve a observação, a formulação de hipóteses, a realização de trabalho de campo e investigação e a análise dos resultados, com o objetivo de obter um conhecimento válido e confiável sobre o objeto de estudo (Freixo, 2012).

A metodologia científica é composta por diversas etapas, como a definição do problema, a revisão bibliográfica, a formulação de hipóteses, a recolha e análise de dados, a interpretação dos resultados e a elaboração das conclusões. Cada uma dessas etapas deve ser realizada com rigor e precisão, seguindo as normas e procedimentos estabelecidos pela comunidade científica (Normas *American Psychological Association* (APA)) (Fortin, 2009).

Além disso, é importante destacar que a metodologia, por si só, não é um fim, mas sim um meio para se atingir os objetivos da investigação. Por isso, é necessário selecionar a metodologia mais adequada ao objeto de estudo e aos objetivos da pesquisa, tendo em consideração fatores como a disponibilidade de recursos, o tempo disponível e as habilidades do investigador (Sarmento, 2013b).

[28] Cfr. o art.º 20.º, do DL n.º 115/2013, de 7 de agosto.

Torna-se importante referir que este trabalho terá uma abordagem ontológica, com um raciocínio indutivo, uma estratégia qualitativa e com um horizonte temporal transversal (Quivy & Campenhoudt, 2013).

Através da análise da literatura, foi formulada a seguinte **Questão Central (QC)**: **"Quais as principais implicações no recurso a Ativos Virtuais e possíveis formas de atuação no âmbito da missão da investigação tributária da GNR?"**

Para a elaboração do trabalho recorreu-se às normas para a redação de trabalhos de investigação da Academia Militar[29] e às normas APA[30], 7.ª edição.

Em segundo lugar, neste trabalho, ocorreu a construção que levou à elaboração de um modelo de análise (ver **Apêndice I**), que tem como objetivo explicar os conceitos deste TIA interligados entre si (Quivy & Campenhoudt, 2013).

Para alcançar uma resposta fundamentada à QC e alcançar os objetivos específicos deste trabalho, foram elaboradas algumas Questões Derivadas (QD):

QD$_1$: Quais as vantagens e desvantagens do sistema financeiro descentralizado?

QD$_2$: Quais são as principais formas de controlo no recurso a estes ativos?

QD$_3$: Quais são as principais dificuldades que a GNR vai encontrar tendo em conta esta nova problemática?

QD$_4$: Quais as alterações legislativas necessárias para a prevenção da consumação de ilícitos criminais recorrendo a ativos virtuais?

QD$_5$: Quais as formas necessárias e possíveis para a apreensão destes ativos?

Após a finalização da etapa da construção do modelo de análise, surge a verificação/experimentação, que culmina e versa sobre o trabalho de campo e as conclusões do presente trabalho.

4.2. Do Método de Abordagem da Investigação

Sarmento (2013, p. 7) refere que "numa investigação pode ser utilizado mais do que um método para que sejam encontradas as respostas para a (…) investigação".

Para a elaboração deste trabalho de pesquisa, foram empregues dois métodos de investigação científica. Numa fase inicial, foi utilizado o método histórico, o qual envolveu

[29] NEP n.º 522/ 1.ª, de 20 de janeiro de 2016 – Direção de Ensino da Academia Militar.
[30] *American Psychological Association*.

a análise documental e a revisão da literatura relacionada às fontes primárias, secundárias e bibliográficas produzidas pelo investigador (Sarmento, 2013b).

Em seguida, foi adotado o método inquisitivo, tornando-se uma fase crucial da investigação que adotou uma abordagem qualitativa por meio da realização de entrevistas. Este método é baseado em estratégias de pesquisa para observar e descrever comportamentos, com o objetivo de fornecer uma caracterização precisa das variáveis envolvidas (Freixo, 2012).

4.3. Da Técnica de Recolha de Dados

A recolha de dados é crucial para a elaboração de uma abordagem conceitual na pesquisa. É um processo organizado que tem como objetivo obter informações relevantes e, desta forma, a escolha dos métodos de coleta de dados é determinada pela natureza do problema de pesquisa. Em outras palavras, é importante selecionar os métodos mais adequados para garantir informações precisas e fidedignas (Fortin, 2009).

Para realizar a recolha de dados e informações, foram pesquisadas fontes primárias, incluindo relatórios de instituições e jurisprudência no âmbito dos AV. Além disso, foram utilizadas fontes secundárias, como obras de outros autores relevantes para este trabalho de investigação e análise documental de fontes bibliográficas, com o objetivo de complementar a pesquisa (Mota, 2021).

Na realização do planeamento do trabalho de campo, com o objetivo de realizar uma observação indireta, foi elaborada uma Carta de Apresentação juntamente com um Guião de Entrevista[31] (Quivy & Campenhoudt, 2013).

Para abordar certas temáticas, o trabalho de campo mais aconselhável, é a realização de entrevistas com vista à aquisição de dados de forma a permitir informações de fonte segura e elementos de reflexão.

Este tipo de trabalho de campo, na ótica de Quivy & Campenhoudt (2013) tem uma abordagem qualitativa devido ao facto das entrevistas serem de conteúdo subjetivo e baseadas num conjunto de questões diretivas. Este tipo de entrevistas tem como principal objetivo permitir ao entrevistado que se expresse de forma aberta tentando não o limitar a, apenas, um caminho de resposta sempre de forma orientada para os objetivos definidos.

[31] Ver Apêndice B referente ao Guião de Entrevista.

4.4. Do Tratamento de Dados

Depois de recolher os dados necessários, foi realizada uma análise qualitativa do conteúdo, seguindo as técnicas propostas por Bardin (1977). Essa análise procura obter conhecimento para solucionar uma problemática específica, interpretando o conteúdo das mensagens num determinado contexto.

Para realizar a análise mencionada, foram criadas tabelas de análise de conteúdo, com o propósito de facilitar a perceção e o cruzamento das respostas das diversas entidades entrevistadas e conduzir esta investigação até ás respostas às questões propostas inicialmente.

4.5. Da Amostragem - Entrevistados

Relativamente à amostragem, pode-se dizer que esta é, totalmente, de conveniência por se tratarem de entidades que lidam com a temática diretamente afim de dirimir certas questões no âmbito da pesquisa e investigação realizada neste trabalho.

Tendo em conta Sarmento, para a escolha do tipo de amostragem existe todo um procedimento de recolha de dados com vista a assegurar a fiabilidade e a necessidade destes mesmos dados para o beneficio do trabalho. Torna-se importante, também, que a comparação destes resultados seja sólida para que existam conclusões retiradas do trabalho de campo.

Após a investigação inicial e traçados os objetivos da investigação foram reunidas diversas entidades que, potencialmente, teriam importância no desenvolvimento deste trabalho. Esta amostragem tem como principal objetivo representar as entidades com o maior contacto com a temática abordada, os AV.

Assim, com o intuito de recolher informações, surgiu a necessidade de realizar entrevistas dirigidas aos elementos dos vários organismos competentes que têm conhecimento sobre a matéria suprarreferida, nomeadamente a PJ, o Departamento Central de Investigação e Ação Penal (DCIAP), a PGR, a GNR e o *European Financial and Economic Crime Centre* (EFECC).

Quadro 1 – Caracterização dos Entrevistados

N.º	Organização	Função	Modo
E1	GNR	Diretor de Investigação Criminal do CO	Online (Escrito)
E2	GNR	Chefe da SIC-UAF	
E3	PGR	Diretor do Gabinete Cibercrime da Procuradoria-Geral da República	
E4	DCIAP	Procurador da República, coordenador da SIATID - DCIAP	
E5	PJ	Chefe da Secção de Informação da UIF	
E6	PJ	Coordenador da PJ - UNCC	Online (Escrito)
E7	PJ	Responsável pela Secção de Investigação da Criminalidade Informática contra o Património e Vida em Sociedade	
E8	EFECC	*Head of Unit - European Financial and Economic Crime Centre (EFECC) Operations*	

Fonte: Elaboração própria

CAPÍTULO 5 – APRESENTAÇÃO DE RESULTADOS

5.1. Do Método de Análise de Conteúdo das Entrevistas

Com o objetivo de recolher informações necessárias para a continuação da pesquisa, foi elaborado um guião de entrevista que foi aplicado posteriormente aos entrevistados. As perguntas que compuseram este guião foram direcionadas para encontrar respostas às QD e obter os seguintes dados[32]:

Seguindo o raciocínio suprarreferido, a **QD_1** enquadra a pergunta 3 do guião de entrevista *"Quais as vantagens e desvantagens, do ponto de vista da (Entidade), inerentes à utilização destes ativos?"* com o objetivo de perceber qual a perspetiva de cada uma das entidades entrevistadas em relação à utilização dos AV tendo em conta as suas vantagens e desvantagens.

Recorrendo à **QD_2** tem como a sua exposição, no guião de entrevista, a pergunta 4 *"Na ótica da (Entidade), quais são as alterações legislativas necessárias para que os ilícitos económico-financeiros, com recurso a Ativos Virtuais, sejam minimizados?"* que tem por objetivo principal encontrar as principais lacunas legislativas relativamente à temática em apreço.

Já na **QD_3** foram elaboradas duas perguntas no guião de entrevistas sendo elas a pergunta 7, *"Principais dificuldades na atuação da (Entidade) no âmbito do combate à criminalidade económico-financeira com recurso a Ativos Virtuais?"*, que procura perceber as dificuldades de atuação dos diversos *atores* no combate à criminalidade económico-financeira e a pergunta 8, *"Medidas a adotar pela (Entidade), enquanto FFSS, no âmbito do combate à criminalidade económico-financeira com recurso a Ativos Virtuais?"*, com o objetivo de perceber quais as medidas futuras a adotar pelos *atores* no combate à criminalidade económico-financeira.

Na **QD_4** surgem mais duas perguntas no guião de entrevista sendo a pergunta 1, *"Tendo em conta o recurso a Ativos Virtuais, qual é o panorama nacional ao nível da criminalidade económico-financeira?",* uma tentativa de entender o estado da criminalidade económico-financeira com relação ao recurso de AV e a pergunta 2, *"Qual é a principal criminalidade associada aos Ativos Virtuais?",* associar, a este tipo de ilícitos, um tipo de criminalidade mais comum.

[32] Ver Apêndice D.

Por fim, na **QD5**, estão associadas, no guião de entrevista, a questão 5, *"Qual o procedimento de apreensão de Ativos Virtuais utilizado na (Entidade)?"* e a questão 6, *"Quais as principais barreiras à apreensão de Ativos Virtuais?"*, com o intuito de perceber as principais dificuldades inerentes à apreensão deste tipo de ativos e os procedimentos adotados pelas entidades entrevistadas.

5.2. Da Apresentação, Análise e Discussão dos Resultados da Pergunta n.º 1

Tendo em conta a pergunta n.º 1 do Guião de Entrevista, "*Tendo em conta o recurso a Ativos Virtuais, qual é o panorama nacional ao nível da criminalidade económico-financeira?",* sabemos que a utilização de AV está em constante desenvolvimento e que o panorama deste tipo de ativos vai estar sempre em constante evolução, então, o panorama nacional acaba por não se conseguir definir concretamente.

Aquilo que se perspetivava como um nicho de cibercriminalidade passou, aos dias de hoje, a ser, de forma recorrente, uma fonte de branqueamento de capitais numa perspetiva de crime organizado. Estas mudanças levam a uma necessidade de adaptação constante dos OPC e das instituições que regulam este tipo de mercados pois existe uma grande procura, por parte dos *atores* do diverso crime organizado, de profissionais e especialistas na área do DeFi por saberem das dificuldades inerentes aos serviços de investigação. (E8)

De acordo com o E3, com a crescente evolução da utilização dos AV, existem dois tipos de modalidades no que concerne à criminalidade com recurso a estes ativos, sendo elas, a utilização dos AV como objeto de crime e como instrumento de crime.

Quando se trata de objeto de crime, os AV são, muitas vezes visados como alvo de furtos com recurso a ataques informáticos nas plataformas digitais. Por outro lado, existem também, diversos tipos de burlas através de plataformas fraudulentas de investimentos neste tipo de ativos.

Relativamente ao instrumento do crime, os AV servem como forma de pagamento ou moeda de troca para a consumação de ilícitos criminais. Como exemplo temos os casos de ataques informáticos (e.g. *ransomware*) em que são pedidas grandes quantias de AV como forma de resgate.

Nas duas situações existe a exploração do anonimato garantido através dos sistemas DeFi e do desconhecimento comum dos cidadãos em relação este tipo de tecnologias.

Em suma, e tendo em conta o E4, apesar deste ser um "mundo" desconhecido pela maioria da população em geral, já existem alguns tipo de contratos celebrados com recurso a moedas virtuais, como por exemplo, escrituras de habitações. No que concerne a outros

tipos de AV podemos concluir que não existe um mercado desenvolvido apesar de já terem sido detetadas algumas transações com recurso a estes ativos, ao nível da investigação, os OPC não se encontram preparados para as investigar.

5.3. Da Apresentação, Análise e Discussão dos Resultados da Pergunta n.º 2

Relativamente à pergunta n.º 2 do Guião de Entrevista, "*Qual é a principal criminalidade associada aos Ativos Virtuais?",* importa referir que, de acordo com o E1 e recorrendo à área digital forense da GNR, não há criminalidade identificada e associada aos AV, existindo apenas, várias carteiras de ativos identificadas como propriedade de diversos intervenientes em processos crime, não significando estas que sejam detidas de forma criminosa.

Segundo o E2, o crime de fraude fiscal é considerado um ilícito elencado no catálogo de crimes associados à Lei do branqueamento, e representa uma fatia significativa das infrações subjacentes ao branqueamento de capitais em comparação com outras tipologias criminais. Embora não haja conhecimento de um estudo específico sobre esse assunto, acredita-se que o uso de AV é comum em toda a criminalidade organizada, especialmente na área da criminalidade económico-financeira e tributária.

De facto e de acordo com o E3, os crimes que envolvem tecnologias, a utilização de redes de comunicação e ambientes virtuais são, naturalmente, mais propensos ao uso de AV. Além da cibercriminalidade, os AV também são utilizados em muitas vendas fraudulentas na internet, bem como em mercados da *Darkweb*, como a venda de drogas, armas, pornografia infantil e documentos falsos, entre outros.

Além disso e tendo em conta o E4, é comum o uso de AV como um dos modos de ocultação de proveitos de atividades ilícitas para a realização de lavagem de dinheiro e branqueamento do dinheiro obtido de forma ilícita. Esses ativos também são utilizados no comércio de mercadorias proibidas, devido às suas características de anonimato e à falta de regulação em nível global.

Durante o período da pandemia, houve um aumento das fraudes relacionadas com criptomoedas, *forex* e outros AV sendo que os *atores* das fraudes, têm por hábito atrair as suas vítimas com esquemas de pirâmide, convidando-as a pagar mensalidades que podem chegar a centenas de euros para abrir uma conta de cliente. Em troca, prometem recompensas com diversos tipos de bônus à medida que as aplicações financeiras geram retorno.

Atualmente, o crime de fraude é um dos mais comuns na UE, tanto do ponto de vista do bem oferecido que, acaba por não existir, em fraudes de investimento quanto da conversão dos lucros do crime e o processo de branqueamento. Isso significa que o uso de AV se tornou comum na criminalidade económico-financeira. Além disso, há também a utilização frequente destes ativos para repatriar valores por parte de alguns dos maiores cartéis de tráfico internacional de cocaína, bem como a sua utilização massiva na cibercriminalidade.

5.4. Da Apresentação, Análise e Discussão dos Resultados da Pergunta n.º 3

No que concerne à pergunta n.º 3 do Guião de Entrevista, "*Quais as vantagens e desvantagens, do ponto de vista da (Entidade), inerentes à utilização destes ativos?",* chegamos à conclusão que do ponto de vista da entidade não existem grandes benefícios ou malefícios no âmbito do recurso a estes ativos. Por outro lado, do ponto de vista criminal e da investigação de ilícitos, existem algumas considerações a realizar.

De acordo com o E8 as vantagens do uso de AV para a criminalidade incluem a facilidade de acesso e conversão de valores, bem como o transporte e remessa desses valores de forma discreta. Além disso, é difícil para as autoridades policiais e judiciais detetar e identificar o uso desses ativos e apreendê-los. No entanto, as desvantagens incluem a alta volatilidade dos valores, representando um risco para os criminosos que mantêm esses ativos em sua posse por algum tempo. Além disso, o uso desses ativos requer habilidades técnicas e informáticas avançadas, e há um risco elevado de que eles sejam furtados por meio de ataques informáticos.

No entanto, segundo os E1, E2, E3, E4 e E5 é importante salientar que o anonimato e a falta de regulamentação dos AV podem tornar mais difícil a deteção e a investigação de crimes cometidos com o seu uso, o que pode facilitar a consumação de ilícitos. Além disso, a falta de compreensão sobre o funcionamento desses ativos pode ser uma barreira para a investigação criminal, tornando este processo mais complexo.

Apesar do suprarreferido, o uso de AV pode ter algumas vantagens do ponto de vista da investigação criminal. Embora os AV sejam utilizados de forma anonimizada, eles deixam um rasto indelével na cadeia *blockchain*, o que pode ser muito útil para a investigação criminal. Com o uso de tecnologia apropriada, é possível seguir e identificar as transações que ocorreram.

O E4 refere que, embora a tecnologia *blockchain* permita a criação de um registo público de todas as transações realizadas com AV, isso não significa necessariamente que as

operações sejam transparentes ou que a identidade dos operadores seja facilmente identificável. Na verdade, é possível utilizar técnicas de anonimização, como a mistura de moedas (também conhecida como "*coin mixing*") ou o uso de carteiras temporárias, para ocultar a origem e o destino dos criptoativos envolvidos nas transações. Além disso, existem VASP e serviços que operam de forma anônima, dificultando ainda mais a identificação dos responsáveis por determinadas transações. Por isso, embora a tecnologia *blockchain* ofereça certas garantias de segurança e integridade, acaba por não ser uma solução infalível para evitar atividades ilegais com recurso a AV.

No entanto, é importante ressaltar que, embora a tecnologia exista e esteja disponível, nem sempre é fácil para os OPC utilizarem-na de forma eficaz.

Portanto, embora a tecnologia da *blockchain* possa ser uma ferramenta útil na investigação de crimes relacionados com AV, é importante que as autoridades policiais e investigadores estejam devidamente capacitados e equipados para utilizá-la de forma eficaz.

5.5. Da Apresentação, Análise e Discussão dos Resultados da Pergunta n.º 4

Tendo em conta a pergunta n.º 4 do Guião de Entrevista, "*Na ótica da (Entidade), quais são as alterações legislativas necessárias para que os ilícitos económico-financeiros, com recurso a Ativos Virtuais, sejam minimizados?",* de acordo com o E3 é correto afirmar que a regulamentação dos AV é importante para a sua utilização na vida económica normal. No entanto, no que diz respeito ao direito penal e processual penal, é importante que os OPC tenham um conhecimento mais aprofundado dessa realidade para entender e combater melhor os crimes relacionados a este fenómeno.

Por outro lado, os E1, E2, E3, E4 e E5 afirmam que, a ilegalização de mecanismos que permitem a opacidade das operações pode ser uma forma de dificultar a prática de atividades criminosas com criptoativos, e a fiscalização policial e das autoridades de supervisão pode ajudar a detetar e prevenir atividades ilícitas. O E4 refere, ainda, que o aumento do papel do Banco de Portugal e da Comissão do Mercado de Valores Mobiliários na regulação dos criptoativos pode também ser uma forma de garantir uma maior transparência e segurança nestes mercados em Portugal. No entanto, é importante lembrar que qualquer regulação deve ser equilibrada e proporcional, de forma a evitar o sufocamento da inovação e da economia digital.

Por outro lado, E5 defende que, a colaboração entre as entidades que negoceiam AV e as autoridades é fundamental para evitar a utilização destes ativos para fins criminosos. A

regulação internacional poderia ajudar a uniformizar os procedimentos e a criar um quadro regulatório mais eficaz para combater a utilização dos AV em atividades ilegais.

5.6. Da Apresentação, Análise e Discussão dos Resultados da Pergunta n.º 5

Analisando a pergunta n.º 5 do Guião de Entrevista, "*Qual o procedimento de apreensão de Ativos Virtuais utilizado na (Entidade)?",* e de acordo com o E2, E3, E4 e E5, antes de discutir um eventual procedimento de apreensão de AV, é importante destacar que este assunto ainda não possui um conhecimento consolidado devido à falta de situações operacionais. Portanto, até ao momento, não foram emitidas orientações específicas pelo Comando da Guarda em relação aos procedimentos de apreensão destes ativos. No entanto, os procedimentos para qualquer outro ativo são seguidos e estão em conformidade com as diretrizes do MP, que podem envolver o Gabinete de Administração de Bens (GAB) e a Caixa Geral de Depósitos (CGD).

Na ótica do E1, existe um enquadramento legal para proceder à apreensão de ativos, incluindo ativos digitais, e aplicar medidas necessárias para garantir a sua custódia durante o processo criminal. É importante preservar a integridade desses ativos, removendo qualquer forma de acesso externo à carteira que contém os ativos. Da mesma forma que na preservação de provas tradicionais, é fundamental respeitar a Cadeia de Custódia da Prova Digital para validar e sustentar a prova.

Do ponto de vista legal, os criptoativos não são atualmente considerados como uma moeda, portanto, as regras aplicáveis à apreensão de dinheiro em espécie ou em contas bancárias não se aplicam a eles. Como os criptoativos têm um valor econômico geralmente significativo, devem ser entregues numa conta cripto do GAB e, posteriormente, convertida em euros e conservada na CGD seguindo os procedimentos normais para evitar a depreciação. No entanto, surge um problema quando não se tem acesso à chave criptográfica e, por isso, não é possível seguir o procedimento mencionado. Nesse caso, mesmo que seja possível determinar a apreensão formalmente, não é possível realizá-la materialmente. (E3 e E4)

Com base na informação disponível, o E5 afirma que, sem a chave da carteira correspondente, é impossível, obter o acesso à mesma, o que impede uma apreensão efetiva. A chave de acesso pode ser obtida por meio da colaboração dos arguidos ou suspeitos, ou pode ser resultado da investigação, incluindo buscas ou exames, tanto físicos quanto digitais.

5.7. Da Apresentação, Análise e Discussão dos Resultados da Pergunta n.º 6

Relativamente à pergunta n.º 6 do Guião de Entrevista, "*Quais as principais barreiras à apreensão de Ativos Virtuais?",* as respostas dos entrevistados tinham todas a mesma direção. Deste modo as maiores conclusões retiradas desta questão da entrevista são que a falta de formação dos OPC e de enquadramento legal deixa a tarefa da apreensão menos concretizável. (E1 e E2)

Numa fase mais avançada da apreensão, de acordo com o E3, quando se apreende um dispositivo, nem sempre é fácil identificar uma carteira de AV que esteja localmente armazenada. Em relação às carteiras que estejam depositadas em entidades gestoras de AV na internet, a grande dificuldade está na sua deslocalização, uma vez que a maioria dessas entidades tem sede fora de Portugal, algumas delas em locais não determinados ou conhecidos.

Em forma de resumo, de facto existem diversas barreiras técnicas, legais e de conhecimento que dificultam a apreensão de AV. A falta de identificação das carteiras de AV em dispositivos apreendidos e a necessidade de senha para acessá-las é um dos principais obstáculos técnicos. Além disso, a localização de entidades gestoras de AV fora do país e em locais pouco cooperativos também dificulta a obtenção de ordens de apreensão. E mesmo com a apreensão de dispositivos, documentos ou senhas, ainda há o risco dos AV serem dissipados rapidamente a partir de outros terminais ligados à internet, o que torna a apreensão uma operação complexa e taticamente desafiadora. (E8)

5.8. Da Apresentação, Análise e Discussão dos Resultados da Pergunta n.º 7

No que concerne à pergunta n.º 7 do Guião de Entrevista, "*Principais dificuldades na atuação da (Entidade) no âmbito do combate à criminalidade económico-financeira com recurso a Ativos Virtuais?",* é, mais uma vez salientado pelo E1 que, a falta de tecnologia e formação especifica nesta área é a principal dificuldade encontrada no combate a este tipo de criminalidade.

Segundo os E2, E4, E5 e E8 a falta de credenciais ou a recusa do arguido em entregá-las pode ser uma grande dificuldade na apreensão de AV. Nesse caso, as autoridades podem tentar obter acesso às credenciais por meio de mecanismos legais, como mandados de busca e apreensão, ou podem depender da cooperação dos suspeitos.

Em relação às atividades ilícitas de *blockchain,* como *ransomware* e golpes de criptomoedas, é verdade que os criminosos usam técnicas inovadoras para ocultar a sua

atividade, como o uso de *mixers*. Isso torna mais difícil para as autoridades rastrear o dinheiro e identificar os responsáveis por essas atividades criminosas.

As investigações que envolvem o rastreamento de fundos de AV que, geralmente, exigem o uso de ferramentas especializadas, como o *Chainalysis*, que ajudam a identificar a origem e o destino dos fundos em várias cadeias de blocos. Sem essas ferramentas, a investigação pode ser mais lenta e os resultados podem ser de baixa qualidade. No entanto, é possível realizar investigações manuais, embora isso exija mais tempo e recursos.

5.9. Da Apresentação, Análise e Discussão dos Resultados da Pergunta n.º 8

Por último, a pergunta n.º 8 do Guião de Entrevista, "*Medidas a adotar pela (Entidade), enquanto FFSS, no âmbito do combate à criminalidade económico-financeira com recurso a Ativos Virtuais?",* vão muito de encontro às respostas dadas nas duas questões anteriores onde as maiores lacunas detetadas são a falta de pessoal devidamente especializado, a falta de material (*hardware e software*) evoluído tecnologicamente de forma a trabalhar nesta área e a falta de legislação reguladora do uso de AV.

De acordo com o E6 o investimento na prevenção e na investigação é fundamental, e é importante dar continuidade ao trabalho realizado pelas UIF no que diz respeito à recolha, centralização, tratamento, análise e partilha de informações. Também é essencial aderir às recomendações do GAFI e utilizá-las como orientação para eventuais alterações legislativas. É necessário continuar a formar e constituir equipas especializadas com experiência no tratamento de questões relacionadas à investigação de crimes económico-financeiros que envolvam AV. Esta tipologia de ilícitos tem uma investigação que requer uma abordagem divergente da investigação criminal tradicional.

CONCLUSÕES

Chegando ao fim desta investigação, tendo-se realizado um enquadramento teórico na primeira parte deste TIA e numa segunda fase um enquadramento metodológico e trabalho de campo com, mais concretamente, oito entrevistas a diversas entidades e analisando as suas respostas de forma a conectar com os dados recolhidos nos primeiros três capítulos deste TIA, compete-nos responder às QD propostas no início desta investigação.

A investigação na área dos AV é uma temática cada vez mais relevante e complexa, uma vez que se trata de um campo emergente e em constante evolução. Neste contexto, é fundamental compreender as implicações do recurso a AV e as suas implicações no sistema financeiro e económico.

Relativamente à **QD$_1$:** "**Quais as vantagens e desvantagens do sistema financeiro descentralizado?"**, uma das questões mais importantes a ser abordada é a comparação entre sistemas financeiros centralizados e descentralizados (CeFi vs. DeFi) e as vantagens e desvantagens do recurso a AV. A descentralização do sistema financeiro permite maior liberdade e autonomia aos utilizadores, bem como maior transparência e segurança no processo de transações financeiras. No entanto, o recurso a estes ativos também apresenta algumas desvantagens, como a falta de regulamentação e supervisão adequadas, o que pode levar à realização de atividades criminosas.

A utilização de AV apresenta vantagens e desvantagens, mas é inegável o seu impacto na economia e no sistema financeiro. É fundamental que haja uma supervisão e regulação adequadas para prevenir e combater atividades criminosas relacionadas com o recurso a AV. A GNR deverá estar preparada para enfrentar novos desafios e dificuldades nesta área e é essencial que sejam identificadas as alterações legislativas necessárias para a prevenção da consumação de ilícitos criminais. Por fim, é importante desenvolver procedimentos eficazes para a apreensão de AV em caso de práticas ilícitas. A investigação económico-financeira na área dos AV é um tema cada vez mais relevante e deve continuar a ser alvo de estudo e investigação.

Tendo em conta a **QD$_2$: Quais são as principais formas de controlo no recurso a estes ativos?,** a regulação e o controlo são as principais formas de combater a criminalidade económico-financeira relacionada com o uso de AV. É fundamental que existam mecanismos de supervisão e controlo que permitam identificar e prevenir atividades ilícitas relacionadas com o recurso a estes ativos, como o branqueamento de capitais e outras práticas criminosas.

Outra forma de controlo é a utilização de tecnologia para rastrear e monitorizar transações suspeitas. A tecnologia *blockchain*, utilizada na maioria das criptomoedas, permite que as transações sejam registadas de forma permanente e imutável, permitindo assim uma maior transparência no mercado de AV.

Deste modo, é importante a cooperação internacional no combate aos crimes financeiros relacionados com AV. As autoridades e entidades reguladoras de vários países devem trabalhar em conjunto para partilhar informações e implementar medidas de controlo eficazes.

No âmbito da missão da investigação criminal da GNR, é importante que esta tenha capacidade para identificar transações suspeitas de AV e que seja capaz de trabalhar em conjunto com outras entidades nacionais e internacionais para implementar medidas de controlo eficazes.

No que concerne à **QD$_3$: Quais são as principais dificuldades que a GNR vai encontrar tendo em conta esta nova problemática?,** a GNR, como força policial encarregue de investigar e prevenir crimes económico-financeiros, enfrenta várias dificuldades no combate ao uso ilegal de AV. Uma das principais dificuldades é a falta de regulamentação e supervisão adequada das transações em AV. Isso dificulta a identificação e investigação de transações fraudulentas ou ilegais.

Além disso, os AV têm a capacidade de transpor fronteiras e serem transferidos de forma anónima e instantânea, tornando difícil a identificação de suspeitos e o rastreamento do dinheiro. O anonimato é uma característica-chave das criptomoedas e das transações de AV, o que dificulta ainda mais o trabalho de investigação da GNR.

Outra dificuldade é a falta de formação e de recursos técnicos e humanos para lidar com essa nova problemática. A investigação de crimes que envolvem AV requer conhecimentos especializados e tecnologias avançadas.

A natureza descentralizada dos sistemas financeiros baseados em AV e a falta de uma entidade central reguladora e fiscalizadora torna ainda mais difícil o controlo e a prevenção de crimes que envolvem esses ativos. Essa falta de regulamentação e supervisão adequada aumenta a probabilidade de ocorrência de crimes económico-financeiros que envolvem AV.

No que refere à **QD$_4$: Quais as alterações legislativas necessárias para a prevenção da consumação de ilícitos criminais recorrendo a ativos virtuais?,** a prevenção de ilícitos criminais recorrendo a AV requer uma abordagem legislativa adequada e atualizada. Atualmente, a regulamentação desses ativos é complexa e fragmentada, o que torna difícil a sua aplicação em diferentes jurisdições.

A nível internacional, organizações como o GAFI e o FATF têm sido ativos na criação de normativos e orientações para o uso seguro e legal de AV. Essas diretrizes visam combater o branqueamento de capitais, o financiamento do terrorismo e outras atividades ilegais que possam ocorrer.

No âmbito nacional, os Estados devem criar uma legislação clara e abrangente sobre AV que inclua a definição de responsabilidades e penalidades adequadas para as violações. É necessário que as autoridades fiscais sejam capazes de rastrear a origem dos AV e identificar as pessoas envolvidas em transações ilícitas.

Também é importante criar mecanismos de cooperação internacional para garantir que as atividades ilícitas não sejam transferidas de um país para outro. Isso exigirá a coordenação de reguladores e autoridades fiscais em todo o mundo, a fim de criar uma abordagem global uniforme para a regulamentação de AV.

Em resumo, as alterações legislativas necessárias para a prevenção da consumação de ilícitos criminais recorrendo a AV incluem a criação de normativos claros e abrangentes que definam responsabilidades e penalidades adequadas para as violações, bem como a coordenação de esforços entre reguladores e autoridades fiscais em todo o mundo para criar uma abordagem uniforme para a regulamentação destes ativos.

Por último a **QD_5: Quais as formas necessárias e possíveis para a apreensão destes ativos?,** leva à conclusão que, a apreensão de AV pode ser um desafio para as autoridades, já que muitas das vezes são mantidos em carteiras virtuais criptografadas, tornando difícil rastrear e identificar os proprietários. Além disso, as transações em criptomoedas podem ser executadas sem a necessidade de intermediários, o que dificulta ainda mais a identificação dos proprietários desses ativos.

Uma das formas de apreensão desses ativos é através da cooperação internacional entre as autoridades dos diferentes países. As autoridades podem trabalhar em conjunto para rastrear as transações e identificar as pessoas envolvidas nas atividades ilegais. Outra forma de apreensão é através da identificação dos proprietários das carteiras virtuais e a obtenção de ordens judiciais para apreender os ativos.

No entanto, é importante lembrar que a apreensão de AV pode ser complexa e demorada. As autoridades devem estar preparadas para lidar com situações que envolvam tecnologia avançada e investir em recursos para desenvolver novas técnicas de investigação que possam ser aplicadas a esses casos.

Por fim, é importante destacar que a prevenção é sempre o melhor caminho. É necessário investir em consciencialização e educação para evitar que as pessoas se envolvam

em atividades ilícitas que envolvam AV. Além disso, a regulamentação adequada do mercado de criptomoedas pode ajudar a prevenir e combater o uso desses ativos em atividades criminosas.

Respondidas, assim, as QD chega a altura de obter uma resposta à **QC**: **Quais as principais implicações no recurso a Ativos Virtuais e possíveis formas de atuação no âmbito da missão da investigação tributária da GNR?,** onde o recurso a AV apresenta diversas implicações no âmbito da investigação tributária da GNR. Devido à sua natureza descentralizada e ao anonimato que proporciona, torna-se mais difícil a identificação dos titulares desses ativos, bem como a sua rastreabilidade. Isso pode facilitar a evasão fiscal e a prática de ilícitos criminais, como Branqueamento de Capitais e financiamento ao terrorismo.

Para atuar no combate a essas atividades, a GNR deve estar preparada para lidar com tecnologias avançadas e com formas de pagamento cada vez mais sofisticadas. É necessário desenvolver capacidades para análise de dados e investigação de transações em *blockchain*, além de estabelecer parcerias com outros órgãos e agências de inteligência financeira.

As formas de atuação no âmbito da missão da investigação tributária da GNR passam pela sensibilização dos contribuintes e pela fiscalização mais rigorosa das atividades suspeitas. Deve-se também investir em formação e capacitação de recursos humanos para lidar com estas novas tecnologias, assim como em novos métodos de investigação e de combate a ilícitos fiscais.

Em suma, é necessário que haja uma revisão da legislação tributária em relação aos AV, incluindo a criação de novas regras para tributação e a tipificação de crimes fiscais cometidos por meio desses ativos. Dessa forma, a investigação tributária da GNR terá mais meios para combater atividades ilegais e garantir a colheita de impostos devidos, bem como a perseguição processual das condutas e a completa desarticulação e desmantelamento das redes/grupos criminosos.

Após o estudo realizado, é recomendável conduzir estudos adicionais que complementem a atual pesquisa e procurem explorar e traduzir para o campo científico a importância da evolução tecnológica neste âmbito. Essa evolução não se limita apenas à tentativa da repressão e prevenção da criminalidade, mas também abrange a formação e a partilha de conhecimentos nesta área que se torna cada vez mais atual e iminente.

REFERÊNCIAS BIBLIOGRÁFICAS

Abrahão, M. A. (2011). *A Elisão Fiscal Como Ferramenta Para O Planejamento*.

Academia Militar. (2015). *NEP 520/4.ª: Trabalho de Investigação Aplicada*.

Aguiar, R. D. A. (2021). *Bitcoin como meio no crime de lavagem de dinheiro e o papel da regulamentação*.

Almeida, C. (2022). *Criptoativos e Segurança*.

Ante, L. (2021). The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum. *SSRN Electronic Journal*, 216–224. https://doi.org/10.2139/ssrn.3861106

Antonoulos, A. M. (2017). Mastering BitCoin. In *Journal of World Trade* (Vol. 50, Issue 4). https://bitcoinbook.info/

Antunes, J. E. (2018). *aS criPtoMoedaS*. *2018*, 83–108.

Assunção. (2010). Unidade de Ação Fiscal - Um ano de Atividade no Combate aos Ilícitos Tributários. *Pela Lei e Pela Grei -Revista Da GNR*, *2–7*.

Azevedo, P. A. (2017). *A Penalização Das Contraordenações Fiscais No Âmbito Do RGIT : Principais Destaques*. *10*.

Bardin, L. (1977). *Análise de Conteúdo*.

Bravo, J. dos R. (2013). Para um modelo de segurança e controlo da criminalidade económico-financeira - um contributo judiciário. In *Working Papers - OBEGEF* (Vol. 2013). http://www.gestaodefraude.eu

Broby, D., & Quimbayo, C. V. (2021). The Regulation of Initial Coin Offerings, Virtual Assets and Virtual Asset Service Providers. *SSRN Electronic Journal*, 1–15. https://doi.org/10.2139/ssrn.3946331

Brody, A., & Couture, S. (2021). Ideologies and Imaginaries in Blockchain Communities: The Case of Ethereum. *Canadian Journal of Communication*, *46*(3), 543–561. https://doi.org/10.22230/cjc.2021v46n3a3701

Campos, D. J. P. L. (1999). *Problemas fundamentais do direito tributário.*

Carapella, F., Dumas, E., Gerszten, J., Swem, N., Dumas, E., Gerszten, J., Swem, N., & Wall, L. (2022). *Decentralized Finance (DeFi): Transformative Potential & Associated Risks Decentralized Finance (DeFi): Transformative Potential & Associated Risks Table of Contents Overview DeFi Products and Services Risk Implications of DeFi Conclusion References*. *2854*.

Cardoso, J. (2020). *A investigação criminal da GNR - escutas telefónicas e a criminalidade tributária*.

Carron, L. (2021). ABCs of NFTs, art and law. *Entertainment, Arts and Sports Law Journal*, *32*(2), 13–14.

Catarino, L. G. (2022). *Ofertas públicas de crip tomoedas: fintech, tokens, smart contracts, blockchain,*.

Checco, P. dal, & Rossetti, A. (2020). *Best practices for asset tracing, seizure and confiscation in the field of virtual currency*.

Coelho, R. de C. e L. B. (2013). *A recuperação de ativos à luz da Lei n. 30/2017, de 30 de maio*. 1–194.

Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo. (2015). *Missão*. https://portalbcft.pt/pt-pt/content/missão

Comité Económico e Social Europeu. (2012). Parecer do Comité Económico e Social Europeu sobre Cooperativas e reestruturações (parcer de iniciativa). *Jornal Oficial Da União Europeia*, *C 191*(29.6.2012), 31–38. http://www.cases.pt/0_content/sobre_nos/legislacao_comunitaria/04LC-Parte-I-EcoSocial-Cooperativas.pdf

Conselho da União Europeia, & Parlamento Europeu. (2018). *DIRETIVA (UE) 2018/843 DO PARLAMENTO EUROPEU E DO CONSELHO de 30 de maio de 2018 que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que*. *2018*, 43–74.

Correia, J. C. (2015). *Apreensão ou Arresto preventivo dos proveitos do crime?*

Costa, P. (2014). *a Autoridade Tributária E Aduaneira (At) E O Exercício Da Justiça Tributária Não Aduaneira*. https://repositorio.ual.pt/bitstream/11144/985/1/A AT E O EXERCÍCIO DA JUSTIÇA TRIBUTÁRIA NÃO ADUANEIRA versão final.pdf

Costa, R. (2013). *A Unidade de Ação Fiscal e a Interoperabilidade com as Autoridades de Combate ao Crime Fiscal e Aduaneiro Academia Militar A Unidade de Ação Fiscal e a Interoperabilidade com as Autoridades de Combate ao Crime Fiscal e Aduaneiro*.

Costa, R. (2020). *Relatório Final - International Asset Recovery*. 1–19.

Costa, V. (2022). *O Papel da Unidade de Ação Fiscal no combate ao Trade-Based Money Laundering*.

Cruz, N. (2018). *A investigação económica , financeira e tributária da criminalidade organizada transnacional na União Europeia*.

Dawson, M. (2016). New Modes of Governance. *A Companion to European Union Law and*

International Law, 119–135. https://doi.org/10.1002/9781119037712.ch9

Dias, E. (2011). Padrões De Actuação Com Maior Relevância No Âmbito Da Criminalidade Económico- Financeira. *CEPESE / Fronteira Do Caos*, 151–158.

Dias, P. (2017). O Papel da Guarda Nacional Republicana no Combate e Prevenção do Ciberterrorismo. *Academia Militar*, 113.

Dowling, M. (2022). Fertile LAND: Pricing non-fungible tokens. *Finance Research Letters*, *44*(April 2021), 102096. https://doi.org/10.1016/j.frl.2021.102096

Dziura, M., Jaki, A., & Rojek, T. (2020). *Restructuring management. models - changes - development*. *September*.

Europol. (2021). Cryptocurrencies - Tracing the evolution of criminal finances. *Europol Spotlight Report Series*, *Publicatio*.

Evans, D. (2012). The Internet of Everything - How More Relevant and Valuable Connections Will Change the World. *CISCO Internet Business Solution Group (IBSG)*, 1–9.

Fassano, D. M. C. (2020). *Blockchain Aplicada à Aviação: Uma Revisão Integrativa da Literatura*.

FATF. (2014). *FATF REPORT - Virtual Currencies - Key Definitions and Potential AML/CFT Risks*. *June*.

Ferreira, B. (2018). *O papel da Unidade de Ação Fiscal no combate às fraude e evasão fiscais no comércio eletrónico: o Imposto sobre o Valor Acrescentado na transmissão de bens*.

Ferreira, R. (2022). *A HIPERDIGITALIZAÇÃO DOS SERVIÇOS FINANCEIROS E O DESAFIO DAS MOEDAS DIGITAIS DE BANCOS CENTRAIS (CBDCS)*. 1–22.

Figueiredo, H. (2021). Direito processual penal económico – (dis)funcionalidades conexas com as pessoas coletivas. *Galileu-Revista de Economia e Direito*, *XXII*(2), 65–73. https://doi.org/10.26619/2184-1845.xxii.2.5

Filipe, M. J. P. dos S. (2018). *A criminalidade económica e financeira : o tipo legal de burla e os agentes do crime*.

Financial Action Task Force - GAFI. (2020). *Trade-Based Money Laundering Trends and Developments*. *December*, 6. www.fatf-gafi.org

Florysiak, D. (2022). Utility Tokens, Markets in Crypto Assets Regulation (MiCAR), and the Costs of Being Public. *SSRN Electronic Journal*, 1–17. https://doi.org/10.2139/ssrn.4295913

Fontes, J. F. P. N. (2022). *A crescente abertura dos mercados derivada da globalização*. 1–

44.

Fortin, M.-F. (2009). *O Processo de Investigação: da concepção à realização* (Lusociência (ed.); 5ª).

Fraga, W. G., Da Costa, N. R., Almeida, F. V., Rebelo, R. M., Moraes, K. O. C., Rezende, J. A., Santana, M. H. P., & Maldaner, A. O. (2016). Identification of the major active ingredients in illegal pesticide seized by Brazilian federal police and quantification of metsulfuron-methyl and tebuconazole. *Revista Virtual de Quimica*, *8*(3), 561–575. https://doi.org/10.5935/1984-6835.20160043

Freixo, M. (2012). *Metodologia científica: fundamentos, métodos e técnicas* (I. Piaget (ed.); 4ª).

GAFI. (2021). *VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS*. *October*.

Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). *Price Manipulation in the Bitcoin Ecosystem*.

Garção, H. M. G. (2008). *A Unidade De Acção Fiscal: Uma Análise Estrutural para o Sucesso*.

Gonçalves, J. P. da C. (2021). *Blockchain & Bitcoin - O Impacto na Contabilidade : Perspetivas de Contabilistas Certificados e Revisores Oficiais de Contas Portugueses*.

Gortsos, C. (2021). The Commission's 2020 Proposal for a Markets in Crypto-Assets Regulation ('MiCAR'): A Brief Introductory Overview. *SSRN Electronic Journal*, 1–114. https://doi.org/10.2139/ssrn.3842824

Gouveia, L. D. (2021). *Blockchain*.

Griffith, K. (2014). *A Quick History of Cryptocurrencies BBTC — Before Bitcoin*.

Guillot, J. D. (2022). Cryptocurrency dangers and the benefits of EU legislation. *European Parliament*.

Hardjono, T., Lipton, A., & Pentland, A. (2020). *Wallet Attestations for Virtual Asset Service Providers and Crypto-Assets Insurance*. 1–35. http://arxiv.org/abs/2005.14689

Helbig, J. M. (2022). *Da Blockchain ao Criptoinvestidor*.

Kafteranis, D., & Turksen, U. (2022). Art of Money Laundering with Non-Fungible Tokens: A myth or reality? *European Law Enforcement Research Bulletin*, *22*(101022004), Nr.6: tbd-Nr.6: tbd. https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/531

Kalodner, H., Carlsten, M., Ellenbogen, P., Bonneau, J., & Narayanan, A. (2015). An empirical study of Namecoin and lessons for decentralized namespace design. *14th Annual Workshop on the Economics of Information Security (WEIS)*.

Kushwaha, S. S., Joshi, S., & Member, S. (2022). Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract. *IEEE Access*, *10*, 6605–6621. https://doi.org/10.1109/ACCESS.2021.3140091

Li, C., Li, P., Zhou, D., Yang, Z., Wu, M., Yang, G., Xu, W., Long, F., & Yao, A. C. C. (2020). A decentralized blockchain with high throughput and fast confirmation. *Proceedings of the 2020 USENIX Annual Technical Conference, ATC 2020*, 515–528.

Lopes, D. (2022). *A Unidade de Ação Fiscal no Combate ao Comércio ilegal de A Unidade de Ação Fiscal no Combate ao Comércio ilegal de*.

Lourenço, A. F. F. (2017). O papel da Unidade de Ação Fiscal no combate ao crime organizado. *Academia Militar*.

Maia, E. G. D. V. (2018). *A criptomoeda na Ordem Jurídica: velhas soluções para um novo problema?* 1–58.

Marques, S. R. P. (2009). A Fraude fiscal e a Simulação. *Eunomía. Revista En Cultura de La Legalidad.*, 170–175. https://e-revistas.uc3m.es/index.php/EUNOM/article/view/2081/1014

Martins, D. A., Frederico, D., Pinto, C., & Nova, U. (2021). *A Constituição de Assistente nos Crimes Económicos*.

Meireles, T. (2011). *A NATUREZA DO CRIME FISCAL E A ACTUAÇÃO DA GNR*.

Melkevik, B., & Melkevik, Å. (2017). Why Individual Freedom and the Autonomy of Law Stand or Fall Together. *Revista Acadêmica Da Faculdade de Direito Do Recife*, *89*(01), 04. https://doi.org/10.51359/2448-2307.2017.22982

Ministério Público. (2009a). *O que Fazemos*. https://cibercrime.ministeriopublico.pt/pagina/o-que-fazemos-0

Ministério Público. (2009b). *Quem somos*. https://cibercrime.ministeriopublico.pt/pagina/quem-somos

Mota, L. (2021). A Intervenção da GNR nos Crimes de Violência Doméstica e o Curso de Especialização CIAVE. *Academia Militar*, 113.

Nance, M. T. (2018). *The regime that FATF built : an introduction to the Financial Action Task Force*. 109–129.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.

Nogueira, A. F. P. (2020). *O impacto da criptomoeda nas empresas de software em Portugal*. https://repositorio-aberto.up.pt/bitstream/10216/130406/2/431804.pdf

Nunes, C. C. (2018). *O Ministério Público na prevenção do branqueamento e do financiamento do terrorismo*. 93–140.

Oliveira, P. G. (2009). *Contabilidade tributária*. 3.

Pacheco, A. V. (2018). *Bitcoin*.

Parlamento Europeu. (2022). *Procedure file - Digital finance: Markets in Crypto-assets (MiCA)*.

Pellizarri, D. (1990). *A grande farsa da tributação e sonegação.*

Pereira, L. (2012). *Autoridade Tributária e Aduaneira (AT) - Inspeção Tributária e as ações conjuntas com outras Entidades*.

Perset, K. (2010). The Economic and Social Role of Internet Intermediaries. *Notes, April*, 49. http://www.oecd.org/dataoecd/49/4/44949023.pdf

Peter, L. (2021). *Investing in Virtual Assets*. *March*.

Procuradoria-geral da república - Despacho de criação Gabinete Cibercrime, de 7 de dezembro de 2011., 1 (2011).

Polícia Judiciária. (2011). *GRA*. https://www.policiajudiciaria.pt/gra/

Polícia Judiciária. (2017). *UIF*. https://www.policiajudiciaria.pt/uif/

Polícia Judiciária. (2020). *UNC3T*. https://www.policiajudiciaria.pt/unc3t/

Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021). CeFi vs. DeFi -- Comparing Centralized to Decentralized Finance. In *Proceedings of ACM Conference (Conference'17)* (Vol. 1, Issue 1). Association for Computing Machinery. http://arxiv.org/abs/2106.08157

Quivy, R., & Campenhoudt, L. V. (2013). *Manual de Investigação em Ciências Sociais* (Gradiva (ed.); 6ª).

Riegelnig, D., & Suisse, B. (2019). *OpenVASP : An Open Protocol to Implement FATF ' s Travel Rule for Virtual Assets*. 1–36.

Roberge, I. (2011). *Finantial Action Task Force*.

Sampaio, L., Abijaude, J., Coutinho, A., Greve, F., Valcy, Í., & Queiroz, S. (2018). *Blockchain e a Revolução do Consenso sob Demanda*.

Santos, J. V. dos. (2018). Soft Law e boa governança no mercado das criptomoedas. *Revista Electrónica de Direito, 2*. https://doi.org/10.24840/2182-9845_2018-0002_0008

Sarmento, M. (2013a). *Guia Prático sobre a Metodologia Científica para a Elaboração, Escrita e Apresentação de Teses de Doutoramento, Dissertações de Mestrado e Trabalhos de Investigação Aplicada* (Universidade Lusíada (ed.); 3ª).

Sarmento, M. (2013b). *Metodologia científica para a elaboração, escrita e apresentação de*

teses. (Universidade Lusíada (ed.)).

Seiça, A. (2019). *Aplicação de técnicas de Text Mining na perceção dos cidadãos quanto ao funcionamento da Autoridade Tributária e Aduaneira*.

Souza. (1998). *Carga tributária no Brasil*.

Teive, P. C., & Petri, S. M. (2022). *Elisão Fiscal: Impacto Tributário do Regime Especial de Tributação no Processo de Adesão por uma Empresa de Incorporação Imobiliária da Grande Florianópolis.* 1–23.

Teixeira, J. (2022). *Branqueamento e criptomoedas Uma análise das novas entidades obrigadas do sistema*.

Toguchi, M. S. (2021). *O Crime de Lavagem de Dinheiro com o Uso de Bitcoin*. 6.

Vasconcelos, A. I. G. de. (2022). *Bitcoin, (des)regulação e barreiras estaduais à internacionalização: O caso de El Salvador*.

Vasek, M., Bonneau, J., Castellucci, R., Keith, C., & Moore, T. (2016). The Bitcoin Brain Drain: A Short Paper on the Use and Abuse of Bitcoin Brain Wallets. *20th International Conference on Financial Cryptography and Data Security (FC 2016)*.

Vieira, S. F. C. (2019). *Bitcoin: Propridades Empíricas*.

Wieandt, A., & Heppding, L. (2022). *Centralized and decentralized finance: Coexistence or convergence? Axel Wieandt*.

Yamashita, D. (2005). *Elisão e evasão de tributos: planejamento tributário: limites à luz do abuso do direito e da fraude à lei*.

Zarrin, J., Wen Phang, H., Babu Saheer, L., & Zarrin, B. (2021). Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Computing*, *24*(4), 2841–2866. https://doi.org/10.1007/s10586-021-03301-8

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. *Journal of Financial Regulation*, *6*(2), 172–203. https://doi.org/10.1093/jfr/fjaa010

Legislação, jurisprudência e outra documentação

Assembleia da República (1995) - Decreto-Lei n.º 48/95, de 15 de março, que aprova o Código Penal. Procuradoria-Geral Distrital de Lisboa. Disponível na Internet em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=109&tabela=leis

Assembleia da República (2001) - Lei n.º 15/2001, de 05 de junho, que reforça as garantias do contribuinte e a simplificação processual, reformula a organização judiciária tributária e estabelece um novo regime geral para as infrações tributárias. Procuradoria-Geral

Distrital de Lisboa. Disponível na Internet em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=259&pagina=1&ficha=1

Assembleia da República (2008) - Lei n.º 49/2008, de 27 de agosto, que aprova a Lei de Organização da Investigação Criminal. Procuradoria-Geral Distrital de Lisboa. Disponível na Internet em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1021&tabela=leis&so_miolo=

Assembleia da República (2008) – Lei nº37/2008 de 6 de agosto, que aprova a Lei Orgânica da Polícia Judiciária. Procuradoria-Geral Distrital de Lisboa. Disponível na Internet em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3215&tabela=leis&so_miolo=

Assembleia da República (2009) – Decreto-Lei nº42/2009 de 12 de fevereiro, que estabelece competências das unidades da polícia judiciária. Procuradoria-Geral Distrital de Lisboa. Disponível na Internet em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=1050A0029&nid=1050&tabela=leis&pagina=1&ficha=1&nversao=

Assembleia da República (2011) – Decreto-Lei nº 118/2011 de 15 de dezembro, Autoridade Tributária. Procuradoria-Geral Distrital de Lisboa. Disponível na Internet em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1578&tabela=leis&so_miolo=

Assembleia da República (2013) - Decreto-lei n.º 115/2013, de 7 de agosto, que Procede à terceira alteração ao Decreto-Lei n.º 74/2006, de 24 de março, que aprova o regime jurídico dos graus académicos e diplomas do ensino superior, em desenvolvimento do disposto nos artigos 11.º a 17.º da Lei n.º 46/86, de 14 de outubro (Lei de Bases do Sistema Educativo). Procuradoria-Geral Distrital de Lisboa. Disponível na Internet em: https://dre.pt/dre/detalhe/decreto-lei/115-2013-498487

Assembleia da República (2013) - Lei n.º 67/2013, de 28 de agosto, Lei-quadro das entidades administrativas independentes com funções de regulação da atividade económica dos setores privado, público e cooperativo. Procuradoria-Geral Distrital de Lisboa. Disponível na Internet em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1983&tabela=leis&so_miolo=S

Assembleia da República (2017) – Lei n.º 83/2017, de 18 de agosto, que estabelece medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo, transpõe parcialmente as Diretivas 2015/849/UE, do Parlamento Europeu e do Conselho, de 20 de maio de 2015, e 2016/2258/UE, do Conselho, de 6 de dezembro de 2016, altera o Código Penal e o Código da Propriedade Industrial e revoga a Lei n.º 25/2008, de 5 de junho, e o Decreto-Lei n.º 125/2008, de 21 de julho. Procuradoria-Geral Distrital de Lisboa. Disponível na Internet em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=2750A0034&nid=2750&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=

Assembleia da República (2019) – Decreto-Lei n.º 137/2019, de 13 de setembro, que aprova a nova estrutura organizacional da Polícia Judiciária. Procuradoria-Geral Distrital de Lisboa. Disponível na Internet em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3215&tabela=leis&so_miolo=

Conselho de Ministros (2015) - Resolução do Conselho de Ministros n.º 88/2015, de 6 de outubro, que cria a Comissão de Coordenação das Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo. Disponível na Internet em: https://dre.pt/dre/detalhe/resolucao-conselho-ministros/88-2015-70462183

APÊNDICES

APÊNDICE A – CARTA DE APRESENTAÇÃO

CARTA DE APRESENTAÇÃO

No âmbito da elaboração do Relatório Científico Final do Trabalho de Investigação Aplicada da Academia Militar, surge a investigação com o tema **"Investigação Económico-Financeira: Implicações do Recurso a Ativos Virtuais"** para obtenção do grau académico de mestre em Ciências Militares, na especialidade de Segurança.

Admitindo que a prevenção dos comportamentos criminosos é considerada, cada vez mais, uma atividade basilar para o bem-estar da sociedade, o fenómeno dos ativos virtuais é uma novidade no âmbito da ação fiscal por parte da Guarda Nacional Republicana e das Forças e Serviços de Segurança de forma geral, que leva à necessidade da criação de procedimentos e métodos de combate aos crimes tributários cometidos através desta inovação tecnológica no panorama económico nacional.

Esta tecnologia "elimina" a forma como o paradigma das entidades bancárias é visto e ainda a sua importância e necessidade como terceiro membro de uma transação. Surge então o problema da criminalidade económico-financeira.

Assim, com o intuito de recolher informações, surge a necessidade de realizar entrevistas dirigidas aos elementos dos vários organismos competentes que têm conhecimento sobre a matéria suprarreferida, nomeadamente a Polícia Judiciária (PJ), o Departamento Central de Investigação e Ação Penal (DCIAP), a Procuradoria Geral da República (PGR), a Guarda Nacional Republicana e o *European Financial and Economic Crime Centre* (EFECC).

Saliento que a entrevista que dirijo a V. Exa. reveste uma importância fundamental para a presente investigação, na medida em que permite desenvolver um levantamento de constrangimentos e projetar soluções, as quais se pretendem úteis para a Instituição.

Agradecendo a atenção dispensada e despeço-me apresentando os meus melhores cumprimentos. Bem-haja pela colaboração de V. Exa.

Agradeço a disponibilidade e a colaboração.

Atenciosamente,

Paulo Alcobia Carvalho

Aspirante GNR-Infantaria

APÊNDICE B – GUIÃO DE ENTREVISTA

ACADEMIA MILITAR

Investigação Económico-Financeira
— Implicações do Recurso a Ativos Virtuais

Autor: Aspirante de GNR Infantaria Paulo Alcobia Carvalho

Orientador: Professor Catedrático Doutor José Fontes

Coorientador: Capitão GNR Infantaria Gabriel Oliveira

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Dissertação de Mestrado

Lisboa, maio de 2023

1. IDENTIFICAÇÃO DO ENTREVISTADO

Nome:
Idade:
Habilitações Literárias:
Cargo/Posto:
Função:
Local:
Data:
Hora de início;
Hora do fim:

2. GUIÃO DE ENTREVISTA

Pergunta 1 – Tendo em conta o recurso a Ativos Virtuais, qual é o panorama nacional ao nível da criminalidade económico-financeira?

Pergunta 2 – Qual é a principal criminalidade associada aos Ativos Virtuais?

Pergunta 3 – Quais as vantagens e desvantagens, do ponto de vista da (Entidade), inerentes à utilização destes ativos?

Pergunta 4 – Na ótica da (Entidade), quais são as alterações legislativas necessárias para que os ilícitos económico-financeiros, com recurso a Ativos Virtuais, sejam minimizados?

Pergunta 5 – Qual o procedimento de apreensão de Ativos Virtuais utilizado na (Entidade)?

Pergunta 6 – Quais as principais barreiras à apreensão de Ativos Virtuais?

Pergunto 7 – Principais dificuldades na atuação da (Entidade) no âmbito do combate à criminalidade económico-financeira com recurso a Ativos Virtuais?

Pergunta 8 – Medidas a adotar pela (Entidade), enquanto FFSS, no âmbito do combate à criminalidade económico-financeira com recurso a Ativos Virtuais?

APÊNDICE C – MODELO DE ANÁLISE DE CONTEÚDO DO TIA

Quadro 2 – Modelo de análise de conteúdo do TIA

<table>
<tr><th>Objetivos</th><th>Questões</th><th>Enquadramento Teórico e Concetual</th><th>Análise de Resultados</th></tr>
<tr><td>OG: Analisar a implicação do recurso a ativos virtuais na futura atividade da Guarda Nacional Republicana.</td><td>QC: Quais as principais implicações no recurso a Ativos Virtuais e possíveis formas de atuação no âmbito da missão da investigação tributária da GNR?</td><td>Todo o trabalho concorre</td><td rowspan="5">Capítulo 5 – Apresentação, Análise e Discussão de Resultados

Apresentação e Análise das entrevistas elaboradas à UNCC, UNC3T, UIF, SIC – UAF, DIC – CO, EFECC, Gabinete de Cibercrime da PGR e Branqueamento e Cibercrime do DCIAP.</td></tr>
<tr><td>OE₁: Descrever as vantagens e desvantagens dos sistemas centralizados e descentralizados.</td><td>QD₁: Quais as vantagens e desvantagens do sistema financeiro descentralizado?</td><td rowspan="3">Capítulo 1 – Ativos Virtuais: Origem e História

Capítulo 2 – Investigação Económico Financeira

Entrevistas</td></tr>
<tr><td>OE₂: Compreender as principais formas de controlo no recurso a Ativos Virtuais.</td><td>QD₂: Quais são as principais formas de controlo no recurso a estes ativos?</td></tr>
<tr><td>OE₃: Analisar estruturas e atores no combate à criminalidade económico-financeira.</td><td>QD3: Quais são as principais dificuldades que a GNR vai encontrar tendo em conta esta nova problemática?</td></tr>
<tr><td>OE₄: Entender quais as principais atividades criminais e ilícitos associados aos Ativos Virtuais.</td><td>QD4: Quais as alterações legislativas necessárias para a prevenção da consumação de ilícitos criminais recorrendo a ativos virtuais?</td><td rowspan="2">Capítulo 3 – Implicações do Recurso a Ativos Virtuais

Entrevistas</td></tr>
<tr><td>OE₅: Compreender a forma necessária e possível de apreensão deste tipo de ativos de acordo com o panorama jurídico nacional.</td><td>QD₅: Quais as formas necessárias e possíveis para a apreensão destes ativos?</td></tr>
</table>

Fonte: Elaboração própria

APÊNDICE D – RELAÇÃO ENTRE AS QUESTÕES DA ENTREVISTA E AS QUESTÕES DE INVESTIGAÇÃO

Quadro 3 – Relação entre as questões da entrevista e as Questões Derivadas

Questão Central	Questões Derivadas	Questões de Entrevista
Quais as principais implicações no recurso a Ativos Virtuais e possíveis formas de atuação no âmbito da missão da investigação tributária da GNR?	**QD$_1$:** Quais as vantagens e desvantagens do sistema financeiro descentralizado?	P3- Quais as vantagens e desvantagens, do ponto de vista da (Entidade), inerentes à utilização destes ativos?
	QD$_2$: Quais são as principais formas de controlo no recurso a estes ativos?	P4- Na ótica da (Entidade), quais são as alterações legislativas necessárias para que os ilícitos económico-financeiros, com recurso a Ativos Virtuais, sejam minimizados?
		P8- Medidas a adotar pela (Entidade), enquanto FFSS, no âmbito do combate à criminalidade económico-financeira com recurso a Ativos Virtuais?
	QD3: Quais são as principais dificuldades que a GNR vai encontrar tendo em conta esta nova problemática?	P7- Principais dificuldades na atuação da (Entidade) no âmbito do combate à criminalidade económico-financeira com recurso a Ativos Virtuais?
	QD4: Quais as alterações legislativas necessárias para a prevenção da consumação de ilícitos criminais recorrendo a ativos virtuais?	P1- Tendo em conta o recurso a Ativos Virtuais, qual é o panorama nacional ao nível da criminalidade económico-financeira?
		P2- Qual é a principal criminalidade associada aos Ativos Virtuais?
	QD$_5$: Quais as formas necessárias e possíveis para a apreensão destes ativos?	P6- Quais as principais barreiras à apreensão de Ativos Virtuais?
		P5- Qual o procedimento de apreensão de Ativos Virtuais utilizado na (Entidade)?

Fonte: Elaboração própria

APÊNDICE E – QUADROS DE ANÁLISE DE CONTEÚDO DAS ENTREVISTAS

Quadro 4 – Análise de conteúdo das respostas à questão n.º 1

Respostas à Questão n.º 1 da Entrevista ***Tendo em conta o recurso a Ativos Virtuais, qual é o panorama nacional ao nível da criminalidade económico-financeira?***	
E1	*"Não detemos informação/dados que permitam aferir o panorama nacional na área económico-financeira. Sobre este assunto em concreto poderá ser contactada a PJ, sugerindo-se a consulta a dois órgãos em particular: a* ***Unidade de Informação Financeira (UIF) o Gabinete de Recuperação de Ativos (GRA)****"*
E2	*"No que concerne à criminalidade económico-financeira,* ***as organizações criminosas transnacionais, evoluíram para formas de empresas multinacionais, concentrando o seu esforço na maximização dos proveitos económicos, alternando com facilidade o setor económico em que atuam, surgindo dotadas da capacidade de providenciar a prestação se serviços ou transmissão de bens, sejam eles lícitos ou ilícitos, de um modo transparente ou oculto das autoridades de controlo.*** *A liberalização dos mercados financeiros, especialmente dos mercados de capitais e mercados não regulamentados, onde poderemos considerar os ativos virtuais,* ***impossibilita as autoridades nacionais, a par dos restantes Estados soberanos e organizações internacionais de conhecerem as suas operações, logo de as regularem e de as sujeitarem aos ordenamentos jurídicos nacionais e internacionais.*** *Deste modo, as organizações criminosas transnacionais,* ***abrigam as suas operações nestes fundos*** *e veículos financeiros, que enformam um* ***método de excelência para conduzir crimes primários e, consequentemente, para adquirir, canalizar, e reinvestir proveitos lícitos ou ilícitos de um modo oculto e dissimulado****."*
E3	*"De forma crescente,* ***os ativos virtuais, ou criptoativos, têm vindo a ser utilizados na criminalidade em geral, em duas modalidades: por um lado, como instrumento do crime; por outro, como objeto do crime****.*

	*Enquanto **instrumento do crime, os criptoativos têm servido de moeda de troca e pagamento**. É o caso, por exemplo, do pagamento de resgates em casos de ataques informáticos de ransomware, ou outros ataques informáticos.* *Enquanto **objeto do crime, os criptoativos têm sido objeto de furto, por via do ataque informático a plataformas digitais**. Mas também têm sido objeto de diversas formas de burlas, sobretudo em plataformas fraudulentas de supostos investimentos em criptoativos. Sobre este tema foi emitido um "alerta cibercrime" pelo Gabinete Cibercrime da Procuradoria-Geral da República (https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/2021-05-02_alerta_cripto_forex.pdf).* ***Em ambos os casos os criminosos exploram a possibilidade de anonimização que os criptoativos conferem e também o grande desconhecimento que o comum dos cidadãos tem sobre estas realidades e a forma como elas podem ser utilizadas**."*
E4	*"A utilização de ativos virtuais encontra-se em pleno desenvolvimento. Se estivermos a pensar em moedas virtuais as transações ocorrem com normalidade e **inclusivamente já são utilizadas (aceites) em escrituras públicas que titulam a aquisição de imóveis**. Evidentemente existem problemas que podem surgir como a integração de capital advindo **de crime de branqueamento de capitais**. Quanto outros ativos como os tokens fungíveis, stablecoins, tokens não fungíveis (NFTs), protocolos de finanças descentralizadas (DeFi) e similares ainda não existe um mercado desenvolvido mas já temos algumas experiências de venda desses produtos em território nacional **para os quais os OPC não estão preparados para investigar."***
E5	*"A utilização de ativos virtuais em Portugal não é, ainda, muito significativa. Contudo, **existem casos em que foram reportadas ações que envolveram ativos virtuais, tendo-se já apreendido carteiras de ativos virtuais** em investigações em curso."*
E6	*"O crime tem acompanhado as mudanças de paradigma da sociedade, caraterizado pela globalização e nova era tecnológica, bem como recurso a novas formas de realizar a circulação, integração e colocação dos seus*

	proventos. Assim, ***os objetivos dos criminosos na criminalidade económico-financeira organizado e de cariz transnacional é o lucro****. Por isso existe a necessidade de* ***ocultarem os proventos do crime, fazendo-o de forma anónima, pelo que cada vez mais recorrem aos ativos virtuais****. Porque permitem aos criminosos* ***dissipar os seus proventos****, tudo à distância de um "click" neste mundo global e sem deixarem registo e por isso de difícil rastreamento."*
E7	*"Verifica-se o aumento, na nossa opinião, quase exponencial do recurso a ativos virtuais, para a retirada de proveitos da prática criminosa."*
E8	*"Aquilo que era um* ***nicho de transmissão de valor do cibercrime*** *está a tornar-se num instrumento* ***habitual de branqueamento de capitais****/transmissão de valor do crime organizado.* ***Estamos perante um desafio de conhecimento, em que rapidamente temos de ter investigadores e ferramentas capazes de analisar, seguir, identificar os verdadeiros proprietários e apreender ativos virtuais****. O crime organizado consciente da dificuldade inerente aos serviços de investigação do estado em adaptar-se às novas tecnologias, especialmente às de natureza descentralizada,* ***está a abraçar esta tecnologia de forma muito mais rápida visto que possui a capacidade financeira para contratar o apoio de especialistas de topo na área."***

Fonte: Elaboração própria

Quadro 5 – Análise de conteúdo das respostas à questão n.º 2

Respostas à Questão n.º 2 da Entrevista ***Qual é a principal criminalidade associada aos Ativos Virtuais?***	
E1	*"(Falando pela atividade desenvolvida na área digital forense, nos casos em que a Guarda é solicitada a intervir e no enquadramento das suas competências)* *Não temos identificada criminalidade associada aos ativos virtuais.* ***O que temos identificado é a detenção de carteiras de ativos virtuais por diversos atores em***

	***processos crime de moldura penal diversa**, exemplo de processos por **tráfico de estupefacientes e violência doméstica**, não significando necessariamente que o uso ou detenção dessas carteiras seja um ato criminoso e que essa seja uma criminalidade associada.* *Sabe-se que, noutras molduras penais, investigadas no uso de competências exclusivas da PJ, o uso de ativos virtuais potencialmente associado a práticas de atividade criminal é uma realidade."*
E2	*"A Avaliação nacional de riscos de branqueamento de capitais e de financiamento do terrorismo consecutivamente releva **os crimes tributários como sendo aqueles que constituem a maior ameaça ao branqueamento de capitais**.* *Com efeito, o crime de fraude fiscal além de ser um ilícito que se encontra elencado no catálogo de crimes subjacentes à Lei do branqueamento, assume uma fatia significativa das infrações subjacentes ao branqueamento de capitais (mais de 45%) face às restantes tipologias criminais, pelo que embora, não disponha de conhecimento sobre um eventual estudo sobe esta matéria**, julga-se que o recurso aos ativos virtuais é transversal a toda a criminalidade organizada, e em particular na criminalidade económico-financeira e tributária."***
E3	*Não creio que possa associar-se qualquer tipo específico de criminalidade à utilização de criptoativos. Como acima já referi, os criptoativos têm sido utilizados diversificadamente, como acima referi.* *Em todo o caso, os **crimes que supõem tecnologias e utilização das redes de comunicação e dos ambientes virtuais são naturalmente mais propícios à utilização de criptoativos.** Além da cibercriminalidade, recorrem também aos criptoativos as **inúmeras vendas fraudulentas na Internet, ou outro tipo de vendas em mercados na Darkweb, como por exemplo a venda de drogas, de armas, de pornografia infantil ou ainda de documentos falsos**.*
E4	*"**Os criptoativos encontram-se associados a diversas atividades ilícitas**. São a **forma de pagamento mais comum** (quase única) nas compras de produtos **ilícitos na darkweb** (como droga clássicas e sintéticas, armas, e outros objetos*

	de circulação restrita ou condicionada como medicamentos, ouro, etc…). São, também, vulgarmente utilizados como um dos ***modus operandi para ocultas os proveitos de atividades ilícitas efetuando a lavagem de dinheiro e branqueando o dinheiro ilicitamente obtido****. São, ainda, utilizados no comércio de mercadorias proibidas, devido às suas caraterísticas de anonimato, e ausência de regulação com uma natureza global.* *Durante o período da pandemia assistimos a um aumento das burlas relacionadas com criptomoedas, forex e outros ativos financeiros.* *Os burlões aliciam as vítimas* ***para esquemas piramidais****, convidando-os a pagar mensalidades que podem atingir as centenas de euros para abrir uma conta de cliente. Em contrapartida, prometem recompensá-los com vários tipos de bónus, à medida que as aplicações financeiras forem gerando retorno.* ***Encontram-se pendentes várias burlas deste tipo no DCIAP e noutros departamentos do MP."***
E5	*"Desconheço se existem estudos, análises ou avaliações para se poder responder de forma cabal.* ***Porém, empiricamente, pode-se dizer que as burlas e fraudes internacionais são os tipos criminais em que se têm identificado mais conexões com ativos virtuais****.* ***Saliento que os criminosos relacionados com o vários tráficos (droga, armas, seres humanos), foram dos primeiros a explorar a possibilidade de branquear valores através de ativos virtuais****, admitindo-se a continuação da sua utilização de forma mais elaborada."*
E6	*"Por ser um conceito associado à obtenção de "****dinheiro fácil****", criando a convicção de ser um bom investimento, com uma enorme e rápida rentabilidade, temos grupos organizados dispersos por vários países que recorrem a estas* ***burlas através da intranet****, prometendo e propondo investimentos em moeda virtual – criptomoedas - principalmente bitcoin, que faz com que milhares de pessoas invistam, uns apenas por curiosidade outros pensando que irão obter lucros elevados, face à rentabilidade prometida.* ***Posteriormente quando tentam resgatar o investimento e os respetivos juros, verificam que foram enganados e que não existe moeda virtual, mas sim prejuízo no valor investido****. Estes crimes são praticados sob a ocultação de um computador, em diferentes jurisdições em*

	simultâneo, o que faz com que a sua investigação seja morosa e existam dificuldades na recuperação dos valores investidos pelos lesados."
E7	*"**A criminalidade informática, criminalidade com recurso à tecnologia/alta tecnologia informática** (ex:"ransomware", burlas qualificadas/"falsos investimentos", infrações tributárias, branqueamento de capitais…)."*
E8	*"**Neste momento é o crime de fraude**. Isto do ponto de vista do bem que é oferecido em fraudes de investimento (e que não existe) bem como do ponto de vista da conversão dos lucros do crime para facilitar a remessa de valor/processo de branqueamento dos mesmos. **Tendo em conta que o crime de fraude é um dos mais numerosos na EU, isto significa que a utilização de ativos virtuais já se tornou um lugar comum no âmbito da criminalidade económica e financeira**. De igual modo vemos a utilização regular de Ativos Virtuais para **repatriar valores por parte de alguns dos maiores carteis de trafico internacional** de cocaína e a sua utilização massificada no âmbito da cibercriminalidade."*

Fonte: Elaboração própria

Quadro 6 – Análise de conteúdo das respostas à questão n.º 3

Respostas à Questão n.º 3 da Entrevista ***Quais as vantagens e desvantagens, do ponto de vista da (Entidade), inerentes à utilização destes ativos?***	
E1	*"Vantagens: **podem permitir um seguimento do movimento dos ativos e associar esse movimento à atividade criminosa, desenvolvida pelos alvos de um processo crime.*** *Desvantagens: **é necessário um investimento por parte da instituição em novos recursos, formação do efetivo e adoção de novas formas de fazer investigação**,*

	mais digital e tecnologicamente mais evoluída, o que sugere logo que seja mais dispendiosa."
E2	*A utilização de ativos virtuais, desprovidos de ordem jurídica, jurisdição e controlo oficial, repartidos em centenas de diferentes e-currencies/cryptocurrencies que enformam um mercado monetário e financeiro fora do setor financeiro regulamentado,* ***meramente monitorizadas por mecanismos inócuos como o Blockchain, enformam um método de excelência para conduzir crimes primários e, consequentemente, para adquirir, canalizar, e reinvestir proveitos lícitos ou ilícitos de um modo oculto e dissimulado*** *(inviabilizando o "****follow the monney****").* *Contrariamente ao que acontece com instrumentos de pagamento regulados,* ***não existe qualquer proteção legal que garanta direitos de reembolso ao consumidor.*** *Realça-se ainda, que em* ***caso de desvalorização parcial ou total dos ativos virtuais, os seus utilizadores terão de suportar todo o risco associado às operações, não existindo um fundo que cubra eventuais perdas.***
E3	*"Como acima* ***disse é desvantagem deste tipo de ativos o facto de poderem ser utilizados com facilidade na prática de crimes****. Em todo o caso, esta é uma característica comum a outras realidades. Veja por exemplo as armas de fogo que, sendo instrumentos úteis e necessário à manutenção da ordem e à aplicação da lei, pelas autoridades policiais, podem também ser utilizadas na prática de crimes.* ***Da mesma forma que os circuitos bancários habituais podem também ser utilizados na prática de crimes económico-financeiros, também os cripto ativos podem ser utilizados com essa finalidade.*** *No caso especial dos criptoativos tem ainda que considerar-se serem uma realidade pouco conhecida, cujo entendimento supõe dominar técnicas e tecnologias que não são do conhecimento comum do cidadão nem dos investigadores criminais.* *Quanto a vantagens,* ***ao contrário do que comumente se pensa, a generalidade dos criptoativos e em particular das moedas virtuais, sendo de utilização anonimizada, deixam atrás de si um rasto indelével na cadeia blockchain****. Este*

	registo ***é muito útil para a investigação criminal se souber procurar e se estiver disponível tecnologia que o permita fazer.*** *A tecnologia em causa, nos dias que correm, é ainda muito cara e pouco difundida. Porém existe e está disponível."*
E4	*"****Supostamente as operações na blockchain tem mais garantias de transparência****. Tal é um mito pois existem procedimentos bem conhecidos que permitem aos operadores ocultarem a sua identidade dividindo as operações e misturando-as de* ***forma a não serem passiveis de ser seguidas*** *(o tal* ***"follow the Money").*** ***Acresce que as operações com ativos virtuais têm riscos tanto para os seus utilizadores, como para todos os participantes do mercado sendo suscetíveis à prática de burlas de vários tipos****. Na linha dos alertas das Autoridades de Supervisão Europeias e do Conselho Nacional de Supervisores Financeiros, chamando-se à atenção para diversos riscos:* *Os ativos virtuais não têm curso* ***legal em Portugal, pelo que a sua aceitação pelo valor nominal não é obrigatória; Não existe qualquer proteção legal que garanta direitos de reembolso ao consumidor que utilize ativos virtuais para fazer pagamentos, ao contrário do que acontece com instrumentos de pagamento regulados****; Em caso de desvalorização parcial ou total dos ativos virtuais, não existe um fundo que cubra eventuais perdas dos seus utilizadores, que terão de suportar todo o risco associado às operações com estes instrumentos;* ***O utilizador de ativos virtuais pode perder o seu dinheiro na plataforma de negociação****;* ***As transações com ativos virtuais podem ser utilizadas indevidamente, em atividades criminosas, incluindo de branqueamento de capitais e financiamento do terrorismo****."*
E5	*"A principal vantagem (na ótica dos seus utilizadores) é a* ***dificuldade que as autoridades (todas elas) têm em rastrear as transações de ativos virtuais, e que são as pessoas, singulares ou coletivas, e quem são os efetivos detentores dos mesmos. Sendo uma vantagem para os utilizadores é uma desvantagem quando se torna necessária a intervenção da Polícia Judiciária."***

E6	*"A vantagem para a PJ – **É o facto destes ativos serem muito voláteis, com grande oscilação de valor e carecerem de elevados conhecimentos técnicos a nível do mercado financeiro para os conseguir ocultar a fim de serem transacionados,** o que leva a que os criminosos recorram a terceiros, pessoas mais bem informadas para os coadjuvarem, o que permite que fiquem mais expostos, mantendo sempre uma ligação (física) à pessoa ou local virtual onde as mesmas estão guardadas/depositadas, como códigos de acesso, que podem ser identificados e assim permitir às policias o seu acesso, e proceder à sua localização/apreensão.* *A desvantagem para a PJ – **Estes ativos podem estar ocultos em qualquer local do mundo, sendo para isso utilizadas as diferentes aplicações informáticas ao dispor de qualquer pessoa via "online" que permite uma circulação fácil por múltiplas jurisdições. Face à facilidade como se procede a essa ocultação e anonimato como se caraterizam, não permite uma fácil identificação dos ativos virtuais, bem como quem são os seus beneficiários efetivos**. E por ser um fenómeno recente, só com o decurso do tempo as polícias se irão preparar para poderem combater esta forma de atuação. E também, **a existência cada vez maior de plataformas digitais para os colocarem, permite uma maior circulação e colocação, a fim de os dissiparem sem deixar rasto pela economia real**."*
E7	*"Vantagens para a investigação, só se for **a utilização por parte de agentes encobertos deste tipo de ativos virtuais** (mais facilmente anonimizável) …* *Desvantagens para a investigação, **são a facilidade de branqueamento dos capitais e sua fácil dispersão, que levam ao anonimato e impossibilidade de ligação/identificação ao beneficiário final das quantias provenientes dos ilícitos criminais**, bem como a impossibilidade de cobrança de impostos sobre os ativos virtuais que o estado não consegue controlar, por via do anonimato, utilização em locais não sujeitos a controle estatal."*
E8	*"Penso que esta pergunta é relativa ao ponto de vista dos criminosos, visto que o EFECC não tem opinião/é neutro em relação a questões de macroeconomia. Vantagens: facilidade de acesso/conversão de valor, facilidade de transporte/remessa de valores, dificuldade de deteção/identificação*

	policial/judicial, dificuldade de apreensão policial/judicial. ***Em suma facilitam a ocultação, transporte e remessa dos lucros do crime e dificultam a deteção/apreensão por pare das policias****. Desvantagens:* ***O seu valor tem uma alta volatilidade/representa um risco elevado para os criminosos que as mantêm em carteira por algum tempo, a sua utilização exige hardware e conhecimento informáticos acima da média e o risco de as mesmas serem furtadas por via de ataques informáticos/engenharia social é elevado.*** *"*

Fonte: Elaboração própria

Quadro 7 – Análise de conteúdo das respostas à questão n.º 4

Respostas à Questão n.º 4 da Entrevista ***Na ótica da (Entidade), quais são as alterações legislativas necessárias para que os ilícitos económico-financeiros, com recurso a Ativos Virtuais, sejam minimizados?***	
E1	*"Fazer* ***um enquadramento legal específico dos ativos virtuais****, atribuir-lhes valor económico-financeiro objetivo e regular o seu uso, detenção e movimentação.* ***A existência de um regulador/controlador específico para esta matéria."***
E2	*"Torna-se* ***premente implementar uma regulamentação mais completa nesta matéria, por forma a permitir um controlo mais efetivo destas transações, pelas autoridades competentes (permitindo o follow the monney).*** ***Diminuir as limitações no acesso à informação*** *por parte das entidades responsáveis pela investigação deste tipo de ilícitos.* ***Maior responsabilização dos profissionais do sistema bancário aquando da deteção de fluxos financeiros e manobras bancárias*** *altamentes potenciadoras da prática deste tipo de ilícitos;* ***Aumentar a moldura penal para os responsáveis pela prossecução da atividade criminosa;"***

E3	*"A imprensa noticiou que o Parlamento Europeu acabou de aprovar um quadro normativo que regulamenta a utilização na vida económica normal dos criptoativos. Trata-se ainda de um projeto de futuro quadro regulamentar, por natureza provisório, não finalizado, que terá que merecer melhor análise quando publicado no Jornal Oficial da União Europeia. Este passo é importante.* ***Porém, no campo do direito penal ou do direito processual penal, não creio que haja vantagem em alteração legislativa específica a este propósito.*** ***O que importa, sim, é que os investigadores criminais tenham um melhor e maior conhecimento desta realidade para que melhor a possam entender****. Um melhor entendimento vai conferir mais eficácia à investigação criminal****. Por outro lado, importa dotar os órgãos de polícia criminal de ferramentas tecnológicas que permitam fazer o "rastreamento" dos criptoativos na blockchain."***
E4	*"Implementação de uma* ***regulamentação mais completa e específica com a ilegalização dos mecanismos que permitem criar a opacidade das operações, impedindo a utilização de produtos do tipo "mixers" e "tumblers",*** *a par com uma maior fiscalização policial e pelas autoridades de supervisão.* *Aumento do* ***papel da regulação do Banco de Portugal e CMVM, bem como dos poderes de fiscalização em geral****."*
E5	*"Não lhe posso responder em nome da Polícia Judiciária. Enquanto responsável por uma Secção que recebe, analisa, trata e difunde informação relacionada com o branqueamento de capitais e financiamento do terrorismo, a nível interno e externo, apenas posso dizer que, de uma forma geral,* ***as maiores entidades que negoceiam estes ativos estão cientes das potencialidades que os mesmos apresentam para a sua utilização por parte dos criminosos, em especial da criminalidade organizada****. Assim, têm estado a trabalhar com as autoridades, em especial com as Unidades de Informação Financeira, para limitar essas fragilidades.* ***Sendo possível alguma regulação internacional, seria um passo significativo para a minimização referida."***

E6	*"Que **seja regulado todo este mercado e legislado no sentido de existir enquadramento legal diretamente relacionado para esta atividade**, tanto no direito adjetivo como substantivo. **Por isso deve ser obrigatório registar todo o processo de transações com moeda virtual, E sempre que sejam realizadas transações as mesmas tenham que ser declaradas à administração tributária**. Porque como é sabido, as técnicas utilizadas para ocultação dificultam o seu rastreamento."*
E7	*"**Obrigatoriedade de comunicação de transações com ativos virtuais, superiores a determinado montante** (ex: compra de imóveis), **obrigatoriedade de fiscalização/autorização das exchanges** (casas de câmbio) **por parte do Banco de Portugal para funcionamento em Portugal.** Neste momento o Banco de Portugal não tem intervenção nas criptomoedas e criptoativos, sendo somente entidade a quem se devem comunicar as ações suspeitas de branqueamento pela Lei 83/2017."*
E8	*"Ver recomendações número 1, 2 e 5 da declaração da Europol: https://www.europol.europa.eu/publications-events/publications/seizing-opportunity-five-recommendations-for-crypto-assets-related-crime-and-money-laundering"*

Fonte: Elaboração própria

Quadro 8 – Análise de conteúdo das respostas à questão n.º 5

Respostas à Questão n.º 5 da Entrevista ***Qual o procedimento de apreensão de Ativos Virtuais utilizado na (Entidade)?***	
E1	*"Haver **enquadramento legal para se proceder à apreensão, tal como em qualquer ativo, e praticar as medidas necessárias para garantir a sua custódia ao abrigo do processo crime que determinou a apreensão, preservando a sua integridade, retirando toda e qualquer forma de acesso externo à carteira que contém os ativos.** Tal como na preservação de prova tradicional, é também*

	fundamental respeitar a Cadeia de Custódia da Prova Digital para efeitos de validação/sustentação da mesma."
E2	*"Antes de abordar um eventual procedimento de apreensão, importará* ***transmitir que o assunto embora não seja propriamente uma novidade, ainda se detém de um conhecimento pouco consolidado sobre esta matéria, até pela ausência de situações operacionais.*** *Deste modo, ainda não foram emanadas pelo Comando da Guarda, orientações especificas relativas a procedimentos de apreensão de Ativos Virtuais, tendo-se neste momento em consideração****, as definidas para quaisquer outros ativos, e obviamente em linha com os procedimentos advenientes do Ministério Público, e que poderão envolver o Gabinete de Administração de Bens (GAB) e Caixa Geral de Depósitos (CGD)."***
E3	*"Em termos legais, atualmente,* ***os criptoativos não são uma moeda****. Portanto, não se lhe podem aplicar as regras aplicáveis à apreensão de dinheiro em numerário ou de dinheiro em contas bancárias.* ***São um ativo ao qual devem ser aplicadas as regras gerais que se aplicam aos ativos apreendidos em processo penal.*** *Tendo um valor económico, normalmente significativo, devem seguir o mesmo procedimento que outros ativos com valor económico relevante****: isto é, devem ser entregues ao Gabinete de Administração de Bens (GAB), que funciona no âmbito do IGFEJ."***
E4	*"****A apreensão da carteira (por exemplo em bitcoins) deve ser imediatamente transferida para uma conta "cripto" do GAB (Gabinete de Administração de Bens) e, subsequentemente convertida para euros e conservada na CGD nos termos normais para evitar depreciação****.* ***O problema está quando não se tem a "chave" criptográfica*** *e não é possível implementar o referido procedimento pois embora podendo formalmente determinar-se a apreensão materialmente não é possível realizá-la."*
E5	*"A Unidade a que pertenço não faz apreensões, incluído ativos virtuais. Já houve casos a decorrer nesta instituição em que se apreenderam carteiras de ativos virtuais. A informação que disponha, mas pode não estar atualizada, é que,* ***sem***

	***a chave da respetiva carteira é impossível proceder ao domínio da mesma, o que impossibilita uma efetiva apreensão**. **Tal chave de acesso pode ser obtida por colaboração dos arguidos ou suspeitos, ou resultado da investigação, nomeadamente através de buscas ou exames**, tanto físicas como em ambiente digital. Já aconteceram as duas situações em casos em curso."*
E6	*"**São semelhantes às outras apreensões de ativos e recorrendo à cooperação das entidades a nível nacional e internacional** que colaboram na sua localização."*
E7	*"É algo ainda em fase de desenvolvimento, à medida que se conseguem identificar entidades fiáveis e países que cooperam. **Existindo, contudo, algumas situações em que é possível proceder apreensão de ativos virtuais, desde que, atempadamente, se consiga detetar e identificar esse ativo de valor ou direito e esteja associado à cooperação.** Para o efeito, podem ser utilizados os canais de cooperação judiciária e/ou policial."*
E8	*"A Europol não tem poderes coercivos/não apreende ativos nem interfere nos procedimentos coercivos que os EM decidem adotar. Fazemos apenas sugestões baseadas nas melhores praticas e elas são disseminadas através de manuais próprios (são documentos confidenciais que podem ser obtidos via UNE ou pelo acesso direto à EPE do EC3)"*

Fonte: Elaboração própria

Quadro 9 – Análise de conteúdo das respostas à questão n.º 6

Respostas à Questão n.º 6 da Entrevista ***Quais as principais barreiras à apreensão de Ativos Virtuais?***	
E1	***"A falta de enquadramento normativo/legal e a falta de recursos técnicos e de alguma formação do efetivo."***

E2	*"**Diminuta especialização/conhecimentos técnicos** dos recursos humanos;* ***Inexistência de ferramentas tecnológicas especificas;*** ***Falta de formação."***
E3	*"A principal Dificuldade está, antes de mais na **sua identificação**. Quando se apreende um dispositivo, nem sempre é fácil ou óbvio **identificar uma carteira de criptoativos que esteja localmente alojada.*** *Já quanto às carteiras que estejam depositadas em entidades gestoras de criptoativos na Internet, a **grande dificuldade está na deslocalização, uma vez que a generalidade destas entidades tem sede fora de Portugal, algumas delas mesmo em local não determinado ou conhecido."***
E4	*"**A inexistência de formação especializada e de se dispor de software específico para este tipo de investigações** (como o "Chainalysis") o que potenciaria a atuação das investigações. Os programas do tipo Chainalysis, ou outras soluções de monitoramento de transações e investigação de criptomoedas, são a única **forma eficaz de acompanhar o que se passa na blockchain permitindo não só monitorizar as transações, como a triagem de endereços dos usuários que se conectem à plataforma, interrompendo operações criminosas, reduzindo atividades ilícitas e recuperando fundos para as vítimas."***
E5	*"Primeiro a **identificação da carteira de ativos virtuais. Depois a obtenção e domínio da chave da respetiva carteira**".*
E6	*"É o **anonimato, dificuldade de rastreamento, as operações transnacionais e o desconhecimento do beneficiário efetivo** e não ser preciso a intermediação física de qualquer das partes envolvidas, porque não carece de contacto direto para a realização de transações, o que constitui uma barreira à apreensão."*
E7	*"A **identificação dos ativos, da sua localização** (ex: carteiras frias), ligação dos ativos virtuais ao seu beneficiário, **acesso às carteiras onde estes se encontram**."*
E8	*"Temos **barreiras técnicas/práticas** (carteiras que não estão associadas a exchangers não podem ser abertas/aprendidas sem passwords e muitas das vezes as passwords apenas podem ser obtidas com a colaboração do suspeito – coisa*

	rara). ***Temos barreiras legais*** *(outras vezes as carteiras estão associadas a exchangers que não tem representação na EU mas sim em estados pouco/nada cooperantes, dificultando/impossibilitando o recurso a ordens de apreensão emitidas por Autoridades Judiciarias Europeias).* ***E temos barreiras que resultam da falta de conhecimento*** *(a apreensão de computadores, discos, documentos com passwords não significa automaticamente a apreensão de ativos virtuais, visto que estes podem ser dissipados rapidamente a partir de um qualquer outro terminal ligado à internet.* ***Doutra feita a apreensão de carteiras que não estão associadas a exchangers tem de ser taticamente bem preparada para assegurar o controlo da carteira/passwords previamente a uma intervenção física sobre os suspeitos).”***

Fonte: Elaboração própria

Quadro 10 – Análise de conteúdo das respostas à questão n.º 7

Respostas à Questão n.º 7 da Entrevista ***Principais dificuldades na atuação da (Entidade) no âmbito do combate à criminalidade económico-financeira com recurso a Ativos Virtuais?***	
E1	*“Como já foi referido,* ***a falta de recursos técnicos e formação****, específicos para esta matéria.”*
E2	*Desde logo, a* ***deteção/identificação de que o suspeito da atividade criminosa recorre a ativos virtuais****, e que eventualmente poderiam ser minimizadas com efetivos especializados e ferramentas tecnológicas especificas;* *Num momento subsequente, designadamente durante a apreensão, quando não existem as credenciais ou o suspeito não colabora.*
E3	*“O Gabinete Cibercrime não é um gabinete operacional, isto é, não tem concretos processos de investigação criminal. Trata-se de um gabinete de*

	coordenação nacional. Esta questão deve ser dirigida, ou ao DCIAP, ou aos diversos DIAP do MP."
E4	*"Dificuldades na* ***apreensão de contas quando não existem as credenciais ou o arguido recusa entregá-las.*** *Atividades ilícitas de blockchain, como* ***ransomware e golpes de criptomoedas, usando técnicas inovadoras para ocultar a sua atividade*** *(como os mixers) não são suscetíveis de quaisquer contra-medidas.* *As investigações geralmente envolvem o rastreamento de fundos à medida que são transferidos por vários tokens ou cadeias.* ***Não se dispondo do Chainalysis e fazendo essa investigação de modo manual a morosidade e os resultados são de baixa qualidade."***
E5	*"Mais uma vez não lhe posso responder em nome da Polícia Judiciária e desconheço o trabalho em concreto das várias Unidades da PJ que têm este tipo de desafios.* ***No que respeita à prevenção, realizada pela UIF, a maior dificuldade está em identificar esses ativos e depois atribuir-lhes o seu efetivo beneficiário****."*
E6	*"A existência de muitas plataformas digitais para as transações ocorrerem,* ***desregulação e anonimato, bem como as diferentes jurisdições e por isso o recurso à cooperação policial e judicial em matéria penal.*** *Porque estamos a falar de uma representação digital de valor, não emitida por um Banco Central ou Instituição Financeira., além da sua obscuridade, temos novos conceitos, novas tecnologias (ex. A tecnologia blockchain).* ***Por isso carece de muita formação e conhecimento por parte das Autoridades Reguladoras e Policiais, para o seu combate e prevenção."***
E7	*"Falta de ferramentas de investigação que leva à* ***impossibilidade de rastreio do percurso das criptomoedas, dificuldade na identificação dos beneficiários e locais onde se encontram "depositados" os criptoativos."***
E8	***"A falta de recursos humanos devidamente especializados e em número suficiente para poder fazer face ao elevado número de casos que nos são***

	submetidos. *O aumento de casos foi mais rápido do que o esperado e agora estamos a* ***investir fortemente na contratação de novos recursos já especializados e na formação de recursos pré-existentes*** *que demonstram um apetência natural para esta área. ”*

Fonte: Elaboração própria

Quadro 11 – Análise de conteúdo das respostas à questão n.º 8

Respostas à Questão n.º 8 da Entrevista ***Medidas a adotar pela (Entidade), enquanto FFSS, no âmbito do combate à criminalidade económico-financeira com recurso a Ativos Virtuais?***	
E1	*“A necessidade de* ***fazer um investimento em recursos técnicos e formação do efetivo****.”*
E2	*“No seguimento do referido anteriormente, deverá ser* ***considerada a necessidade de incrementar a formação específica para os elementos adstritos à investigação criminal da GNR.*** ***Ponderar a elaboração de um manual/ficha de procedimentos ao efetivo;*** ***Aquisição de ferramentas tecnológicas especificas;”***
E3	*“Creio que esta questão já está respondida a propósito das perguntas anteriores. Insistiria na* ***formação a este respeito e na dotação, dos serviços de investigação criminal, de ferramentas tecnológicas.****”*
E4	*“Incremento da* ***formação específica para magistrados, analistas e investigadores.*** ***Contratação de especialistas do setor.*** ***Aquisição de programas robustos para identificações das atividades e entidades envolvidas como o Chainalysis”***

E5	*"Não lhe posso responder a esta questão uma vez que não posso falar em nome da Polícia Judiciária e desconheço se existem trabalhos de reflexão em curso sobre isto."*
E6	*"Apostar no âmbito da* ***prevenção e a nível da investigação, dando continuidade ao trabalho que as UIF estão a fazer, a nível da recolha, centralização, tratamento, análise e a difusão de informação, aderir a todas as recomendações do GAFI, como orientação para as diferentes alterações legislativas****. Dar continuidade à* ***constituição de equipas especializadas de polícias com experiência e formação no tratamento das matérias relacionas com a investigação do crime económico financeiro a nível de ativos virtuais****. Porque este tipo de investigação exige uma abordagem policial diferenciada em relação à investigação criminal tradicional."*
E7	***"Aumento da formação na área, especialização das equipas que lidam com estes ativos virtuais e aquisição de ferramentas de investigação de ativos virtuais (tracing e análise)."***
E8	*"Ver recomendações número 1, 3, 4 e 5 da declaração da Europol:* https://www.europol.europa.eu/publications-events/publications/seizing-opportunity-five-recommendations-for-crypto-assets-related-crime-and-money-laundering*"*

Fonte: Elaboração própria