FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

Mestrado em Direito e Prática Jurídica

Especialidade em Ciências Jurídico-Forenses

Relatório de estágio

A PREVENÇÃO DO BRANQUEAMENTO DE CAPITAIS E FINANCIAMENTO AO TERRORISMO

O papel das entidades que exercem atividade com ativos virtuais

Raquel Maria Caldeira Fernandez

Orientadora: Professora Doutora Inês Ferreira Leite

Coorientadora: Professora Doutora Rute Saraiva

Coorientadora de estágio: Madalena Catarino

02-10-2024

FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

Mestrado em Direito e Prática Jurídica

Especialidade em Ciências Jurídico-Forenses

Relatório de estágio

A PREVENÇÃO DO BRANQUEAMENTO DE CAPITAIS E FINANCIAMENTO AO TERRORISMO

O papel das entidades que exercem atividade com ativos virtuais

Relatório de Estágio apresentado perante a Faculdade de Direito da Universidade de Lisboa como requisito parcial para obtenção do título de mestre em Direito e Prática Jurídica, especialidade em Ciências Jurídico-Forenses, sob a orientação da Professora Doutora Inês Ferreira Leite.

2024

Agradecimentos

À Maria Inês, o ser mais pequenino, mas que mais força e luz dá à minha vida.

À minha mãe, Luísa, o meu maior suporte. Sempre.

Às minhas irmãs, Sara e Rute, que fazem parte de mim e são o melhor que tenho.

Ao meu pai, Nicolau, pela força, paciência, sabedoria.

Ao meu cunhado, Rúben, por ser o meu irmão mais velho.

Às minhas tias Elma, Lídia, Dolores, Maria e Paula, por todo o apoio.

Ao meu amigo Luís Filipe. O que nunca me falta.

À minha prima Bia, por me ter mostrado que faz parte do percurso.

À Edleusa e à Sónia, o melhor da FDUL.

Ao Rodrigo, por todo o amor neste trajeto e fase da vida.

À minha psicóloga, Dra. Marta. A solução para cada problema.

À Dra. Armanda, pelas conversas que também sabem a terapia.

À Professora Rute, pela disponibilidade quase imediata.

E à minha avó Luísa, que sei que me acompanha sempre…

Obrigada por tornarem isto possível.

Notas de leitura

De notar que, não raras vezes referir-nos-emos ao branqueamento de capitais como BCFT, embora o conceito de Financiamento ao Terrorismo não se aplique a todas as realidades relacionadas com o Branqueamento de Capitais passaremos, tal como o legislador, a tratar os dois conceitos em conjunto.

As abreviaturas encontram-se devidamente identificadas no índice de abreviaturas, presente no início do relatório.

Na bibliografia é possível encontrar as referências completas de todas as obras citadas, não só o autor e o título, como o local, a editora, ano de publicação e ISBN, entre outras informações conforme o caso. As páginas consultadas são indicadas nas notas de rodapé.

Quanto à colocação das notas de rodapé, cumpre esclarecer que, sempre que estas se refiram exclusivamente à última frase, serão inseridas antes do ponto final; no entanto, se se aplicarem a todo o parágrafo, serão colocadas após o ponto final, de modo a abranger a totalidade do conteúdo referido.

Este relatório de estágio encontra-se redigido conforme o Novo Acordo Ortográfico da Língua Portuguesa, que entrou em vigor a 13 de maio de 2009, excetuando os títulos de obras citadas e citações diretas que tenham sido escritas em conformidade com o acordo anterior.

Lista de abreviaturas

- AML – *Anti-Money Laundering*
- AMLA - *Anti-Money Laundering Authority*
- ANR – Avaliação Nacional de Risco
- Art. – artigo
- BCE – Banco Central Europeu
- BdP – Banco de Portugal
- BCFT – Branqueamento de Capitais e Financiamento ao Terrorismo
- BTC – *Bitcoin*
- CDD – *Customer Due Diligence*
- CCPPCBCFT – Comissão de Coordenação das Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo
- Cfr. – conforme
- CP – Código Penal
- CPP – Código de Processo Penal
- DCIAP - Departamento Central de Investigação e Ação Penal
- EBA – *European Banking Authority*
- ESMA - *European Securities and Markets Authority*
- EUA – Estados Unidos da América
- FBI – *Federal Bureau of Investigation*
- FDUL – Faculdade de Direito da Universidade de Lisbo
- FinCEN – *Financial Crimes Enforcement Network*
- FSA – *Financial Services Agency*
- GAFI / FAFT – Grupo de Ação Financeira Internacional / *Financial Action Task Force*
- ICO – *Initial Coin Offer*
- ITO – *Initial Token Offer*
- KYC – *Know Your Customer*
- LBCFT – "Lei do Branqueamento de Capitais e Financiamento ao Terrorismo" – Lei n.º 83/2017, de 18 de agosto

- N.º - Número
- NFT's – *Non Fungible Tokens*
- OCDE – Organização para a Cooperação e Desenvolvimento Económico
- ONU – Organização das Nações Unidas
- p. – página/páginas
- PBCFT – Prevenção de Branqueamento de Capitais e Financiamento ao Terrorismo
- PEP – *Politically Exposed Person*
- RCBE – Registo Central do Beneficiário Efetivo
- TIN – *Tax Identification Number*
- UIF – Unidade de Informação Financeira
- UNC3T – Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica
- VASP – *Virtual Asset Service Providers*

Resumo

Este Relatório visa desenvolver o tema da Prevenção do Branqueamento de Capitais e do Financiamento ao Terrorismo (PBCFT) no contexto dos ativos virtuais, com ênfase no papel das entidades que operam com estes ativos. A investigação surge a partir de um estágio na *Luso Digital Assets* e explora a evolução do enquadramento legislativo neste domínio, à medida que se torna cada vez mais relevantes no cenário económico-financeiro global.

Dada a crescente popularidade dos ativos virtuais como meio de troca e de investimento, surgiram preocupações devido aos desafios que estes apresentam para o combate à criminalidade económica. Considerando a oportunidade que representam para a integração de ganhos ilícitos na economia, uma mudança de paradigma legislativo é necessária e urgente, com normas rigorosas e harmonizadas entre os vários Estados, de forma a mitigar esses riscos. A crescente sofisticação dos esquemas criminosos e a globalização impulsionaram esta necessidade de adaptação das normas legais, tanto a nível nacional como internacional.

Embora as criptomoedas representem inovações significativas no mercado financeiro, a sua regulamentação, concertação e monitorização eficaz são essenciais para prevenir o uso ilícito destas tecnologias e garantir a segurança e integridade do sistema económico-financeiro global.

Neste contexto, o presente trabalho examina as sucessivas alterações no panorama jurídico, aborda os principais desafios que estas tecnologias representam para o direito penal e expõe os desenvolvimentos mais recentes na regulação desta matéria, particularmente na União Europeia. Com o aparecimento deste admirável mundo novo, impõem-se deveres aos prestadores de serviços de criptoativos, deveres esses que procuraremos também analisar neste trabalho, destacando a importância da conformidade (*compliance*) e da monitorização no combate ao BCFT.

Palavras-Chaves: Branqueamento de Capitais e Financiamento ao Terrorismo; Ativos Virtuais; Regulação; *Compliance*; *Blockchain*.

Abstract

This report aims to explore the topic of Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) in the context of virtual assets, with an emphasis on the role of entities operating with these assets. The research stems from an internship at Luso Digital Assets and delves into the evolving legislative framework in this domain, as it becomes increasingly relevant in the global economic and financial landscape.

Given the growing popularity of virtual assets as a medium of exchange and investment, concerns have arisen due to the challenges they present in combating economic crime. Considering the opportunity they represent for integrating illicit gains into the economy, a paradigm shift in legislation is necessary and urgent, with strict and harmonized regulations across various states to mitigate these risks. The increasing sophistication of criminal schemes and globalization have driven the need for adaptation of legal norms, both at the national and international levels.

While cryptocurrencies represent significant innovations in the financial market, their effective regulation, coordination, and monitoring are essential to prevent the illicit use of these technologies and ensure the safety and integrity of the global economic and financial system.

In this context, this report examines the successive changes in the legal landscape and addresses the main challenges these technologies pose to criminal law, as well as the most recent developments in regulation, particularly within the European Union. With the emergence of this brave new world, obligations are imposed on crypto-asset service providers, obligations that we will also examine in this work, highlighting the importance of compliance and monitoring in combating AML/CTF.

Keywords: Anti-Money Laundering and Counter-Terrorist Financing; Virtual Assets; Regulation; Compliance; Blockchain.

Índice

Introdução

A Faculdade de Direito da Universidade de Lisboa passou a permitir a substituição da Dissertação de Mestrado por um Relatório de Estágio, tendo-se preferido esta opção por representar uma oportunidade para adquirir experiência profissional, aprender na prática o funcionamento de certas entidades, aprofundar conhecimentos sobre o seu domínio de atuação, permitir a consolidação de matérias lecionadas e, ainda, a aprendizagem de outras que, por qualquer motivo, não foram abordadas.

Visando este objetivo procurou-se realizar o estágio numa entidade com uma atividade inovadora e, portanto, com maior margem para aprendizagem. Para a concretização do estágio, escolheu-se a *Luso Digital Assets*, uma entidade que exerce atividade com ativos virtuais (os chamados *Virtual Asset Service Providers* – VASP).

Contudo, enveredar numa temática tão recente e arrojada, acarreta igualmente os seus riscos, pois além de consubstanciar uma matéria que não é devidamente aprofundada nas unidades curriculares, é também um tema pouco desenvolvido doutrinalmente. O surgimento e a rápida expansão dos ativos virtuais não foram acompanhados, do ponto de vista legislativo, por soluções consistentes e consensuais. Até ter sido definido um quadro normativo para as atividades com ativos virtuais e se ter constatado o uso dos mesmos para branquear capitais e financiar o terrorismo, havia uma lacuna a ser explorada no regime jurídico da PBCFT. Ainda hoje, uma das principais críticas apontadas reside na questão de as soluções indicadas pelo legislador português não parecerem ser as mais adequadas para lidar com esta nova realidade.

Adicionalmente, o problema que nos propomos abordar mostra-se particularmente desafiante e premente, considerando não só a novidade e a complexidade dos ativos virtuais, mas também o facto de essas exigências reclamarem uma resposta por parte da comunidade jurídica, resposta essa que nos parece insuficiente.

É indiscutível o avanço tecnológico que se tem verificado nos últimos anos e a passagem das nossas vidas para o mundo digital. Cada vez mais, a vida quotidiana passa pelo uso das novas tecnologias e, consequentemente, mais

crimes são cometidos neste meio. Com este avanço, vieram também novos desafios e a necessidade de uma adaptação do sistema jurídico ao ciberespaço.

Juntando esta passagem da sociedade para o mundo digital, com o fenómeno da globalização, houve um aumento da cibercriminalidade e um aumento exponencial do número de situações jurídico-penais transfronteiriças e, naturalmente, novas formas de branquear capitais e financiar o terrorismo. O BCFT passou a ter um caráter eminentemente internacional revelando-se, assim, um problema à escala global.

A metodologia utilizada na elaboração deste relatório baseou-se, primordialmente, na análise legislativa e nas escassas observações doutrinais. Conscientes do desafio que é descrever com simplicidade um fenómeno complexo, tentaremos compreender o papel das entidades que exercem atividade com ativos virtuais, sem negligenciar a extensão que uma investigação sempre requer.

Passaremos ainda em revista as obrigações de registo das entidades que pretendam exercer atividades com ativos virtuais junto do Banco de Portugal e os deveres a que estas entidades estão obrigadas. Referir-nos-emos também à baixa taxa de reporte de operações suspeitas destas à UIF (Unidade de Informação Financeira) e ainda a alguns ativos virtuais que podem ser potencialmente usados em esquemas de BCFT, como os NFT's (*Non Fungible Tokens*). Analisaremos também a facilidade de criação e uso de novos ativos virtuais, o anonimato de algumas transações que a tecnologia *blockchain* ainda permite, entre outras situações que agravam o risco de BCFT.

Deste modo, partiremos de uma análise dos conceitos mais importantes, para então de seguida aferir de que forma é que estas entidades podem intervir com o objetivo de travar o BCFT. Numa primeira análise, veremos quais as técnicas utilizadas para branquear capitais e financiar o terrorismo. A partir daí será possível atuar na prevenção e estudar de que forma estão as VASP a contribuir para evitar a prática destes crimes, nomeadamente através de deveres preventivos.

Capítulo I – Conceptualização

1. Branqueamento de Capitais

Ainda que este relatório vise averiguar o papel que desempenham as entidades que exercem atividade com ativos virtuais na prevenção do Branqueamento de Capitais, é essencial definir e fazer um enquadramento legal deste crime.

Nos últimos anos, a doutrina tem apontado várias conceções para definir o crime de Branqueamento de Capitais, seguindo-se alguns exemplos.

NUNO BRANDÃO[1] define o branqueamento de capitais como "a actividade pela qual se procura dissimular a origem criminosa de bens ou produtos, procurando dar-lhes uma aparência legal".

Já VITALINO CANAS[2] realça que o crime de branqueamento é "mais do que um acto isolado e localizado", mas "uma sucessão de actos que configuram uma sequência ou processo [relativamente difuso] tendente a um certo objetivo". Esse objetivo será a "utilização lícita de bens ou produtos obtidos através da prática de factos ilícitos típicos", recorrendo, para isso, a um "processo de progressiva ocultação". Acrescenta ainda que o conceito não é feliz, pois também "não têm de ser obrigatoriamente *dinheiro* ou *capitais*". Para ele, seria mais apropriado se a nomenclatura deste tipo legal fosse algo como "dissimulação da proveniência ilícita de bens e produtos".

Similarmente, JORGE ALEXANDRE FERNANDES GODINHO[3] diz que o branqueamento de capitais não é legalmente descrito "como um conjunto mais ou menos circunscrito de condutas concretas mas sim, mais ampla e genericamente". Define-o como "um processo destinado a um certo fim, a ocultação ou dissimulação de um conjunto de características de bens de origem

[1] BRANDÃO, Nuno - Branqueamento de Capitais: O Sistema Comunitário de Prevenção, p. 15.
[2] CANAS, Vitalino - O Crime de Branqueamento: Regime de Prevenção e de Repressão, p. 13 e 21.
[3] GODINHO, Jorge Alexandre Fernandes - Do crime de «Branqueamento» de Capitais: Introdução e Tipicidade, p. 13.

ilícita (origem, localização, disposição, movimentação, propriedade), pelo que a casuística do branqueamento de capitais é inesgotável".

No ordenamento jurídico português, o crime de branqueamento de capitais encontra-se tipificado no artigo 368º-A do Código Penal. Este artigo está inserido no Capítulo III, referente aos crimes contra a realização da justiça.

De forma concisa, podemos afirmar que o crime de branqueamento consiste na conversão, transferência, auxílio ou facilitação de alguma operação de conversão ou transferência de vantagens, obtidas por si ou por terceiro, direta ou indiretamente, provenientes da prática de um determinado conjunto de ilícitos criminais (também designados de *crimes precedentes*), com o objetivo de dissimular a proveniência ilícita dessas vantagens, ou de evitar que o autor ou participante dessas infrações seja criminalmente perseguido ou submetido a uma reação criminal. Também é considerado como crime de branqueamento, a ocultação ou dissimulação da verdadeira natureza, origem, localização, disposição, movimentação ou titularidade das vantagens provenientes da prática de crimes precedentes, ou dos correspondentes direitos[4].

Constatamos que o legislador considera como "vantagens" os bens provenientes da prática de qualquer facto ilícito típico punível com pena de prisão de duração mínima superior a seis meses ou de duração máxima superior a cinco anos.

De seguida, elenca uma série de crimes em que, independentemente das penas aplicáveis, também se consideram vantagens os bens provenientes da sua prática. A tipificação penal do branqueamento de bens ou produtos pressupõe que estes resultem de comportamentos ilícitos, também estes puníveis criminalmente.[5]

Isto significa que, para haver branqueamento de capitais, tem de haver um crime anterior que proporcionou ao seu autor proventos ilícitos (ou também quem as detiver ou utilizar com conhecimento dessa qualidade), que

[4] RODRIGUES, André Alfar – Manual de Inovação Financeira: Uma Introdução ao Universo das Criptomoedas e da Blockchain, p. 165.
[5] CANAS, Vitalino - «Branqueamento de Capitais»: Noções elementares do regime jurídico de prevenção e repressão e evolução previsível, p. 212.

posteriormente ele, ou outrem, pretendessem camuflar, para que pareça que resultam de atividade lícitas.

A este respeito, o Tribunal da Relação de Lisboa referiu que o crime de branqueamento supõe o desenvolvimento de atividades que, podendo integrar várias fases, visam dar uma aparência de origem legal a bens com origem ilícita, encobrindo assim a sua verdadeira origem. Isto conduzirá, na maior parte das situações, a um aumento de valores que não é comunicado às autoridades legítimas[6].

Foi ainda referido pelo Tribunal da Relação que "*sem um crime precedente como tal previsto à data da transferência do capital, não há crime de branqueamento. A punição do branqueamento visa tutelar a "pretensão estadual ao confisco das vantagens do crime", ou mais especificamente, o interesse do aparelho judiciário na deteção e perda das vantagens de certos crimes". Quanto mais eficiente e sofisticada for a conduta de branqueamento mais grave e perigoso é o atentado ao bem jurídico protegido com esta incriminação. Porém, mesmo a simples conduta do agente de apenas depositar na sua conta bancária quantias monetárias provenientes do crime precedente por si cometido, pode integrar a prática do crime de branqueamento*"[7].

O Tribunal da Relação de Lisboa também entendeu que o branqueamento de capitais é um crime de mera atividade e de perigo, que se verifica com a simples execução de um dos comportamentos típicos, independentemente do seu resultado. Trata-se de um crime de perigo (e não de um crime de dano), uma vez que pode não haver uma lesão efetiva do bem jurídico protegido, bastando a existência do perigo dessa lesão. Este é também um crime de perigo abstrato, na medida em que não se exige, caso a caso, a verificação de perigo real para o bem jurídico protegido. Por último, é um crime de mera atividade (em contraposição a um crime de resultado), dado que a tentativa de branqueamento é punível.

[6] RODRIGUES, André Alfar – Manual de Inovação Financeira: Uma Introdução ao Universo das Criptomoedas e da Blockchain, p. 165.
[7] Acórdão do Tribunal da Relação de Lisboa, de 18.07.2013, Processo n.º 1/05.2JFL-SB.L1-3, Relator: Rui Gonçalves.

Noutro acórdão mais recente, o Tribunal da Relação de Lisboa proferiu o seguinte: "*O crime de branqueamento de capitais, tanto na modalidade tipificada no nº 2, como na modalidade prevista no nº 3 do art. 368º A do CP, é um crime de intenção que exige o dolo específico, traduzido no propósito, ou melhor, dois propósitos (os quais podem ser cumulativos ou alternativos), que acrescem à consciência e vontade relativa aos elementos objetivos do crime – o agente tem de atuar com o fim de dissimular a origem ilícita das vantagens em causa, ou com o fim de evitar que o autor ou participante das infrações subjacentes seja criminalmente perseguido ou submetido a uma reação criminal*"[8].

Relativamente ao nº 3, importa ressalvar que a *conversão* é a "alteração da natureza e configuração dos bens gerados ou adquiridos com a prática do facto ilícito típico subjacente". Por outro lado, a *transferência* consubstancia a "deslocação física dos bens, quer na alteração jurídica ao nível da titularidade ou do domínio"[9].

Importa referir que a alínea j) do n.º 1 do artigo 2º da LBCFT, define o branqueamento de capitais como "as condutas previstas e punidas pelo artigo 368º-A do Código Penal", mas acrescenta ainda a participação num dos atos a que se refere esse artigo, especificando que também se considera branqueamento de capitais "a associação para praticar o referido ato, a tentativa e a cumplicidade na sua prática, bem como o facto de facilitar a sua execução ou de aconselhar alguém a praticá-lo".

Note-se que, até 2002, o método que vigorou era o da delimitação de crimes subjacentes ao branqueamento, o método do catálogo. Havia, portanto, uma lista fechada de crimes subjacentes expressamente designados na lei e, com a Lei n.º 10/2002, de 11 de fevereiro, passou a vigorar um método misto de catálogo e cláusula geral: por um lado, uma lista e, por outro, uma cláusula geral através da qual, com referência a uma moldura penal, se definem mais alguns crimes subjacentes ao branqueamento[10]. Sendo este o método utilizado pelo legislador

[8] Acórdão do Tribunal da Relação de Lisboa, de 30.10.2019, Processo n.º 405/14.0TELSB.L1-3, Relator: Cristina Almeida e Sousa.
[9] CANAS, Vitalino - O Crime de Branqueamento: Regime de Prevenção e de Repressão, p. 159.
[10] CANAS, Vitalino - O Crime de Branqueamento: Regime de Prevenção e de Repressão. p. 42 e 43.

e o que se mantém até hoje é, a nosso ver, o mais adequado, porque abre o leque a outros crimes que, à partida, não entrariam no catálogo.

Relativamente à expressão "branqueamento de capitais", importa referir que esta é equivalente a "lavagem de dinheiro", expressão mais utilizada no Brasil, mas que se refere à mesma situação. O termo "branqueamento de capitais" provém da expressão francesa "*blanchiment d'argent*" e é o termo mais utilizado em Portugal, pois foi o vocábulo adotado na nossa legislação e, só por esse motivo, será a expressão usada neste trabalho, pese embora possa ter conotações racistas, uma vez que equivale a dizer que os capitais "bons" são os "brancos" e os capitais "maus" são os "não-brancos". Por outro lado, a expressão "lavagem de dinheiro" é associada à imagem das "lavandarias de dinheiro"[11] como lojas ou negócios, com lucros difíceis de verificar, em que é fácil "misturar" dinheiro proveniente da prática de crimes com os lucros da própria empresa. Contudo, a ideia de "branqueamento" ou de "lavagem" é a mesma, que é dar uma aparência lícita aos vários capitais através de alguma atuação que permita "lavar" ou "branquear" dinheiro "sujo" que resultou de uma atuação ilícita anterior[12].

Retomando a questão das fases pelas quais passa o branqueamento de capitais, importa atentar que, a primeira fase, à qual foi atribuída a designação de **colocação** (ou *placement stage*), consiste na introdução dos capitais nos circuitos financeiros e não financeiros, seja através de, por exemplo, depósitos em instituições financeiras, compra de ativos, investimentos em imóveis, joias e atividades lucrativas ou transferências para contas em jurisdições com leis mais permissivas. Trata-se, geralmente, de grandes quantias em numerário, por isso o branqueador está mais preocupado em desfazer-se do papel-moeda, convertendo-o noutra forma mais facilmente manuseável. O caso mais

[11] A respeito das "lavandarias de dinheiro" importa esclarecer que o contexto do branqueamento de capitais surgiu nos EUA, sobretudo com o esquema das lavandarias automáticas, utilizado por grupos criminosos e mafiosos. Estas lavandarias eram empresas de fachada que permitiam às organizações criminosas efetuar depósitos bancários de notas de baixo valor, que simulavam os lucros resultantes das lavandarias. Na verdade, os montantes que eram depositados eram fruto do comércio de bebidas alcoólicas proibido pela Lei Seca e de outras atividades criminosas que eram praticadas por estas organizações, como o jogo ou a prostituição, cfr. RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 141.

[12] MACHADO, Miguel da Câmara – "Contexto, evolução e tendências do *compliance* em Portugal e na Europa, em especial a partir do Aviso n.º 3/2020, de 15 de julho, do Banco de Portugal" *in* "Estudos sobre *Law Enforcement*, *Compliance* e Responsabilidade Empresarial", p. 177-179.

paradigmático é o dos volumes de notas resultantes do tráfico de droga. Esta fase inicial é a mais vulnerável e detetável pelas autoridades de investigação e fiscalização. Por esse motivo, é frequente os detentores de capitais de origem ilícita introduzirem os montantes nos circuitos de forma fragmentada, para evitar o "*paper trail*", ou seja, o rasto documental que possa revelar a origem dos fundos. Além disso, atualmente, é cada vez menos frequente a liquidação de transações com papel-moeda, sendo cada vez mais suspeita a utilização de largos volumes em numerário. Neste sentido, a recomendação n.º 25 do GAFI sugere aos Estados que estimulem a utilização de outros meios de pagamento, já que, em princípio, todos eles deixam um "*paper trail*" que permitirá reconstituir as transações efetuadas quando necessário[13] e a Lei n.º 92/2017 de 22 de agosto, que proíbe o pagamento em numerário para transações que envolvam montantes iguais ou superiores a 3.000 euros.

A segunda fase, conhecida como a fase da **transformação**, da **circulação**, da **camuflagem** ou da **dissimulação** (ou *layering stage*) ocorre quando se realizam as operações necessárias para ocultar a proveniência criminosa dos capitais. Nesta etapa, é comum a realização de várias transações financeiras consecutivas, com o objetivo de criar "camadas" (ou *layers*) entre a origem real dos proveitos obtidos com as atividades ilícitas e a que se pretende visível. Esta fase visa movimentar os proveitos da prática do crime o máximo possível, distanciando-os da sua origem criminosa e tornando quase impossível identificar o rasto. Muitas vezes, os capitais são objeto de múltiplas e repetidas operações e são feitas transferências de fundos para contas bancárias anónimas ou pertencentes a entidades anónimas[14], com esse propósito de eliminar qualquer vestígio sobre a sua proveniência e propriedade. São igualmente comuns as compras e vendas de ativos em diferentes jurisdições e o uso de empresas de fachada. O objetivo é interromper o "*paper trail*" e, portanto, o conjunto de elementos documentais que permitem a reconstrução dos movimentos efetuados.

[13] GODINHO, Jorge Alexandre Fernandes – Do crime de «Branqueamento» de Capitais: Introdução e Tipicidade, p. 13.

[14] Esta situação acontece, designadamente, em jurisdições que de alguma forma facilitem o processo, seja pela admissão de contas bancárias anónimas, pelo facto do branqueamento de capitais não ser criminalizado ou por falta de controlo das autoridades. Por isto se afirma que o branqueamento de capitais é feito, grande parte das vezes, através de vários sistemas jurídicos.

Por último, a terceira fase, da **integração** (ou *integration stage*), consiste na reintrodução dos capitais já branqueados nos circuitos económicos e financeiros legítimos, de forma aparentemente legal. Após o branqueamento, esses capitais podem ser investidos nas mesmas ou em outras atividades ilícitas, mas também em atividades plenamente lícitas, nomeadamente através de depósitos em contas bancárias ou na aquisição de bens, como imóveis, valores mobiliários, ativos virtuais e metais preciosos, numa perspetiva já de longo prazo. Já não se trata de dissimular a origem dos fundos, mas sim de os fazer "reaparecer" no circuito económico, sob um manto de licitude e de forma visível, designadamente ao fisco.

Tanto VITALINO CANAS como JORGE ALEXANDRE FERNANDES GODINHO consideram que esta última fase já não integra o processo de branqueamento de capitais, uma vez que já não está em causa a dissimulação da origem, os capitais já estão camuflados e prontos para um uso de natureza lícita.

Para estes autores, o branqueamento de capitais poderá corresponder sim às duas primeiras fases, mas mais concretamente à segunda. Não obstante, importa ressalvar que qualquer uma destas três fases pode assumir inúmeras expressões concretas ou não se verificar, de todo, em certos casos. Atualmente, o branqueamento de capitais é uma atividade que pode atingir um grau de sofisticação tal, que só artificialmente se pode reduzir a um esquema único e linear. VITALINO CANAS defende, por isso, uma reavaliação a este modelo descritivo tradicional das três fases com a configuração apresentada[15].

Há ainda quem defenda que, no processo de branqueamento de capitais, só a partida é perfeitamente identificável, não o ponto final, cuja finalidade não consiste apenas em ocultar ou dissimular a origem ilícita dos bens, mas também em conseguir que eles, já "lavados", possam ser utilizados na economia legal[16].

Num Acórdão do Tribunal da Relação de Lisboa pode ler-se que "*face à amplitude da configuração do crime de branqueamento de capitais no art. 368º*

[15] CANAS, Vitalino – O Crime de Branqueamento: Regime de Prevenção e de Repressão, p. 22.
[16] MELO, Júlio César Machado Ferreira de – Crime organizado e delação premiada: com as alterações do pacote anticrime (Lei 13.964/2019), p. 53.

A do CP, deve entender-se que o processo trifásico – conversão; dissimulação e integração – de reciclagem dos bens ou vantagens patrimoniais resultantes de factos típicos e ilícitos das espécies previstas no seu n.º 1 pode ser mais ou menos elaborado, consoante a economia de esforço necessária à produção do resultado antijurídico, pelo que a mera introdução de dinheiro proveniente da prática de crimes base, ou da venda de bens obtidos através do cometimento desses tipos de ilícito, por exemplo, através de um mero depósito bancário, ainda que menos grave e perigosa do que outras mais sofisticadas e engenhosas, é já branqueamento de capitais, sob pena de restrição ilegal do âmbito objetivo do tipo e de desarticulação funcional com o bem jurídico tutelado com a incriminação."[17]

Assim, e seguindo a mesma linha de raciocínio de SARAGOÇA DA MATA[18], o ideal seria a atuação imediata das instituições que recebem os capitais quando estes são introduzidos nos circuitos, para que todo o processo de branqueamento se esgote na fase da colocação. Isto é, no fundo, o que se pretende que façam as entidades que exercem atividade com ativos virtuais, que detetem a intenção de BCFT na primeira fase e, denunciando-as imediatamente, impossibilitem a sua concretização. Veremos como é que este processo decorre utilizando criptoativos adiante.

[17] Acórdão do Tribunal da Relação de Lisboa, de 30.10.2019, Processo n.º 405/14.0TELSB.L1-3, Relator: Cristina Almeida e Sousa.
[18] MATA, Paulo Saragoça da – Política e corrupção: branqueamento e enriquecimento, p. 126.

2. Compliance

O termo *compliance* advém da expressão "to *comply*", que se traduz na adoção de um comportamento conforme uma determinada norma, comando ou instrução, ou seja, conformidade perante o Direito vigente[19].

Também designado por cumprimento normativo, o *compliance* ganhou uma maior visibilidade desde que as empresas começaram a adotar programas corporativos de prevenção de ilícitos, no sentido de diminuir os riscos de responsabilização das sociedades comerciais e dos respetivos dirigentes nos âmbitos civil, contraordenacional e criminal. Inicialmente, o cumprimento normativo consistia numa autorregulação voluntária (*voluntary self-regulation*), passando mais tarde para uma autorregulação regulada ou imposta (*enforced self-regulation*). Isto significa que as empresas passaram a ser obrigadas a redigir os seus próprios programas de cumprimento normativo, os quais devem ser depois certificados por entidades devidamente acreditadas para o efeito. A autorregulação regulada impôs um crescimento exponencial dos departamentos e funções de conformidade nas empresas, embora de forma proporcional à dimensão de cada uma[20]. Na *Luso Digital Assets*, o departamento de *compliance* era composto por duas pessoas, dada a pequena dimensão da empresa.

O *compliance* visa a adoção de normas ou regulamentos internos que ajudam a mitigar não só as situações de BCFT, como a corrupção, conflitos de interesses e proteção de dados pessoais[21], sendo a matéria da PBCFT a área universalmente mais regulada ao nível da imposição de deveres preventivos, a todas as entidades sujeitas, tanto financeiras como não financeiras[22].

Um dos desafios do cumprimento normativo é visar especificamente a PBCFT, pois é natural a tendência dos departamentos de *compliance* em apostar na isenção de responsabilidades empresariais e em evitar eventuais sanções.

---

[19] RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 15 e 23.
[20] MENDES, Paulo de Sousa – "Regulação responsiva, autorregulação regulada e responsabilidade empresarial" *in* "Estudos sobre *Law Enforcement*, *Compliance* e Responsabilidade Empresarial", p. 9 e ss.
[21] RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 17 e 22.
[22] MENDES, Paulo de Sousa – "Regulação responsiva, autorregulação regulada e responsabilidade empresarial" *in* "Estudos sobre *Law Enforcement*, *Compliance* e Responsabilidade Empresarial", p. 29.

Sendo o foco deste trabalho a PBCFT, não poderíamos deixar de mencionar este problema e, tal como PAULO DE SOUSA MENDES[23], reconhecemos o risco de tornar os programas de conformidade "meros estratagemas de encobrimento das más práticas das empresas".

Outro desafio é precisamente medir a eficácia destes programas de *compliance*, isto é, determinar indicadores objetivos da probabilidade (já que é impossível garantir a sua efetividade, sem falhas) de que o programa em questão poderá ajudar a prevenir o BCFT. Esta tarefa afigura-se particularmente complicada, senão impossível[24] o que, por si só, já é elucidativo da complexidade do problema que aqui nos propomos tratar.

De facto, conforme realça MIGUEL DA CÂMARA MACHADO[25], podemos mesmo "estar a falar de um combate com pouca ou nenhuma efetividade". O autor refere ainda que os poucos estudos que têm sido possíveis quanto à proveniência dos capitais têm apontado para que a grande maioria do capital que entra nos mercados com origem ilícita não é detetada.

Na *The Economist*, têm sido publicados vários textos que descrevem esta luta como meramente simbólica, dizendo que podemos estar efetivamente a desviar os esforços de investigação para os lugares errados e que o sistema global para o combate a crimes financeiros, além de excessivamente dispendioso, é ineficaz[26].

É porque, vejamos, não basta que os programas de *compliance* estejam "bem desenhados", nem basta que sejam aplicados de boa-fé e com seriedade, é também preciso assegurar que estes procedimentos possam realmente ser

[23] MENDES, Paulo de Sousa – "Regulação responsiva, autorregulação regulada e responsabilidade empresarial" *in* "Estudos sobre *Law Enforcement*, *Compliance* e Responsabilidade Empresarial", p. 36.
[24] SCANDELARI, Gustavo Britta – "Certificação em *compliance*: bases e possibilidades para o exame da idoneidade do programa" *in* "Estudos sobre *Law Enforcement*, *Compliance* e Responsabilidade Empresarial", p. 99 e ss.
[25] MACHADO, Miguel da Câmara – "Deveres antibranqueamento de capitais: De onde vieram, quais são e como vão evoluir (do "4G" ao "5G")" *in* "Novos Estudos sobre *Law Enforcement*, *Compliance* e Direito Penal", p. 304 e 305.
[26] A título de exemplo, v., https://www.economist.com/special-report/2005/10/20/looking-in-the-wrong-places [consultado em: 12.04.2024] e, mais recente, https://www.economist.com/finance-and-economics/2021/04/12/the-war-against-money-laundering-is-being-lost [consultado em: 12.04.2024].

utilizados na prática[27]. Parece-nos que esta aplicabilidade prática é o mais difícil de garantir e, por este motivo, é muitas vezes um grande entrave do *compliance* das organizações.

Importa referir que estas preocupações com *compliance* em Portugal apareceram muito associadas à banca, aos mercados financeiros e aos seguros, o que se explica pelo impulso internacional do combate ao BCFT, mas não é um exclusivo destes setores. Atualmente, o *compliance* é, cada vez mais, uma preocupação que todas as empresas têm de ter, independentemente do setor em que atuam, interessando a todas as atividades reguladas e supervisionadas[28].

As empresas têm de ser responsáveis pelo cumprimento das leis, regras e regulamentos que sejam aplicáveis à sua atividade, o que deverá ser assegurado por pessoas que podem, ou não, ser juristas. Tem-se verificado uma tendência, cada vez maior, por parte das empresas na alocação de custos com *compliance*. Este aumento significativo deve-se à complexificação dos sistemas internos de controlo, mas também à previsão de elevadas coimas que sancionam o incumprimento dos normativos aplicáveis. Assim, os custos aumentaram para permitir a implementação de estruturas que acompanhem o controlo e o *compliance* exigido às empresas e a tendência é a de que continuem a aumentar, de modo a acompanhar as exigências jurídicas cada vez maiores[29].

As exigências jurídicas são cada vez maiores também porque a legislação referente a BCFT está cada vez mais complexa e aumentou consideravelmente, o que obriga o *compliance* a estar permanentemente a adaptar-se aos novos desafios de uma economia em constante mudança, reforçando os seus sistemas de controlo interno de forma a evitarem consequências, tanto para as próprias empresas, como para o tecido empresarial e o mercado[30]. A não adoção de políticas de *compliance* pode levar a entidade a sofrer prejuízos graves, como

[27] RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 58.
[28] MACHADO, Miguel da Câmara – "Contexto, evolução e tendências do *compliance* em Portugal e na Europa, em especial a partir do Aviso n.º 3/2020, de 15 de julho, do Banco de Portugal" *in* "Estudos sobre *Law Enforcement*, *Compliance* e Responsabilidade Empresarial", p. 178.
[29] *Idem*, p. 179.
[30] RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 15-17.

processos judiciais, contraordenacionais e lesões na sua imagem e reputação, colocando em risco a sua sobrevivência[31].

[31] RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 21-22.

3. Financiamento ao Terrorismo

Por outro lado, o financiamento ao terrorismo tornou-se uma preocupação mundial devido aos ataques terroristas do 11 de setembro de 2001 e foi desde então que os governos começaram a procurar prevenir os sistemas de financiamento das organizações terroristas[32].

Também o GAFI, em outubro de 2001, se juntou ao esforço legislativo mundial e editou oito Recomendações Especiais sobre financiamento ao terrorismo (a que, após 2012, se veio a juntar a nona). A partir deste momento, as "40 + 9" Recomendações do GAFI começaram a ser entendidas como um conjunto único de medidas para enfrentar tanto o branqueamento quanto o financiamento do terrorismo (e a não proliferação de armas de destruição maciça)[33].

De acordo com o artigo 2.º da Lei n.º 52/2003, de 22 de agosto considera-se grupo terrorista a associação de duas ou mais pessoas que, atuando concertadamente, visem cometer infrações terroristas. São infrações terroristas os atos que, podendo afetar gravemente as instituições do Estado, um Estado estrangeiro ou uma organização internacional, são praticados com o objetivo de intimidar certas pessoas, grupos de pessoas ou a população em geral ou compelir de forma indevida os poderes públicos a praticar um ato ou a abster-se de o praticar.

O artigo 2.º da LBCFT define o Financiamento ao Terrorismo como "as condutas previstas e punidas pelo artigo 5.º-A da Lei n.º 52/2003, de 22 de agosto, lei de combate ao terrorismo", remetendo a definição para este artigo que diz "Quem, por quaisquer meios, direta ou indiretamente, fornecer, recolher ou detiver fundos, com a intenção de que sejam usados ou sabendo que podem ser usados, total ou parcialmente, para planear, preparar, praticar ou contribuir para a prática de infrações terrorista (…) é punido com pena de prisão de 8 a 15 anos".

O financiamento ao terrorismo, também de acordo com a Convenção Internacional para a Eliminação do Financiamento do Terrorismo (adotada em

[32] RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 141.
[33] NUNES, Carlos Casimiro – O Ministério Público na prevenção do branqueamento e do financiamento do terrorismo, p. 103.

Nova Iorque a 9 de Dezembro de 1999), consiste no fornecimento ou na recolha de fundos, por quaisquer meios, direta ou indiretamente, com a intenção de serem utilizados ou sabendo que serão utilizados, total ou parcialmente, tendo em vista a prática de atos terroristas ou de qualquer outro ato destinado a causar a morte ou ferimentos corporais graves num civil ou em qualquer pessoa que não participe diretamente nas hostilidades numa situação de conflito armado, sempre que o objetivo desse ato, devido à sua natureza ou contexto, vise intimidar uma população ou obrigar um governo ou uma organização internacional a praticar ou a abster-se de praticar qualquer ato.

No financiamento do terrorismo um dos propósitos primários dos financiadores é a ocultação da finalidade a que os fundos se destinam, sendo que, frequentemente, os montantes envolvidos são relativamente baixos ou mesmo de origem lícita, o que torna mais difícil a sua deteção.

A prevenção do Financiamento ao Terrorismo geralmente vem articulada com o quadro preventivo do Branqueamento de Capitais tendo, porém, sido adotadas medidas legislativas que facilitam especificamente a deteção, a prevenção e a supressão do financiamento do terrorismo, reduzindo as possibilidades de acesso ao sistema financeiro internacional dos autores de atos de terrorismo, de organizações e grupos terroristas e dos seus financiadores.

Incluem-se nessas medidas o congelamento e a perda de bens pertencentes a autores de atos de terrorismo e a quem apoie e financie grupos e organizações terroristas, o dever de comunicação de transações suspeitas de terem algum tipo de conexão com o terrorismo, o reforço dos deveres de PBCFT (em especial do dever de identificação) no âmbito das operações de transferência de fundos e a criminalização do financiamento do terrorismo.

Tal como sucede no caso do branqueamento de capitais, também o financiamento do terrorismo é caracterizado por 3 fases distintas:

- Colocação dos fundos (lícitos ou ilícitos) no sistema financeiro;
- Circulação dos fundos para dissimular a finalidade e os destinatários dos mesmos;
- Armazenamento ou transferência dos fundos para organizações terroristas ou indivíduos terroristas.

Uma vez que a sobrevivência das organizações terroristas depende da sua capacidade de financiamento, afigura-se essencial interromper os fluxos de fundos para o financiamento destes grupos ou organizações terroristas.

A ameaça do financiamento ao terrorismo implica o risco de os fundos e outros ativos destinados aos terroristas serem angariados, movimentados, armazenados ou utilizados num sistema jurídico ou através dele. As vulnerabilidades do sistema podem permitir que estas atividades não sejam detetadas, o que traz consequências a vários níveis. A compreensão do ambiente de ameaça e das vulnerabilidades do sistema pode facilitar a deteção e a interrupção do financiamento ao terrorismo. Por esse motivo, consideramos particularmente importante a colaboração permanente entre as autoridades dos diferentes países tanto para a deteção, como para a avaliação dos riscos do financiamento ao terrorismo transfronteiriço.

4. Ativos virtuais, Tecnologia *Blockchain* e *Know Your Costumer (KYC)*

Antes do regime monetário internacional atual, vigorava o padrão-ouro, segundo o qual o dinheiro tinha um valor intrínseco, associado ao material utilizado na sua produção, nomeadamente o ouro ou a prata. Ao padrão-ouro seguiu-se a generalização da moeda fiduciária, como as moedas e as notas, as quais não têm um valor intrínseco, mas sim um valor determinado por um governo ou uma autoridade central, como é o caso do Banco de Portugal. São ambas moedas físicas, ao contrário das moedas virtuais[34].

Ativos virtuais é a nomenclatura escolhida pelo legislador português e, por isso, será a nossa escolha primordial, embora também se possa falar em criptoativos, criptomoedas ou moedas virtuais.

O termo "criptomoeda" foi criado da aglutinação das palavras criptografia e moeda, uma vez que as criptomoedas utilizam várias técnicas criptográficas para realizar transações entre usuários. Uma criptomoeda é uma forma de dinheiro digital que permite a transferência de valores num ambiente digital. A sua principal função é atuar como um sistema de dinheiro eletrónico que não é detido por nenhuma instituição ou organização[35].

Na apresentação do Orçamento de Estado para 2023 foi consagrada a definição de "criptoativo" como "toda a representação digital de valor ou direitos que possa ser transferida ou armazenada eletronicamente recorrendo à tecnologia de registo distribuído ou outro semelhante".

Não obstante, o termo «ativo virtual» vem definido na alínea ll) do n.º 1 do artigo 1º da Lei n.º 83/2017, de 18 de agosto, de uma forma muito similar, como "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, valor mobiliário ou outro instrumento financeiro, mas que é aceite por pessoas singulares ou coletivas como meio de troca ou de

[34] BRITO, João Rodrigues – "Da sujeição dos *Virtual Asset Service Providers* ao Cumprimento de Deveres de Prevenção do Branqueamento de Capitais" *in* "Novos Desafios da Prova Penal", p. 371.
[35] RODRIGUES, André Alfar – Manual de Inovação Financeira: Uma Introdução ao Universo das Criptomoedas e da Blockchain, p. 36.

investimento e que pode ser transferida, armazenada e comercializada por via eletrónica". Essa "via eletrónica" é a tecnologia denominada *blockchain*.

A tecnologia *blockchain* foi criada em 2008 pelo pseudónimo Satoshi Nakamoto e, até hoje, a sua verdadeira identidade mantém-se desconhecida. Esta tecnologia foi desenvolvida e publicada através do artigo "Bitcoin: A Peer-to-Peer Electronic Cash System"[36], tendo sido utilizada pela primeira vez para a implementação da inovadora criptomoeda *Bitcoin*.

A principal função da tecnologia *blockchain* é proporcionar a realização de transações por indivíduos desconhecidos entre si, através da internet, de forma segura, direta e descentralizada, isto é, sem a interferência de um agente centralizador para a efetivação daquela transação.

Através da *blockchain* ocorre a transação de ativos virtuais, sendo regulado de forma automática através de algoritmos e registados por meio de um consenso entre os usuários da rede, que estão distribuídos por todo o mundo e que são também responsáveis por armazenar, nos seus dispositivos, uma cópia integral e atualizada da *blockchain*.

Todos os registos armazenados na *blockchain* são públicos e podem ser verificados por qualquer pessoa através da internet, embora a identidade dos autores desses registos e de todos os membros da rede esteja preservada através de pseudónimos. Contudo, a necessidade de uma entidade centralizadora e reguladora é substituída pela confiança incorporada nas diversas tecnologias da *blockchain*, pois é possível a verificação dessas transações por qualquer pessoa, bem como o acesso a todas as informações armazenadas.

Por este motivo, considera-se a tecnologia *blockchain* uma alternativa tecnicamente mais eficaz e confiável[37] de coleta e armazenamento de evidências disponíveis na internet e discute-se, inclusivamente, os benefícios da sua

[36] Disponível e traduzido em português em https://bitcoin.org/files/bitcoin-paper/bitcoin_pt.pdf.
[37] Em comparação com outros tipos de provas tradicionais, como o certificado de facto e o *print screen*. A confiabilidade da tecnologia *blockchain* advém, principalmente, da impossibilidade de interferência humana durante a cópia das informações disponíveis no *website* e do facto de armazenar o conteúdo de forma inalterável.

utilização como prova em processo penal[38]. De facto, a utilização da tecnologia *blockchain* como meio de coleta e armazenamento de evidências eletrónicas já é uma realidade na China e no estado de Vermont, nos EUA[39].

A *blockchain* funciona como um banco de dados distribuído pelos computadores em todo o mundo. Por ser altamente tolerante a uma ampla gama de falhas e por não comprometer a privacidade da informação armazenada graças à criptografia[40], a *blockchain* é capaz de armazenar a evidência eletrónica preservando a autenticidade e integridade contra alterações do seu conteúdo e acesso indevido de pessoas à informação. Esta confiabilidade somada à possibilidade da *blockchain* comportar o armazenamento de diversos tipos de informação, tornou a implementação desta tecnologia extensível a uma ampla gama de serviços. A tecnologia é utilizada não só no setor financeiro, como no registo de propriedades, proteção de propriedade intelectual, contratos inteligentes, votação eletrónica, autenticação de conteúdos WEB, entre outros[41].

Os aplicativos públicos baseados em tecnologia *blockchain* são projetados como plataformas abertas e não requerem permissão para entrar, o que significa que qualquer pessoa pode participar. Estes aplicativos tendem a oferecer uma alta transparência e forte integridade de dados e é exemplo a *Blockchain* da *Bitcoin*. Os utilizadores deste tipo de aplicações são identificados pela sua chave pública ou pelo seu endereço, o que dificulta a identificação real do utilizador. No entanto, caso os utilizadores obtenham o seu par de chaves privada e pública num serviço como o das entidades que exercem atividade com ativos virtuais, a sua identidade no mundo real pode ser facilmente encontrada, uma vez que a ideia é que estes serviços solicitem uma prova da identidade dos seus clientes

[38] Contribuiria para a celeridade e para a economia processual, uma vez que não seria necessária a realização de pareceres de especialistas para a autenticidade da evidência, nem a perícia para a confirmação do seu conteúdo.
[39] LAVRADOR, Jasmine Souto – "Benefícios da Coleta e Armazenamento de Evidências Eletrônicas Disponíveis na Internet Através da Tecnologia Blockchain em Comparação com as Provas Tradicionalmente Disponíveis aos Particulares em Portugal" *in* "Novos Desafios da Prova Penal", p. 339 a 365.
[40] O conteúdo é preservado sob a forma de código de assinatura digital, uma sequência numérica única e exclusiva, estabelecida por um algoritmo de criptografia.
[41] LAVRADOR, Jasmine Souto – "Benefícios da Coleta e Armazenamento de Evidências Eletrônicas Disponíveis na Internet Através da Tecnologia Blockchain em Comparação com as Provas Tradicionalmente Disponíveis aos Particulares em Portugal" *in* "Novos Desafios da Prova Penal", p. 339 a 365.

para cumprir o *KYC* e leis contra BCFT[42]. É o que acontece nas entidades que exercem atividade com ativos virtuais e, em particular, na *Luso Digital Assets*.

Como consequência das caraterísticas dos ativos virtuais (o caráter anónimo e a descentralização), surgiu a necessidade de se aplicar verificações de *KYC* a este universo, uma vez que as suas caraterísticas tornaram este "ecossistema financeiro" um lugar ideal para os sujeitos realizarem fraudes, branqueamento de capitais e crimes de evasão fiscal[43].

À medida que o mercado dos ativos virtuais se desenvolveu, aumentaram as preocupações com atividades ilícitas e daí surgiu a necessidade de aprimorar a segurança, não só para proteger os utilizadores como o próprio sistema financeiro. A legislação relativa aos procedimentos de identificação de cliente (*KYC*) varia de país para país, mas existe uma cooperação internacional em relação às informações básicas necessárias. Estas verificações de *KYC* afiguram-se extremamente importantes, uma vez que as transações dentro da *blockchain* têm um caráter irreversível. Os fundos podem ser roubados ou movidos para outras contas, sem qualquer possibilidade de recuperação[44].

Associado ao KYC está o CDD (*Costumer Due Diligence*), podendo definir-se o *due diligence* como a "avaliação preliminar de terceiros (*third parties*), sejam eles clientes, fornecedores ou intermediários, com a qual ou com os quais a empresa pretende contratar ou estabelecer um relacionamento"[45].

O objetivo é conhecer o potencial parceiro, desde os seus acionistas, gestão de topo, reputação e recursos económicos, para avaliar potenciais riscos de integridade da contraparte, identificar transações suspeitas e aplicar medidas de mitigação adequadas. Perfilhamos a opinião de que este momento deve ocorrer

---

[42] DUARTE, Diogo Guerreiro – "An Introduction to Blockchain Technology from a Legal Perspective and its Tensions with the GDPR", *in* "Direito e Ciberespaço – Coletânea de Artigos da Revista *Digital CyberLaw by CIJIC*", p. 437.

[43] OGUNBADEWA, Ajibola – "The Bitcoin Virtual Currency: A Safe Haven for Money Launderers?", 2013. Artigo disponível em SSRN: https://ssrn.com/abstract=2402632 or http://dx.doi.org/10.2139/ssrn.2402632 [consultado em 22.04.2024].

[44] RODRIGUES, André Alfar – Manual de Inovação Financeira: Uma Introdução ao Universo das Criptomoedas e da Blockchain, p. 158-160.

[45] FLYVBJERG, Bent – "*Quality Control and Due Diligence in Project Management: Getting Decisions Right by Taking the Outside View*" *in* "*International Journal of Project Management"*, p. 760-774. Artigo disponível em SSRN: https://ssrn.com/abstract=2229700 [consultado em 22.04.2024].

antes de se iniciar a relação comercial, mas também sempre que ocorram renovações contratuais e suspeitas fundadas de irregularidades[46].

O *due diligence* pode consistir em averiguar, por exemplo, a atividade da empresa; o país onde está sediada (a sede da empresa é um elemento muito relevante, pois podemos estar perante empresas de fachada e também porque existem países que representam, desde logo, um risco acrescido de BCFT); a morada da pessoa singular (se nos é dada uma morada verdadeira ou não); a data de constituição da empresa; o número de identificação fiscal, bem como dos gestores e administradores; o endereço da internet; o montante da transação; o volume de negócios/capacidade financeira; se estamos perante uma Pessoa Politicamente Exposta; a reputação dos acionistas e gestores; se a empresa é detida por outra, etc., sendo estes apenas alguns exemplos de medidas aplicadas pelo departamento de *compliance* da *Luso Digital Assets*.

Quanto às entidades que exercem atividades com ativos virtuais ou *Virtual Asset Service Providers* (VASP – na definição do GAFI) ou *exchangers* (na terminologia da FinCEN), importa dizer que se consideram «atividades com ativos virtuais», "qualquer uma das seguintes atividades económicas, exercidas em nome ou por conta de um cliente:

i) Serviços de troca entre ativos virtuais e moedas fiduciárias;

ii) Serviços de troca entre um ou mais ativos virtuais;

iii) Serviços por via dos quais um ativo virtual é movido de um endereço ou carteira (*wallet*) para outro (transferência de ativos virtuais);

iv) Serviços de guarda ou guarda e administração de ativos virtuais ou de instrumentos que permitam controlar, deter, armazenar ou transferir esses ativos, incluindo chaves criptográficas privadas".

Consideram-se entidades que exercem atividades com ativos virtuais, no território nacional, as seguintes pessoas ou entidades:

[46] RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 61 e 62.

- As pessoas coletivas ou entidades equiparadas a pessoas coletivas constituídas em Portugal para o exercício de atividades com ativos virtuais;
- As pessoas singulares, as pessoas coletivas ou entidades equiparadas a pessoas coletivas com domicílio ou estabelecimento em Portugal afetos ao exercício de atividades com ativos virtuais;
- As demais pessoas singulares, pessoas coletivas ou entidades equiparadas a pessoas coletivas que, em razão do exercício de atividades com ativos virtuais, estejam obrigadas a apresentar declaração de início de atividade junto da Autoridade Tributária e Aduaneira.

Estas obrigações foram trazidas pela Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que foi transposta pela Lei n.º 58/2020, de 31 de agosto.

Todas as entidades que pretendam exercer, em território nacional, atividade com ativos virtuais estão sujeitas a registo junto do BdP. O artigo 112.º-A da Lei n.º 83/2017 e o Aviso do Banco de Portugal n.º 3/2021, de 23 de abril ("Aviso n.º 3/2021") regulam esse processo de registo, bem como das alterações subsequentes aos elementos a registar.

O Banco de Portugal é, desde 2020, a autoridade nacional competente pelo registo e supervisão das entidades que pretendam exercer atividades com ativos virtuais e pela verificação do cumprimento das disposições legais e regulamentares aplicáveis às entidades registadas em matéria de PBCFT[47].

Esta competência do BdP circunscreve-se à PBCFT, não se alargando a outros domínios, de natureza prudencial, comportamental ou outra

Cumpre deixar aqui a ressalva de que as atividades com ativos virtuais dependem do registo prévio junto do BdP, incluindo nos casos em que o requerente exerça outra profissão ou atividade abrangida pela Lei n.º 83/2017 (n.º 1 do referido artigo 112.º-A).

[47] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 260.

À data de entrega do presente Relatório de Estágio, 2 de outubro de 2024, eram apenas 13 as entidades registadas, das quais 8 já se encontram a exercer atividade com ativos virtuais em Portugal[48].

Os pedidos de registo inicial e de alteração devem ser apresentados através do preenchimento de modelos específicos que constam no *site* do Banco de Portugal[49] (acompanhados da devida documentação de suporte). Estes modelos devem ser remetidos ao Banco de Portugal nos termos dos números 3 a 6 do artigo 6.º do Aviso n.º 3/2021.

Os prestadores de serviços relacionados com ativos virtuais não estavam sujeitos, até há pouco tempo, à obrigação de identificação e de comunicação de atividades suspeitas, o que facilitava a inserção de ganhos ilícitos no sistema económico-financeiro. Essa ausência de regulamentação permitia, ainda mais, dissimular transferências e usufruir do anonimato nestas plataformas.

Estão previstas sanções no caso de violação das disposições relativas ao registo de atividades com ativos virtuais, prevendo-se a punição como contraordenação especialmente grave, numa coima entre 5.000€R e 1.000.000€ para pessoas coletivas ou entidades equiparadas e entre 2.500€ e 1.000.000€ para pessoas singulares.

Apesar destas sanções, existem dezenas de entidades que exercem atividades com ativos virtuais em Portugal e que não estão sujeitas à atividade fiscalizadora do Banco de Portugal.[50] Desta forma, não é garantido o cumprimento de deveres de PBCFT, o que consubstancia um elevado risco.

A *Luso Digital Assets*, pelo contrário, é uma entidade fundada em 2020, licenciada e regulada pelo BdP desde 2021 e que exerce atividade com ativos virtuais em toda a zona SEPA. O estágio na *Luso Digital Assets* foi realizado

[48] A lista de prestadores destes serviços registados junto do Banco de Portugal está disponível *online* e pode ser consultada em https://www.bportugal.pt/sites/default/files/documents/2024-01/lista_entidades_ativos_virtuais_pt.pdf [consultado em 29.09.2024].
[49] Disponível em https://www.bportugal.pt/page/registo-de-entidades-que-exercem-atividades-com-ativos-virtuais [consultado em 29.09.2024].
[50] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 261.

entre abril e agosto de 2023, das 9 às 18 horas, em regime 100% remoto e a minha orientadora de estágio foi a Dra. Madalena Catarino.

Desde o primeiro dia de estágio tive contacto com a realidade do BCFT, pois sendo o estágio realizado no departamento de *Compliance*, esta era a principal preocupação do departamento, garantir que a empresa estava *compliant* com a lei e cumpria as normas de PBCFT.

O dia a dia na Luso consistia em abrir a plataforma da empresa e analisar tanto os novos clientes que tinham feito o *onbording* connosco, como os clientes que tinham feitos novas transações.

Para os clientes novos, fazíamos uma análise cuidada das informações que nos forneciam, nomeadamente confirmando os dados do documento de identificação (pode ser um cartão de identificação, carta de condução ou título de residência), se o mesmo estava válido, se tinham dado a informação completa, confirmávamos a morada e se representavam um risco acrescido de BCFT pelo país onde viviam ou pela atividade que desempenhavam. Se estivessem nas chamadas *"listas negras"*[51] e se integrassem as listas dos PEPs, o sistema gerava automaticamente um alerta. Estes alertas eram cautelosamente examinados.

Tal como nos explica NUNO SERDOURA DOS SANTOS[52], a política de KYC da maior parte das operadoras exige aos criadores da carteira/conta uma cópia do cartão de identificação e/ou carta de condução, um email válido para verificar a identidade, um número de telefone para ativar a autenticação de dois fatores e um comprovativo de morada com não mais de 6 meses.

Para os clientes que já haviam sido aprovados e pretendessem fazer nova transação connosco, analisávamos o risco dessas transações e pedíamos, nomeadamente SOFs (*Source of Funds*) sempre que se justificasse.

O *onbording* era realizado pelos clientes através dos procedimentos autónomos de KYC (*Know Your Customer*) e CDD (*Customer Due Diligence*) e

[51] Nestas "*listas negras*" constam indivíduos e empresas sinalizados que pertencem ou agem para determinadas jurisdições de Alto Risco e Não Cooperantes, bem como indivíduos, grupos e entidades terroristas e narcotraficantes.
[52] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 262.

posteriormente passavam pelo departamento de *compliance* para serem analisados. No caso de não revelarem risco de BCFT, os mesmos eram aprovados e os clientes podiam, assim, transacionar os ativos virtuais pretendidos.

No caso de representarem riscos ou suspeita de BCFT, os alertas não eram limpos, a situação era examinada pela direção para posterior decisão de comunicar ou não ao BdP.

Foi uma excelente oportunidade para conhecer como é aplicada na prática a matéria da PBCFT, para aprender mais sobre este crime, sobre os riscos associados às novas tecnologias nesta temática e descobrir como é difícil detetá-los, bem como confirmar as suspeitas levantadas. Foi uma experiência muito relevante e muito útil para conhecer a realidade de uma entidade que exerce atividade com ativos virtuais e o papel que estas desempenham na PBCFT.

Além das funções relacionadas com a PBCFT, como a análise de clientes e do risco que representam, também assumi a tarefa de preparar as formações que foram dadas aos trabalhadores da *Luso Digital Assets* durante o período em que realizei o estágio, ao abrigo do dever de formação.

Assumi a responsabilidade de preparar três formações, no total, com os seguintes temas:

- O Branqueamento de Capitais e Financiamento ao Terrorismo (BCFT): uma visão global sobre a legislação;
- Os deveres específicos das empresas que exercem atividades com ativos virtuais;
- Os procedimentos específicos da LDA relativamente a *compliance* e BCFT.

A experiência de preparar as formações para todos os colaboradores da empresa, juristas e não juristas, permitiu-nos ter contacto com a matéria da PBCFT e ganhar a capacidade de descrevê-la de uma maneira mais simples e pedagógica.

O estágio na *Luso Digital Assets* foi, de facto, uma ótima oportunidade para ver, na prática, inserida no mundo atual, o que se faz em matéria de PBCFT.

5. O GAFI e a sua abordagem à atividade com ativos virtuais

O *Groupe d'Action Financière sur le Blanchiment de Capitaux*, *Financial Action Task Force on Money Laundering* ou Grupo de Ação Financeira Internacional, em português, é um organismo intergovernamental, criado a 16 de julho de 1989, na reunião da Cimeira dos Países do G7, em Paris.

Este organismo tem como objetivo desenvolver e promover políticas de combate ao BCFT. É, no fundo, uma organização de peritos que funciona no âmbito da OCDE em consequência da decisão da Cimeira dos 7 países mais industrializados do mundo[53]. O GAFI promove padrões internacionais e a aplicação efetiva das medidas legais, regulamentares e operacionais necessárias para combater o BCFT e outras ameaças à integridade do sistema económico-financeiro internacional.

O GAFI (i) emite recomendações destinadas a prevenir e a reprimir esses crimes (consideradas *standards* internacionais nestas matérias), (ii) promove a avaliação mútua da observância desses *standards* (iii) determina contramedidas relativamente às jurisdições com deficiências relevantes e (iv) identifica novos riscos e metodologias de combate a estas atividades criminosas.

Nas palavras de JAIME WINTER ETCHEBERRY[54] o GAFI é, atualmente, a organização internacional mais importante do mundo na luta contra o BCFT, sendo particularmente relevante para o desenvolvimento desta luta, as suas Quarenta Recomendações. As Recomendações do GAFI constam, desde 2012, num documento único.

As Quarenta Recomendações do GAFI originais foram criadas em 1990 como uma iniciativa para combater o branqueamento de capitais provenientes do tráfico de droga e são consideradas "ainda hoje a base dos modernos regimes

[53] Os sete países que integram o grupo são: Alemanha, Canadá, Estados Unidos, França, Itália, Japão e Reino Unido.
[54] ETCHEBERRY, Jaime Winter – "La regulación internacional del lavado de activos y el financiamento del terrorismo" *in* "Lavado de Activos y Compliance – Perspectiva internacional y Derecho comparado", p. 36.

de prevenção"[55]. Em 1996, as Recomendações foram revistas pela primeira vez para refletir as novas tendências e técnicas de branqueamento de capitais e para ampliar o escopo das Recomendações para além do branqueamento de capitais relacionado apenas com drogas. Na sequência do ataque terrorista de 11 de setembro de 2001, a 10 de outubro do mesmo ano, o GAFI expandiu o seu mandato para poder tratar também da questão do financiamento dos atos e organizações terroristas e deu um importante passo ao criar as Oito (posteriormente expandidas para Nove) "Recomendações Especiais sobre Financiamento do Terrorismo". As Recomendações do GAFI foram revistas, pela segunda vez, em 2003 e essas, juntamente com as Recomendações Especiais (desenvolvidas por notas interpretativas e atualizadas em 2004), foram adotadas por mais de 180 países, sendo reconhecidas universalmente como o padrão internacional de PBCFT[56].

Atualmente são membros do GAFI 35 países ou territórios (África do Sul, Alemanha, Argentina, Austrália, Áustria, Bélgica, Brasil, Canadá, China, Dinamarca, Espanha, E.U.A., Finlândia, França, Grécia, Hong Kong, Índia, Irlanda, Islândia, Itália, Japão, Luxemburgo, Malásia, México, Noruega, Nova Zelândia, Países Baixos, Portugal, Reino Unido, República da Coreia, Rússia, Singapura, Suécia, Suíça e Turquia) e duas organizações regionais (Comissão Europeia e Conselho de Cooperação do Golfo). O GAFI também promove a avaliação periódicas dos sistemas de PBCFT, tendo o sistema português sido avaliado no âmbito do GAFI em 1994, 1999 e 2006 e 2017[57].

A nova era dos ativos virtuais tem trazido mudanças legislativas significativas nas várias jurisdições. Por este motivo, uma das principais preocupações é, precisamente, a compatibilização da regulação no domínio da PBCFT[58], uma

[55] MACHADO, Miguel da Câmara – "Deveres antibranqueamento de capitais: De onde vieram, quais são e como vão evoluir (do "4G" ao "5G")" *in* "Novos Estudos sobre *Law Enforcement*, *Compliance* e Direito Penal", p. 269.

[56] Disponível em https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/Recommendations/FATF-40-Rec-2012-Portuguese-GAFISUD.pdf.coredownload.inline.pdf - p. 7.

[57] Os resultados da avaliação de 2017 podem ser consultados no relatório *Anti-money laundering and counter-terrorist financing measures in Portugal – Mutual Evaluation Report* (*December* 2017) - https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/relatorio_de_avaliacao_mutia_de_portugal_-_2017.pdf.

[58] BRITO, João Rodrigues – "Da sujeição dos *Virtual Asset Service Providers* ao Cumprimento de Deveres de Prevenção do Branqueamento de Capitais" *in* "Novos Desafios da Prova Penal", p. 369 a 399.

vez que cada país adota as suas políticas nesta matéria, essas políticas vão variando ao longo do tempo e é necessária uma compatibilização global nesta matéria para concretizar a cooperação internacional. A atividade do GAFI afigura-se, por esse motivo, essencial.

Relativamente à atividade com ativos virtuais e tal como já havia acontecido no passado, foram os EUA a dar o primeiro passo[59] ao atribuir a alguns prestadores de serviços de ativos virtuais a classificação de *money services business,* uma categoria dentro da instituição financeira ao abrigo do *Bank Secrecy Act*[60]. Desta forma, fizeram cair sobre estas entidades as mesmas tipologias de deveres de PBCFT, tais como o dever de identificação, de conservação de registos e de comunicação de operações suspeitas.[61]

Desta feita, vários países e organizações internacionais têm seguido o exemplo americano, embora algumas vezes fossem impostos a estas entidades deveres de PBCFT, ainda antes de obrigações fiscais ou de regulação financeira pura, o que contraria o movimento habitual (geralmente, primeiro impõem-se obrigações fiscais ou de regulação financeira e, depois, a exigência de deveres de PBCFT).[62]

Sendo o GAFI considerado o mais importante emissor de *soft law* ao nível internacional no domínio da PBCFT (ao ponto de tomarem as suas Recomendações como inevitável emissão de legislação nesta temática), era expectável que se pronunciasse sobre o domínio dos ativos virtuais.

[59] Os EUA já haviam sido o primeiro país no mundo a criminalizar o branqueamento de capitais, em 1986, através do *Money Laundering Control Act* e acredita-se que tenha sido a pressão dos EUA que motivou a criação do GAFI, porque aos americanos interessava uma unidade, para o mundo inteiro, que garantisse que todos os países tinham as mesmas regras AML, de forma que o dinheiro não "fugisse" dos bancos americanos para a Europa.
[60] *Bank Secrecy Act* é a designação do *Currency and Foreign Transactions Reporting Act* de 1970, que constitui a lei americana de combate ao branqueamento de capitais.
[61] BRITO, João Rodrigues – "Da sujeição dos *Virtual Asset Service Providers* ao Cumprimento de Deveres de Prevenção do Branqueamento de Capitais" *in* "Novos Desafios da Prova Penal", p. 369 a 399.
[62] *Idem*, p. 369 a 399.

De facto, foi na sequência das recomendações do GAFI que se salientou a necessidade de existir uma abordagem baseada no risco em relação ao cumprimento do *KYC*, aquando da compra e venda de criptomoedas[63].

Cronologicamente, foi em 2010 que o GAFI mencionou pela primeira vez o aparecimento de novos métodos de pagamento e os perigos associados aos ativos virtuais e às suas plataformas, sendo que só em 2014 é que esta organização produziu o primeiro estudo compreensivo sobre a matéria, assente no tal *risk based approach* no contexto da PBCFT. Este estudo abrangia uma análise a diferentes tipos de ativos virtuais e também articulava descrições sobre os mecanismos e formas de funcionamento das plataformas que operam na rede, incluindo métodos de mineração, mercados de câmbio (*exchanges*), misturadores (*mixers*/*tumblers*) e carteiras de ativos virtuais (*wallets*). Com este diagnóstico, abriu-se a porta à regulação do mercado dos ativos virtuais e, em 2015, o GAFI propôs mecanismos de adaptação das suas *Recommendations – International standards on combating money laundering and the financing of terrorism & proliferation* para implementação no âmbito dos ativos virtuais[64].

A Recomendação do GAFI de 2014 evidenciou, portanto, os principais conceitos relacionados com ativos virtuais, assim como os riscos para efeitos de BCFT associados a estas novas tecnologias[65], ao passo que na orientação emitida em 2015, os objetivos foram, essencialmente, aprofundar o reconhecimento dos riscos associados a estas novas tecnologias e alertar as autoridades nacionais e decisores políticos para a necessidade de implementar sistemas regulatórios para os ativos virtuais; e, por outro lado, alertar os próprios operadores do mercado para a necessidade de desenvolver estratégias para mitigar esses riscos – prescindindo, portanto, de estabelecer restrições ou impor ónus aos próprios utilizadores dos ativos virtuais. Na Nota Interpretativa da Recomendação 15 (GAFI 19b) foi também publicada uma vasta orientação do GAFI relativamente à implementação de novos padrões internacionais de combate ao BCFT através de ativos virtuais. Em 2019, o GAFI sentiu

[63] RODRIGUES, André Alfar – Manual de Inovação Financeira: Uma Introdução ao Universo das Criptomoedas e da Blockchain, p. 159.
[64] RAMALHO, David Silva e MATOS, Nuno Igreja – Branqueamento e *Bitcoin*: uma introdução, p. 96 e 97.
[65] Esta Recomendação do GAFI é inspirada no relatório do BCE de 2012 e na *guidance* da FinCEN de 2013.

necessidade de incluir uma referência expressa aos ativos virtuais e às entidades que exercem atividade com ativos virtuais e foi na GAFI 2019a que foram apelidados de *Virtual Asset* e *Virtual Asset Service Providers* (VASP), respetivamente[66].

Em 2019, o GAFI recomendou que todos os países deveriam impor obrigações de registo ou licenciamento às entidades que exercem atividade com ativos virtuais e sujeitá-las ao cumprimento dos mesmos deveres de PBCFT que são aplicáveis às instituições financeiras (GAFI 2019a), como o dever de identificação e diligência e o de comunicação de operações suspeitas.

Seguindo a linha da Recomendação relativamente à obrigação de registo ou licenciamento, surgiu o Aviso do Banco de Portugal n.º 3/2021, que regula, como já vimos, o processo de registo e de alteração das entidades que exercem atividade com ativos virtuais, junto do Banco de Portugal.

Quanto à sujeição dos mesmos deveres que são aplicáveis às entidades financeiras, importa assinalar que continua a haver, todavia, algumas situações em que se estabelecem diferenças, como é o caso das transações ocasionais. Para as entidades que exercem atividade com ativos virtuais, o limiar mínimo a partir do qual estas ficam obrigadas a levar a cabo deveres de identificação e diligência (*Customer Due Diligence* – CDD) corresponde a 1.000 dólares ou euros, em oposição aos 15.000 dólares ou euros aplicáveis às instituições financeiras. Isto é justificado pelo maior potencial de risco e pela natureza transfronteiriça das atividades com ativos virtuais.[67]

[66] BRITO, João Rodrigues – "Da sujeição dos *Virtual Asset Service Providers* ao Cumprimento de Deveres de Prevenção do Branqueamento de Capitais" *in* "Novos Desafios da Prova Penal", p. 369-399.
[67] *Idem*.

Capítulo II – Evolução legislativa

1. Introdução da legislação

Cumpre fazer uma breve análise da evolução legislativa nacional e internacional nos últimos anos. Conforme assinalou OLIVEIRA ASCENSÃO[68], a legislação portuguesa andou sempre a reboque de movimentos internacionais em matéria do BCFT, pelo que nos pareceu preferível associar ambos os contextos.

Está claro que o crime de BCFT, até pelo seu *modus faciendi*, implica a utilização de meios sofisticados e envolve, muitas vezes, vastas redes de contactos que ultrapassam as fronteiras. As relações entre os Estados e a colaboração transfronteiriça são, por este motivo, vitais. Indo aos primórdios da questão, conseguimos detetar certos sinais marcantes do progressivo e redobrado esforço de cooperação e vinculação internacional através da aprovação de certos diplomas[69].

Diríamos que o primeiro marco histórico na legislação sobre BCFT aconteceu com a aprovação em Viena, em dezembro de 1988, da Convenção das Nações Unidas contra o tráfico ilícito de estupefacientes e de substâncias psicotrópicas [70], ratificada em 1991 por Portugal[71]. Este diploma determinou "a inclusão, na legislação de cada país, da reciclagem de capitais provenientes do tráfico de droga no quadro das infracções criminais, possibilitando e facilitando, deste modo, a cooperação judiciária e a extradição"[72].

Seguiu-se a Convenção n.º 141 do Conselho da Europa, assinada em Estrasburgo a 8 de novembro de 1990, relativa ao Branqueamento, Deteção,

[68] ASCENSÃO, José de Oliveira – "Branqueamento de Capitais: Reacção Criminal", i*n* "Estudos de Direito Bancário", p. 338-339.
[69] CANAS, Vitalino - «Branqueamento de Capitais»: Noções elementares do regime jurídico de prevenção e repressão e evolução previsível, p. 206
[70] Disponível em https://www.unodc.org/pdf/convention_1988_en.pdf.
[71] Pela Resolução da Assembleia da República n.º 29/91 https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_NU_contra_trafico_ilic_estupefacientes_sbst_psicotropicas.pdf.
[72] PAÚL, Jorge Patrício – "A Legislação Portuguesa sobre Branqueamento de Capitais e as suas Repercussões no Exercício da Actividade Bancária" *in* "Estudos de Direito Bancário", p. 321-336.

Apreensão e Perda dos Produtos do Crime, que ampliou a definição de branqueamento incluída na Convenção da ONU e deu, entretanto, lugar à Convenção do Conselho da Europa Relativa ao Branqueamento, Deteção, Apreensão e Perda dos Produtos do Crime e ao Financiamento do Terrorismo, assinada por Portugal a 16 de maio de 2005[73]. Com esta Convenção passou a contemplar-se não só o financiamento ao terrorismo através de atividades de branqueamento de capitais, mas também através de atividades lícitas. Esta convenção foi ratificada por todos os Estados-Membros da União Europeia[74].

Específica para as entidades financeiras, tivemos a Diretiva n.º 91/308/CEE do Conselho das Comunidades Europeias, de 10 de junho de 1991[75], relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais. Esta diretiva foi parcialmente alterada pela Diretiva n.º 2001/97/CE, do Parlamento Europeu e do Conselho, de 4 de dezembro de 2001[76] e que foi depois transposta pela Lei n.º 11/2004, de 27 de março[77] para o nosso ordenamento jurídico. Esta lei estabeleceu um regime de prevenção e repressão do branqueamento de vantagens de proveniência ilícita, trouxe o branqueamento para o Código Penal e introduziu o "esqueleto" do que é hoje a Lei n.º 83/2017.

Podemos assinalar como primeiro diploma português relativo a BCFT o Decreto-Lei n.º 15/93, de 22 de janeiro (inspirado na Convenção de Viena e na Convenção de Estrasburgo). Trata-se do diploma geral sobre estupefacientes e substâncias psicotrópicas, reviu a legislação de combate à droga e foi emitido em consequência de autorização legislativa contida na Lei n.º 27/92, de 31 de agosto. No seu artigo 23º, sob a epígrafe «conversão, transferência ou dissimulação de bens ou produtos», surgiu a incriminação do branqueamento de capitais[78]. Era limitada aos bens provenientes das infrações previstas nos artigos 21º, 22º, 24º e 25º daquele diploma e, portanto, ao domínio da droga.

[73] Disponível em https://files.dre.pt/1s/2009/08/16600/0564705674.pdf.
[74] Retirado de https://www.europarl.europa.eu/meetdocs/2009_2014/documents/crim/dt/925/925991/925991pt.pdf.
[75] Disponível em https://eur-lex.europa.eu/eli/dir/1991/308/oj?locale=pt.
[76] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32001L0097.
[77] Disponível em https://diariodarepublica.pt/dr/detalhe/lei/11-2004-210422.
[78] Nesta expressão já se abrangia não só o branqueamento de capitais propriamente ditos, mas também o branqueamento de outros bens provenientes da prática de crimes.

Seguiu-se o Decreto-Lei n.º 313/93, de 15 de setembro, que é precedido da autorização legislativa n.º 16/93, de 3 de Junho e é a transposição da Diretiva 91/308/CE. Neste diploma estabelecem-se, nos artigos 8º e seguintes, os primeiros deveres das entidades financeiras perante transações suspeitas, como o dever de informar a autoridade judiciária competente (artigo 10º). São também estabelecidas medidas sancionatórias de natureza contraordenacional no caso de incumprimento desses deveres, cuja aplicação compete ao Ministério das Finanças.

Em 1995, surge o Decreto-Lei n.º 325/95, de 2 de dezembro, que alargou ainda mais os limites da criminalização e dos deveres de prevenção. Este diploma é emitido no seguimento da autorização legislativa contida na Lei n.º 32/95, de 18 de agosto e unificou (relativamente) esta matéria, generalizando-a em dois sentidos, um relativo ao crime e outro ao ilícito de mera ordenação social:

- O branqueamento de capitais passou a ser estendido aos proventos originados por outros crimes, além dos relativos ao tráfico de droga;
- Os deveres acessórios das entidades ao abrigo deste diploma estendem-se a outras entidades, além das financeiras.

De elevada importância também o Regulamento (CE) n.º 2580/2001 do Conselho, de 27 de dezembro de 2001[79], relativo a medidas restritivas específicas de combate ao terrorismo dirigidas contra determinadas pessoas e entidades. Constatamos que as instituições da União Europeia começaram a legislar sobre o fenómeno do BCFT durante a década de 90, mas a preocupação com a sua prevenção e a consagração do combate ao terrorismo evidenciou-se, como seria de esperar, após o atentado de 11 de setembro de 2001. A resposta, a nível nacional, veio em 2003, com a Lei n.º 52/2003, de 22 de agosto, que aprova a Lei de combate ao Terrorismo.

Contudo, no que concerne à repressão do branqueamento de capitais, importa referir a Lei n.º 5/2002, de 11 de janeiro, relativa a medidas de combate à criminalidade organizada e económico-financeira, dado que estabeleceu um

[79] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32001R2580.

regime especial de recolha de prova, quebra do segredo profissional e perda de bens a favor do Estado para este crime.

2. As gerações de instrumentos normativos de combate ao BCFT

Ao contrário do Direito a que estamos habituados, que é um Direito estável (os códigos são feitos para vigorarem "para sempre"), as leis da PBCFT já vêm, nas diretivas da União Europeia, com um "prazo de validade", usando as palavras de MIGUEL DA CÂMARA MACHADO[80].

Estes diplomas preveem a sua revisão periódica porque os branqueadores de capitais também os estudam, razão pelo qual o Direito tem de estar em constante evolução e a alterar os sistemas preventivos.

O autor identifica cinco (quase seis) gerações de instrumentos normativos no combate ao BCFT:

- Uma primeira geração ("1G") que surgiu nos anos 80/90, no contexto da luta contra o tráfico de droga[81]. Como consequência, foi impulsionada, nos EUA, a criação de regras que obrigavam os bancos a reportar determinados comportamentos dos seus clientes[82];
- A segunda geração ("2G"), que surge no contexto das medidas contra o terrorismo e que se intensificaram após o 11 de setembro de 2001. Nesta altura, os deveres de denúncia pelas empresas e pelos bancos também foram ainda mais aprofundados[83];

[80] MACHADO, Miguel da Câmara – "Contexto, evolução e tendências do *compliance* em Portugal e na Europa, em especial a partir do Aviso n.º 3/2020, de 15 de julho, do Banco de Portugal" *in* "Estudos sobre *Law Enforcement*, *Compliance* e Responsabilidade Empresarial", p. 187 e ss.
[81] Neste contexto, surgiu a Diretiva n.º 91/308/CEE, do Conselho, de 10 de Junho de 1991, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais; o Decreto-Lei n.º 15/93, de 22 de Janeiro, que revê a legislação de combate à droga; e o Decreto-Lei n.º 325/95, de 2 de Dezembro, que introduziu os primeiros deveres de prevenção do branqueamento de capitais no nosso ordenamento jurídico.
[82] Nesta altura, alguns deveres que foram exigidos, e que analisaremos adiante, foram previstos de uma maneira que funcionou de forma contraditória, desde logo, o dever de identificação: quando os bancos suspeitavam de alguma operação eram obrigados a pedir mais informações, o que funcionava como um aviso para os ordenantes que passavam assim a saber que eram suspeitos e estavam a ser investigados, sendo fácil reconhecer efeitos contrários aos desejados.
[83] Sobressaem aqui a Convenção do Conselho da Europa relativa ao Branqueamento, Deteção, Apreensão e Perda dos Produtos do Crime e ao Financiamento ao Terrorismo, assinada por

- A terceira geração ("3G"), com instrumentos mais reforçados e detalhados, ainda a propósito do terrorismo e da criminalidade internacional – contexto em que foi feita a Lei n.º 25/2008 – que orientou os profissionais portugueses nesta matéria ao longo da última década[84];
- Uma quarta geração ("4G"), que alargou o combate à luta contra a corrupção e os crimes fiscais, marcas sentidas na Lei n.º 83/2017 hoje vigente[85];

Portugal em 17 de maio de 2005; o Regulamento (CE) n.º 2580/2001, do Conselho, de 27 de Dezembro de 2001, que prevê medidas restritivas específicas de combate ao terrorismo; a Diretiva n.º 2001/97/CE, do Parlamento Europeu e do Conselho, de 4 de Dezembro de 2001, que foi transposta pela Lei n.º 11/2004, de 27 de Março, que estabelece um regime de prevenção e repressão do branqueamento de vantagens de proveniência ilícita, trouxe o branqueamento para o Código Penal e introduziu o "esqueleto" do que é hoje a nova Lei n.º 83/2017. Também relevante nesta época foi o Regulamento (CE) 1889/2005 do Parlamento Europeu e do Conselho, de 26 de Outubro de 2005, relativo ao controlo das somas em dinheiro líquido que entram e saem da União Europeia, que ainda hoje se mantem em vigor; e a Lei n.º 11/2004, a "Lei da prevenção do branqueamento" que antecedeu a de 2008 e foi alvo de bastantes críticas, tendo introduzido no nosso ordenamento a estrutura de deveres que apenas seria desenvolvida em 2008 e muito detalhada em 2017.

[84] O quadro normativo que vigorou até 2017 é o que decorre de duas importantes Diretivas: a Diretiva n.º 2005/60/CE (relativa à prevenção da utilização do sistema financeiro e de outras atividades e profissões especialmente designadas para efeitos de branqueamento) e a Diretiva n.º 2006/70/CE (com medidas de execução da outra), transpostas através da Lei n.º 25/2008, que entretanto sofreu várias alterações, das quais destacamos: (i) o Decreto-Lei n.º 317/2009 (com mudanças relativas às instituições de pagamento); (i1) o Decreto-Lei n.º 242/2012 (relativo às instituições de moeda eletrónica); (iii) o Decreto-Lei n.º 18/2013 (quanto à colaboração com autoridades europeias); (iv) o Decreto-Lei n.º 157/2014 (que veio reforçar as sanções pela violação dos deveres de prevenção e prever uma nova sanção acessória); (v) a Lei n.º 62/2015 (desde logo quanto ao jogo online); (vi) e, por fim, a Lei n.º 118/2015 (que aprofunda a definição do conceito de beneficiário último das transações). Deste quadro normativo, importa ainda lembrar o Decreto-Lei n.º 125/2008, de 21 de julho, que estabelecia as medidas nacionais necessárias à efetiva aplicação do Regulamento (CE) n° 1781/2006, do Parlamento Europeu e do Conselho, relativo às informações sobre o ordenante que deviam acompanhar as transferências de fundos (e que antecedeu o Regulamento (UE) 2015/847).

[85] Destacam-se aqui: i) a Diretiva "4G" (ou AML IV), a Diretiva (UE) 2015/849, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, mas também (ii) a Diretiva (UE) 2016/2258 do Conselho, de 6 de Dezembro de 2016, relativa ao acesso às informações anti branqueamento de capitais por parte das autoridades fiscais; os regulamentos delegados (ii) (UE) 2018/1108 da Comissão, de 7 de maio 2018 e (iv) (UE) 2016/1675 da Comissão, de 14 de julho de 2016; (v) o Regulamento (UE) 2015/847 do Parlamento Europeu e do Conselho, de 20 de maio 2015, que estabelece as informações sobre o ordenante que devem acompanhar as transferências de fundos.

No plano nacional, releva principalmente a Lei n.º 83/2017, de 18 de agosto que "estabelece medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo", mas também as Leis n.º 89/2017, 92/2017, 96/2017, 97/2017 (o "pacote anti lavagem do verão de 2017"), a Lei n.º 15/2017, de 3 de maio (que proíbe a emissão de valores mobiliários ao portador; o Decreto-Lei n.º 123/2017, de 25 de setembro (que estabelece o regime de conversão dos valores mobiliários ao portador em valores mobiliários nominativos, em execução daquela Lei n.º 15/2017); a Resolução do Conselho de Ministros n.º 88/2015, de 1 de outubro, que criou a Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo; e a Portaria n.º 233/2018, de 21 de agosto, que regulamenta o Regime Jurídico do RCBE.

- E, por último, uma quinta geração ("5G"), de que é paradigmática a Quinta Diretiva AML, a Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, identificando como áreas distintivas de preocupação e inovação o mercado da arte[86] (também comicamente apelidado de "*Monet laundering*", em referência ao famoso pintor) e, principalmente, o mundo das *fintechs* e dos ativos virtuais.

Com esta separação, conseguimos distinguir diferentes fases que, pelo combate a um tipo de crime ou fenómeno cujos proveitos seriam branqueados, impulsiona determinado tipo de respostas normativas (ou serve de fundamento para o reforço ou alargamento das preexistentes). Em suma, os regimes de PBCFT aparecem no quadro da luta contra o tráfico de estupefacientes (1G), evoluíram no quadro do combate ao terrorismo (2G) e, mais recentemente, contra a criminalidade inter ou transnacional (3G), estando atualmente a ser alargados ao combate à corrupção e à fraude fiscal (4G), crescentemente preocupados com os avanços tecnológicos relacionados, nomeadamente, com os ativos virtuais.

Relativamente aos ativos virtuais em específico, importa mencionar, que os Estados começaram gradualmente a sensibilizar-se para a necessidade de enquadrar legalmente e blindar os seus sistemas aos riscos emergentes dos novos mercados e ativos virtuais. Em 2012, o Banco Central Europeu publicou o seu primeiro estudo sobre *Virtual Currency Schemes*[87], que alertava para a insegurança destas novas plataformas em face da inexistência de regulação, supervisão e superintendência em relação a esta matéria. Logo em 2013, o FinCEN, não obstante distinguir os mercados de ativos virtuais dos designados *Money Service Business* (MSB) veio expressamente clarificar «*the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies*», bem como sujeitar os administradores de empresas prestadores de

[86] Para compreender melhor as preocupações relativas a BCFT no âmbito do mercado da arte recomenda-se a leitura dos seguintes artigos: https://www.dentons.com/en/insights/articles/2024/march/11/the-art-market-a-money-launderers-haven, https://www.whitecase.com/insight-alert/money-laundering-issues-art-market e https://www.moneylaunderingnews.com/2022/02/treasury-report-no-immediate-need-for-bsa-regulations-for-the-art-industry/ [todos os artigos consultados em 18.04.2024].
[87] Disponível em https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

serviços sobre ativos virtuais às regras da FinCEN[88]. No panorama europeu, no entanto, apenas com a aprovação da "Quinta Diretiva AML", que examinaremos já de seguida, é que se consolidou e uniformizou uma política regulatória comum no quadro dos ativos virtuais[89].

Iremos aprofundar esta Diretiva pois refere-se especificamente a matéria de regulação da PBCFT, contudo não podemos deixar de referir que, em matéria de regulação da própria atividade, foi muito relevante o Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho, de 31 de maio de 2023 (também conhecido por Regulamento MiCA), que introduziu novas regras quanto à classificação, à emissão e à admissão à negociação de criptoativos, assim como quanto à prestação de serviços com criptoativos.

A ideia era adotar um conjunto de medidas destinadas a fomentar ainda mais o potencial do financiamento digital em termos de inovação e concorrência, garantindo que a Europa estava preparada para a era digital e criando uma economia preparada para o futuro, ao lado dos cidadãos europeus.[90]

[88] Disponível em https://www.fincen.gov/sites/default/files/guidance/FIN-2013-G001.pdf.
[89] RAMALHO, David Silva e MATOS, Nuno Igreja – Branqueamento e *Bitcoin*: uma introdução, p. 98.
[90] RODRIGUES, André Alfar – Manual de Inovação Financeira: Uma Introdução ao Universo das Criptomoedas e da Blockchain, p. 168.

3. A Quinta Diretiva AML

A Quinta Diretiva AML nasce da constatação do aumento exponencial das transações levadas a cabo em mercados digitais e de uma paralela convicção de que os prestadores de serviços na *blockchain*, especialmente os mercados de câmbio entre moedas virtuais e moedas fiduciárias e os prestadores de serviços de carteiras virtuais, enquanto pontos de acesso privilegiados ou sucedâneos virtuais ao sistema financeiro tradicional, não se encontravam claramente sujeitos aos deveres de controlo, identificação, diligência e comunicação de suspeitas estabelecidos nas anteriores Diretivas AML (e correspondente legislações nacionais de transposição)[91].

Nesse sentido, a Quinta Diretiva veio assumir o propósito de «incluir os prestadores cuja atividade consista na realização de serviços de câmbio entre moedas virtuais e moedas fiduciárias, bem como os prestadores de serviços de custódia de carteiras digitais»[92], fixando, para o efeito, definições de **moeda virtual** e de **prestador de serviços de custódia de carteiras**[93], que foram expressamente abrangidos pelas disposições da Diretiva.

Apesar de as moedas virtuais poderem ser utilizadas como meio de pagamento, também podem servir para outros fins e ter aplicações mais vastas, servindo como meio de troca, investimento, produtos de reserva de valor ou utilização nos casinos *online*. A Diretiva tinha por objetivo abranger todas as possíveis utilizações das moedas virtuais.[94]

Já as carteiras custodiadas são um tipo de carteira digital que é controlada e mantida por terceiros, como uma *exchange* ou uma empresa de custódia de

[91] RAMALHO, David Silva e MATOS, Nuno Igreja – Branqueamento e *Bitcoin*: uma introdução, p. 99.
[92] cfr. § 8 da Quinta Diretiva AML.
[93] cfr. alínea d), do n.º 2 do artigo 1º da Quinta Diretiva AML - "**Moeda virtual**": uma representação digital de valor que não seja emitida ou garantida por um banco central ou uma autoridade pública, que não esteja necessariamente ligada a uma moeda legalmente estabelecida e não possua o estatuto jurídico de moeda ou dinheiro, mas que é aceite por pessoas singulares ou coletivas como meio de troca e que pode possa ser transferida, armazenada e comercializada por via eletrónica; e "**Prestador de serviços de custódia de carteiras**": uma entidade que presta serviços de salvaguarda de chaves criptográficas privadas em nome dos seus clientes, com vista a deter, armazenar e transferir moedas virtuais.
[94] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 256.

ativos virtuais e, nesse caso, as chaves privadas necessárias para aceder e controlar os ativos virtuais são mantidas e protegidas pela entidade custodiante em nome do usuário.[95]

Quanto aos mercados de câmbio, já vimos que a Diretiva é inequívoca na abrangência dos «Prestadores cuja atividade consista em serviços de câmbio entre moedas virtuais e moedas fiduciárias»[96] (também denominados *crypto-to-fiat exchanges*).

Esta é a atividade primordial das entidades habilitadas a exercer atividade com ativos virtuais em Portugal e é a única que todas essas entidades registadas junto do BdP exercem. É também o caso de outros conhecidos servidores, como a *Coinbase*, *EXMO*, *Bitpanda* ou a *Binance*, que se dedicam a serviços de troca entre ativos virtuais e moeda fiduciária, permitindo a compra e a venda de ativos virtuais através de pagamentos por moeda fiduciária. Estes prestadores constituem os principais pontos de acesso ao mercado dos ativos virtuais e estão, consequentemente, mais expostos, constituindo simultaneamente locais de maior exposição global a riscos de BCFT.

Por outro lado, é preocupante o facto de a Diretiva ter excluído do seu âmbito de aplicação os serviços de câmbio exclusivamente de moedas virtuais (as chamadas *crypto-to-crypto exchanges*, como a *ShapeShift*[97]). Esta exclusão dá azo a um vazio regulatório, embora os prestadores destes serviços possam vir a estar sujeitos à Diretiva quando ofereçam aos seus utilizadores (e até é comum oferecerem) serviços de custódia de carteiras[98]. Mesmo assim, essas casas de câmbio poderão contornar a incidência regulatória se evitarem qualquer função de armazenamento de «chaves criptográficas privadas em nome dos seus cientes», o que é possível, por exemplo, se exigirem que sejam os clientes a introduzir manualmente as respetivas chaves.

---

[95] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 256 [nota de rodapé].
[96] Este aditamento vem, desde logo, previsto na alínea c), do n.º 1 do artigo 1º.
[97] Em 2018, o *Wall Street Journal* acusou a *ShapeShift* de facilitar o branqueamento de capitais de 9 milhões de dólares de fundos provenientes de atividades criminosas durante um período de dois anos – disponível em https://www.wsj.com/articles/how-dirty-money-disappears-into-the-black-hole-of-cryptocurrency-1538149743 [consultado em 18.08.2024].
[98] Desta forma, passam a estar sujeitos à Diretiva, não nos termos da alínea c), do n.º 1 do artigo 1º, mas do n.º 19 da alínea d), do n.º 2 do artigo 1º.

Relativamente aos prestadores de serviços de custódia de carteiras, e como já foi visto, estes encontram-se agora expressamente sujeitos aos deveres de PBCFT, uma vez que prestem serviços de «salvaguarda de chaves criptográficas privadas em nome dos seus clientes, com vista a deter, armazenar e transferir moedas virtuais»[99].

Igualmente preocupante foi a exclusão dos prestadores de serviços de mistura (*mixing*/*tumblers*) do âmbito da Diretiva, o que constitui porventura a mais problemática opção regulatória, na medida em que as operações de mistura, embora sirvam muitas vezes propósitos lícitos de proteção do património pessoal ou da privacidade do utilizador, são também muitas vezes utilizados para ocultar a proveniência ilícita de vantagens.

Desempenhando os misturadores um papel relevante tanto na salvaguarda legítima de ativos virtuais como na dissimulação da sua eventual origem criminosa[100], seria especialmente importante que os prestadores de serviços desta natureza se encontrassem expressamente abrangidos pela Diretiva, até como forma de melhor distinguir os casos em que o recurso aos mesmos exorbita a proteção patrimonial ou corresponde a um propósito materialmente de BCFT. Ainda que também estes serviços surjam algumas vezes acoplados a serviços de custódia de carteiras (tornando-os, assim, sujeitos à Diretiva), a sua inclusão direta reforçaria a eficácia do sistema, evitando potenciais esquivos regulatórios e operações de BCFT através deles.

Com tudo isto, e conforme apontam DAVID SILVA RAMALHO e NUNO IGREJA MATOS[101], esta Diretiva revela uma opção fundamental de aplicação dos deveres de PBCFT às entidades que exercem atividades com ativos virtuais, sem, no entanto, acautelar todos os propósitos preventivos, pois não tem em consideração as características essenciais das criptomoedas e o *quasi*-anonimato nas transações com ativos virtuais. Estes autores referem ainda que a política regulatória inscrita nesta Diretiva é “essencialmente *realpolitik* e não uma política marcadamente intervencionista: regula as moedas virtuais na estrita

[99] cf. n.º 19, da alínea d) do n.º 2 do artigo 1º da Diretiva.
[100] Na GAFI2014 já se alertava para os riscos de BCFT associados a estes serviços de mistura.
[101] RAMALHO, David Silva e MATOS, Nuno Igreja – Branqueamento e *Bitcoin*: uma introdução, p. 100 a 103.

medida e no preciso momento em que as mesmas estão na iminência de contactar com o sistema financeiro tradicional, recusando-se, portanto, a impor qualquer regra que descaracterizasse a essência do funcionamento dos mercados virtuais".

De facto, parece-nos que, apesar de necessária e inovadora nesta matéria, esta Diretiva fracassou quando excluiu do seu âmbito de aplicação os serviços de câmbio entre ativos virtuais e os *mixers*/*tumblers*, que nos debruçaremos novamente adiante, aquando da análise às desvantagens da normalização das transações com ativos virtuais.

Se esta tensão entre a regulação de um novo fenómeno de risco em expansão, por um lado, e o reconhecimento da inevitabilidade da sua subsistência, por outro, gera neste plano de prevenção soluções cujo racional e eficiência é discutível, também no plano repressivo vão surgir problemas muito específicos quando se confrontam comportamentos que são passíveis de ser percebidos como adequados ao contexto descentralizado da *blockchain*, mas que simultaneamente também podem ser percebidos como atos ilícitos à luz dos crimes de BCFT.[102] [103]

Já NUNO SERDOURA DOS SANTOS[104] destaca outras omissões desta Diretiva, pois, ainda que tenha introduzido obrigações de reporte de transações suspeitas às UIF's nacionais, esqueceu, todavia, não só o importante mercado dos NFT's, como os particulares e a própria criação dos ativos virtuais. Ora, "sendo a criptomoeda uma moeda digital na qual se usam meios de encriptação (criptografia) para regular a criação de unidades de moeda e verificar a regularidade da transferência de fundos, operando independentemente (e apesar de) um Banco Central, e estando a sua tecnologia aberta (*open source*) e livremente disponível, é extraordinariamente fácil proceder à criação de uma,

[102] RAMALHO, David Silva e MATOS, Nuno Igreja – Branqueamento e *Bitcoin*: uma introdução, p. 103.
[103] Os autores referem-se especificamente no artigo à "rede bitcoin", todavia, na nossa opinião, o mesmo entendimento é extensível à rede geral, da *blockchain*, motivo pelo qual referir-nos-emos a esta.
[104] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 257 a 259.

e, consequentemente, realizar uma ICO (*Initial Coin Offer*), convencendo os investidores a trocar moeda fiduciária pela moeda virtual ora criada".

A oferta inicial de moeda (ICO) é um método de arrecadação de fundos operando através da emissão de ativos virtuais trocáveis por outros durante a fase de inicialização de um projeto. Esses ativos, denominados de "*tokens*" (*token* digital) são emitidos e trocados utilizando a tecnologia *blockchain*. O software de criação de moeda encontra-se em repositório livre (*open source*) e esta facilidade de criação deste tipo de ativos, associada à falta de regulação, gerou uma infinidade de ativos virtuais cujo valor não se encontra associado a nenhum outro produto ou moeda (ao contrário das *stable coins*, que mantêm um valor relativo associado, por exemplo, ao dólar ou ao ouro). Desta forma, estes ativos podem ser facilmente utilizados por criminosos e ficam totalmente fora do sistema de comunicação associado às transações de moeda fiduciária.

Relativamente aos NFT's, a sua criação e posterior transação em mercados não sujeitos a obrigações de reportes, acabam por comportar um sério risco de BCFT, havendo inclusivamente já notícias do seu uso para esta atividade[105]. Em maio de 2023, o valor de mercado deste tipo de ativos virtuais era de cerca de 20 biliões de dólares[106].

Como explica NUNO SERDOURA DOS SANTOS[107], os NFT's são um tipo de *token* criptográfico que representa a propriedade ou a autenticidade de um item digital único ou raro. Ao contrário das criptomoedas tradicionais, como a *Bitcoin*, que são fungíveis e, por isso, podem ser trocadas por outras unidades idênticas, os NFT's são únicos e não podem ser substituídos um pelo outro.

Os NFT's são baseados na tecnologia *blockchain* e registam informações específicas sobre cada item digital, como o nome do proprietário, histórico de

[105] Chainalysis Team, 2022, August 8. Noutra nota, em 2022, conforme dados da Chainalysis (2023), o valor total das transações ilícitas com criptomoedas atingiu um recorde de 20,6 mil milhões de dólares americanos, marcando o nível mais elevado já registado. Desse montante, 43% estavam diretamente associados a transações relacionadas com entidades sancionadas, representando um aumento impressionante de 152,844% em comparação ao ano de 2021. Além disso, segundo informações do Ciphertrace (2023), entre os meses de julho e setembro de 2022, os ataques cibernéticos a diversas plataformas somaram perdas de 383 milhões de dólares americanos devido a hacks nas diferentes plataformas.

[106] Analytics, 2023.

[107] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 258 e 259.

transações e características exclusivas do item em si. Uma das suas principais características é, portanto, a capacidade de rastrear a sua proveniência e propriedade, garantindo a autenticidade e possibilitando a negociação no mercado secundário. Isto implica que os NFT's podem ter valores únicos e variados, dependendo da procura e do reconhecimento que recebem no mercado.[108]

Contudo, a facilidade de criação de criptomoedas ou de *tokens*, a sua disponibilização ao público mediante uma ICO ou uma ITO (*Initial Token Offer*), bem como a facilidade de criação de uma imagem proprietária e a sua disponibilização ao público em geral para venda em mercados não regulados e não sujeitos a reporte, fazem deste mecanismo um grande aliado à criminalidade organizada e ao BCFT, que não foi contemplado, erradamente, nesta Diretiva.

4. Novo pacote legislativo da União Europeia

A 31 de maio de 2024, o Conselho da União Europeia e o Parlamento Europeu aprovaram um pacote de novas regras em matéria de PBCFT, para proteção dos cidadãos e do sistema financeiro da União Europeia com vista à harmonização das regras nesta matéria em todos os Estados-Membros. Podemos considerar como os principais diplomas as seguintes quatro propostas legislativas:

- **Regulamento (UE) 2024/1620, de 31 de maio de 2024**[109], que cria a Autoridade Europeia para o Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, conhecida como "AMLA" (do inglês, *Anti-Money Laundering Authority*).

Este regulamento é aplicável a partir de 1 de julho de 2025, com exceção de algumas disposições específicas que serão aplicáveis a partir de 26 de junho de 2024 e 31 de dezembro de 2025.

[108] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 258 e 259.
[109] Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401620 [consultado em 18.08.2024].

A AMLA, uma das principais alterações e inovações deste pacote legislativo há muito aguardada, servirá para supervisionar diretamente as entidades obrigadas de alto risco e acompanhar e coordenar as autoridades nacionais. Este era um dos problemas do pacto anterior que se procurou resolver, uma vez que não existia uma supervisão centralizada da União Europeia em matéria de PBCFT e as autoridades nacionais e as UIFs tinham dificuldade em cooperar entre si. As funções são, por isso, essencialmente duas:

- Coordenação e Harmonização: A AMLA coordena e padroniza os critérios de atuação entre as autoridades do setor não financeiro, emitindo guias técnicos (orientações) que facilitam a cooperação e o intercâmbio de informações entre UIFs. Além disso, pode desenvolver os meios eletrónicos utilizados pelas UIFs e pela Europol para partilhar e comparar informações.
- Supervisão: A AMLA supervisiona diretamente as entidades obrigadas, garantindo que estas cumpram as suas obrigações:
    - Por sua iniciativa, no caso de entidades de alto risco de BCFT;
    - A pedido das UIF dos Estados-Membros ou por iniciativa própria, quando tal for de interesse da União.

Com sede em Frankfurt (onde já se encontra sediado o Banco Central Europeu), a AMLA iniciará a sua atividade em meados de 2025.

As entidades que serão supervisionadas diretamente pela AMLA serão selecionadas da seguinte forma:

- As autoridades nacionais podem escolher entidades obrigadas do setor financeiro que operem em, pelo menos, seis Estados-Membros e que apresentem um perfil de risco residual elevado, de acordo com a metodologia harmonizada aprovada pela AMLA. A seleção baseia-se em critérios harmonizados de atividade e risco transfronteiriço.
- A AMLA pode solicitar à Comissão Europeia que coloque temporariamente uma entidade do setor financeiro sob a sua supervisão em situações específicas, quando a entidade não tiver cumprido as obrigações de combate ao BCFT.

- As autoridades nacionais podem pedir à AMLA que supervisione uma entidade que não esteja a cumprir as suas obrigações em matéria de PBCFT ou cuja atividade constitua uma ameaça ao nível da União Europeia.

A AMLA tem ainda a capacidade de analisar o cumprimento das regras de PBCFT pelas entidades sob a sua supervisão direta e de aplicar sanções em caso de incumprimento. Substituirá, assim, as funções da EBA.

Em suma, a AMLA:

i. criará um mecanismo integrado com os supervisores nacionais para assegurar que as entidades obrigadas cumprem as obrigações em matéria de PBCFT no setor financeiro;

ii. desempenhará um papel de apoio no que diz respeito ao setor não financeiro;

iii. coordenará e apoiará as UIFs; e

iv. poderá aplicar sanções pecuniárias às "entidades obrigadas selecionadas", em caso de infração grave, sistemática ou repetida de requisitos diretamente aplicáveis.

- **Regulamento (UE) 2024/1624, de 31 de maio de 2024**[110], relativo à prevenção da utilização do sistema financeiro para efeitos de BCFT.

Este regulamento será aplicável a partir de 10 de julho de 2027 (exceto no caso de novas entidades obrigadas específicas, para as quais será aplicável a partir de 10 de julho de 2029) e visa estabelecer um conjunto único de regras para a PBCFT.

A maior parte do regulamento é amplamente familiar das regras existentes ao nível europeu no âmbito da Quarta Diretiva relativa ao BCFT (alterada pela Quinta Diretiva), mas, pela primeira vez, será sob a forma de um regulamento para harmonizar a abordagem adotada em relação ao BCFT em toda a União

[110] Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401624 [consultado em 18.08.2024].

Europeia, dado que, tendo a natureza de regulamento, será diretamente aplicável.

Existem também alguns novos requisitos e melhorias nas regras existentes que as empresas precisarão de considerar. De entre as novidades, destacamos as seguintes:

i. Alargamento das regras em matéria de combate ao BCFT a novas entidades, abrangendo, agora, todo o setor dos criptoativos (como os prestadores de serviços de criptoativos), mas também as plataformas de financiamento coletivo, intermediários de crédito para créditos hipotecários e ao consumo (com exceção das instituições de crédito e das instituições financeiras), comerciantes de bens de luxo (joias, relógios e veículos de luxo, como veículos a motor avaliados em mais de 250.000€ e aeronaves e embarcações avaliadas em mais de 7.500.000€) e clubes de futebol profissional e agentes quando efetuam determinadas transações;

ii. Fixa o limite máximo de 10.000€ para os pagamentos em numerário em toda a União Europeia. Ao limitar os pagamentos em numerário de somas avultadas**,** a União Europeia tornará mais difícil para os criminosos o branqueamento de capitais de origem criminosa. Porém, os Estados-Membros terão flexibilidade para impor um limite máximo mais baixo, se assim o entenderem;

iii. Estipula novas regras relativas aos beneficiários efetivos das entidades jurídicas, que passam a ser mais pormenorizadas para ajudar a identificar mais facilmente os beneficiários efetivos, especialmente no caso das empresas com estruturas empresariais complexas. Este Regulamento especifica as informações necessárias para identificar os beneficiários efetivos e garante que a regra se aplica uniformemente em toda a União Europeia (obrigando, nomeadamente, as entidades obrigadas a declarar quem é o seu beneficiário efetivo e a registar essa informação no registo central de beneficiários efetivos correspondente). O limite de 25% ou mais das ações ou direitos de voto na entidade legal por ter um interesse de propriedade é mantido, contudo este regulamento prevê a possibilidade de a Comissão Europeia estabelecer, após um período de avaliação que termina em 10 de julho de 2029, um limiar mais

baixo de 15% para certas categorias de entidades empresariais expostas a riscos mais elevados de BCFT;

iv. E estabelece requisitos de dever de diligência mais rigorosos. Nos termos do novo quadro, um notário, advogado ou outro profissional forense deve aplicar medidas de diligência não só em relação aos seus clientes, mas também em relação às outras partes na transação, quando são os únicos profissionais que atuam na transação. Outra novidade do novo pacote é o facto de se exigir que as entidades nomeiem um *compliance manager* para garantir a conformidade e o cumprimento das disposições de PBCFT. Este "diretor de conformidade" deve também ser um membro do conselho de administração da entidade obrigada. O novo quadro utiliza a expressão "órgão de direção na sua função de gestão", que, de acordo com o regulamento, é definido como o órgão de direção responsável pela gestão corrente da entidade obrigada. Além disso, como o regulamento inclui a figura do Responsável pelo Cumprimento Normativo sobre BCFT, é o órgão de gestão da entidade obrigada que o nomeia para implementar políticas, procedimentos e controlos que garantam o cumprimento adequado dessas normas. Em relação ao relatório de transações suspeitas, o regulamento também instituiu que as entidades obrigadas devem comunicar todas as transações suspeitas à UIF.

Por último, especificamente quanto aos prestadores de serviços de criptoativos, estes ficam agora obrigados a exercer o dever de diligência relativamente aos seus clientes, o que significa que terão de verificar os factos e informações sobre os seus clientes e comunicar eventuais suspeitas às UIFs. O Conselho exige que os prestadores de serviços de criptoativos apliquem medidas de diligência sempre que se efetuarem transações de valor igual ou superior a 1 000€ e acrescenta medidas para mitigar os riscos relacionados com as transações que envolvam carteiras de autocustódia. O Conselho introduziu igualmente medidas específicas de diligência reforçada para as relações transfronteiras de correspondência para os prestadores de serviços de criptoativos. Relativamente às transferências de fundos, o regulamento da União Europeia relativo às informações que acompanham as transferências de fundos também viu o seu âmbito de aplicação alargado às transferências de criptoativos.

As novas regras, que constam das diretrizes da chamada *travel rule*[111], impõem a estes prestadores de serviços a obrigação de recolher e disponibilizar certas informações sobre os ordenantes e beneficiários envolvidos nas transferências de criptoativos. Isso garantirá a rastreabilidade dessas transações, facilitando a identificação e o bloqueio de operações potencialmente suspeitas.

Desta forma, verifica-se um quadro sólido e proporcional que cumpre as normas internacionais mais exigentes em matéria de troca de criptoativos e são seguidas as recomendações formuladas pelo GAFI, bem como o critério já expresso para as instituições financeiras nas Orientações da EBA (*European Banking Authority*) de 14 de junho de 2022 que é agora alargado a todas as entidades obrigadas.

Neste novo quadro legislativo, as regras aplicáveis ao setor privado são transferidas para este Regulamento que, após três anos da sua entrada em vigor, será diretamente aplicável em todos os Estados-Membros.

- **Diretiva (UE) 2024/1640, de 31 de maio de 2024**[112] (já conhecida como Sexta Diretiva AML) relativa aos mecanismos a estabelecer pelos Estados-Membros para efeitos de prevenção da utilização do sistema financeiro para o BCFT, que altera a Diretiva (UE) 2019/1937 e altera e revoga a Diretiva (UE) 2015/849 (também conhecida por Quarta Diretiva AML).

Os Estados-Membros devem transpor esta diretiva o mais tardar até 10 de julho de 2027.

[111] A *travel rule*, originalmente uma recomendação do GAFI, exige que prestadores de serviços financeiros, incluindo agora os prestadores de serviços de criptoativos, coletem e transmitam informações sobre o remetente e o destinatário em transações, assegurando a rastreabilidade das transferências e facilitando a identificação de atividades suspeitas. Com a aprovação dos novos diplomas legislativos da União Europeia em maio de 2024, especialmente o Regulamento (UE) 2024/1624, a aplicação da *travel rule* tornou-se obrigatória para criptoativos, reforçando a estrutura regulatória da UE contra o BCFT. A nosso ver, este regulamento, juntamente com outras medidas, representa um passo significativo para aumentar a transparência e a segurança no uso de criptoativos dentro da União Europeia.

[112] Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401640 [consultado em 18.08.2024].

Esta nova diretiva visa, essencialmente, agrupar a matéria relativa à organização das autoridades nacionais competentes no combate ao BCFT e inclui, em grande medida, requisitos para as autoridades de supervisão e as UIFs.

Tem em vista melhorar a organização dos sistemas nacionais de combate ao BCFT, estabelecendo regras claras sobre o modo como colaboram as UIFs, os organismos nacionais que recolhem informações sobre atividades financeiras suspeitas ou invulgares nos Estados-Membros e as autoridades de supervisão.

Estabelece também várias medidas aplicáveis aos setores suscetíveis de BCFT a nível nacional, tais como a obrigação de registar, identificar e controlar os gestores de topo e os beneficiários efetivos das entidades obrigadas. Obriga também à criação de registos de beneficiários efetivos e de contas bancárias e impõe obrigações específicas às UIFs e aos organismos que supervisionam as entidades obrigadas.

- **Diretiva (UE) 2024/1654, de 31 de maio de 2024**[113], que altera a Diretiva (UE) 2019/1153 no que diz respeito ao acesso pelas autoridades competentes a registos centralizados de contas bancárias através do sistema de interconexão e às medidas destinadas a facilitar a utilização dos registos de transações.

Em relação às informações sobre contas bancárias é importante ressalvar que o quadro atual exige que os Estados-Membros criem mecanismos automatizados centralizados (tais como registos centralizados ou sistemas EDR) para identificar quem controla efetivamente as contas bancárias.

O novo pacote alarga a informação a incluir nos registos centrais de modo a incluir questões de segurança e contas de criptoativos. Estabelece igualmente a obrigação de dispor de mecanismos automatizados centralizados.

A Comissão Europeia criará o Sistema de Interconexão de Contas Bancárias (BARIS, do inglês *bank account registers interconnection system*), que entrará

[113] Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401654 [consultado em 18.08.2024].

em funcionamento, o mais tardar, a 10 de julho de 2029. O AMLA, as UIFs nacionais e as autoridades de controlo de PBCFT dos Estados-Membros terão acesso a este sistema.

Os Estados-Membros devem transpor esta diretiva o mais tardar até 10 de julho de 2027.

Podemos desta forma concluir que, com a entrada em vigor deste novo pacote, serão alcançados determinados objetivos que estavam, até então, a ser amplamente criticados, inclusivamente por nós, na elaboração deste trabalho.

O pacote modifica, substantivamente, o regime operacional das entidades obrigadas, através do estabelecimento de um conjunto de regras comuns para todos os Estados-Membros no combate ao BCFT, pela criação de uma nova autoridade de supervisão e, não menos relevante, pela previsão e exigência de cumprimento de novos requisitos da diligência devida no contexto da PBCFT.

Em primeiro lugar, ficou acautelada a criação de um regulamento europeu único em matéria de PBCFT que reunisse todas as normas que regulam esta matéria. Este avanço representa a passagem de um modelo baseado exclusivamente em diretivas para um modelo baseado num regulamento único, com exceção, obviamente, dos aspetos que continuam a ser regulados por diretivas após a harmonização. As regras aplicáveis ao setor privado serão transferidas para o Regulamento relativo à prevenção da utilização do sistema financeiro para efeitos de BCFT, diretamente aplicável, enquanto a matéria da organização das autoridades nacionais competentes no combate ao BCFT para as Diretivas.

Também se materializará, finalmente, a supervisão da luta contra o BCFT a nível da União Europeia e o reforço da cooperação e coordenação entre as autoridades nacionais, bem como a criação de um mecanismo de apoio e colaboração entre estas (através da AMLA).

Na nossa ótica, o surgimento desta Autoridade constitui a maior prova do reconhecimento da União Europeia quanto à necessidade de adotar uma abordagem holística e harmonizada dos múltiplos e, muitas vezes,

descoordenados esforços, que os diferentes países têm vindo a desenvolver neste contexto.

Ficarão, assim, resolvidos certos problemas trazidos pelo quadro anterior. Note-se que a regulamentação da matéria através de diretivas revelou-se problemática, uma vez que as diretivas têm de ser transpostas para o direito nacional, o que exige tempo para que seja efetivamente aplicada. Além disso, como a diretiva não era suficientemente pormenorizada, os Estados-Membros acabaram por aplicar quadros divergentes.

Por outro lado, dado que não existia uma supervisão centralizada ao nível europeu em matéria de PBCFT, as autoridades nacionais e as UIFs tinham dificuldade em cooperar entre si e, por conseguinte, o combate à criminalidade organizada não era eficaz.

Valorizamos, portanto, o esforço de harmonização da regulamentação europeia e louvamos, igualmente, a tentativa de aumentar a transparência e o acesso aos registos centrais dos beneficiários efetivos. A existência de lacunas legais, disposições ambíguas, pouco claras e coerentes, a supervisão insuficiente no mercado interno e a falta de coordenação na troca de informações entre as UIFs de cada Estado-Membros, eram fragilidades utilizadas pelos criminosos.

É igualmente digno de nota que, apesar de o novo e ambicioso quadro regulatório ser altamente exigente, o legislador europeu tomou a precaução de suavizar a sua implementação pelos diversos Estados-Membros. De forma sábia e prudente, foi prevista uma entrada em vigor gradual, garantindo assim as condições necessárias para que os procedimentos internos possam ser adequados às novas exigências regulatórias. Dessa forma, minimiza-se o risco de incumprimentos e das consequentes penalidades financeiras e sanções administrativas que, habitualmente, lhes estão associadas.

Por agora resta-nos esperar para saber de que forma é que estas ideias serão efetivamente concretizadas, se resolverá os problemas que têm vindo a ser detetados (ou se, porventura, se encontrarão outros) e se os Estados-Membros estão preparados para adotar estes mecanismos e retirar o melhor proveito deles. As legislações locais relativas a BCFT terão de ser alteradas (ou

revogadas, embora o mais recente Aviso do Banco de Portugal já tenha acautelado uma série de questões a prever a entrada em vigor deste pacote legislativo) uma vez que as regras de prevenção serão incorporadas no regulamento e serão diretamente aplicáveis em todos os Estados-Membros. As empresas que estão sujeitas ao novo regime, onde se inclui a *Luso Digital Assets*, terão de considerar as suas políticas e práticas existentes e fazer as alterações necessárias para garantir que estão em condições de cumprir o novo panorama legislativo.

5. Legislação específica para as entidades que exercem atividades com ativos virtuais

O Banco de Portugal (BdP) é a autoridade responsável pela supervisão das entidades que exercem atividades com ativos virtuais, no que diz respeito ao cumprimento das regras de PBCFT.

As entidades que exercem atividades com ativos virtuais em Portugal, como *exchanges*, plataformas de custódia e prestadores de serviços de carteira, são, portanto, obrigadas a registar-se no BdP e a cumprir um conjunto de obrigações, tais como, implementar medidas de diligência devida aos seus clientes, monitorizar as transações realizadas pelos seus clientes e comunicar transações suspeitas às autoridades competentes.

O registo, como já vimos, deriva da Recomendação do GAFI 2019a, que recomendou a todos os países obrigações de registo ou licenciamento das entidades que exercem atividade com ativos virtuais e, nessa medida, surgiu o Aviso do Banco de Portugal n.º 3/2021, que regula o processo de registo e de alteração das entidades que exercem atividade com ativos virtuais, junto do Banco de Portugal.

Mais tarde, no dia 24 de janeiro de 2023, é publicado em Diário da República o Aviso n.º 1/2023 do BdP em matéria de PBCFT, particularmente focado no setor dos ativos virtuais. O projeto deste Aviso havia sido submetido a consulta pública e recebeu ainda parecer favorável da Comissão Nacional de Proteção de Dados.

Este Aviso regulamenta matérias previstas na Lei n.º 83/2017, de 18 de agosto (“Lei do BCFT”), bem como na Lei n.º 97/2017, de 23 de agosto (Lei n.º 97/2017), que regula a aplicação e a execução de medidas restritivas aprovadas pela Organização das Nações Unidas ou pela União Europeia e estabelece o regime sancionatório aplicável à violação destas medidas. Neste sentido, o Aviso veio adaptar à realidade das entidades que exercem atividades com ativos virtuais as disposições do Aviso n.º 1/2022, de 6 de junho que, na mesma matéria, regula os deveres a que estão sujeitas as entidades financeiras alvo de supervisão pelo BdP. Este Aviso surge ainda na sequência do Aviso n.º 3/2021,

de 23 de abril, que veio regular o procedimento de registo junto do BdP e dos VASP, obrigatório em virtude do artigo 112.º-A da Lei do BCFT, denotando uma crescente regulamentação de um setor associado a um considerável risco de prevenção do BCFT.

Esta crescente regulamentação acompanha uma tendência global, sendo cada vez mais frequentes as sanções relacionadas com a violação de deveres de prevenção do BCFT nesta indústria. Casos como o da *Coinbase*, uma plataforma de compra e venda de criptomoedas norte-americana que acedeu ao pagamento de 50 milhões de dólares ao Departamento Financeiro de Nova Iorque (NYDFS) por não ter adequadamente implementado um sistema de deteção de atividade ilegal, devendo ainda investir pelo menos 50 milhões de dólares no desenvolvimento de um sistema adequado de *compliance*, vêm expandindo a dimensão sancionatória que as entidades reguladoras podem exercer sobre este setor.

Os destinatários deste novo Aviso são as entidades que exercem, em território nacional, atividades com ativos virtuais (cf. o n.º 6 do artigo n.º 4 da Lei do BCFT, em articulação com as alíneas ll) e mm) do n.º 1 do artigo 2.º da Lei de prevenção do BCFT, bem como com o n.º 1 do artigo 2.º, alínea k) do Aviso), como tal registadas no BdP (cf. artigo 112.º-A da Lei do BCFT e Aviso n.º 3/2021). As entidades não sedeadas em território nacional são consideradas "entidades de natureza equivalente" (cf. artigo n.º 2, n.º 1, alínea l), do Aviso) e, embora não estejam sujeitas às disposições do Aviso, a relação de negócio entre estas entidades em território nacional é regulada em alguns aspetos, nomeadamente no que se refere à implementação de medidas de diligência reforçada no âmbito da relação estabelecida.

Este Aviso foi altamente inovador, pois teve ainda como finalidade a harmonização da legislação nacional com o enquadramento internacional de combate ao BCFT, refletindo antecipadamente algum do conteúdo que se constatou vir a integrar o regime legal decorrente do Novo Pacote Legislativo de combate ao BCFT ao nível da União Europeia, que foi recentemente aprovado. É também influenciado pela recomendação 15 do GAFI, revista em 2018 para incluir os VASP, bem como pelas orientações do GAFI, em documento designado *Updated Guidance for a Risk-Based Approach to Virtual Assets and*

Virtual Asset Service Providers, de 2021, conforme decorre, desde logo, da introdução da *travel rule*, tal como recomendado pela organização.

O objetivo do Aviso consiste em definir os procedimentos, os instrumentos, os mecanismos, as formalidades de aplicação, as obrigações de prestação de informação e os demais aspetos necessários ao cumprimento dos deveres preventivos associados ao combate ao BCFT, numa área identificada como tendo riscos de BCFT potencialmente mais elevados e em que a experiência de cumprimento destes deveres preventivos é relativamente recente – não fossem as particularidades associadas ao dever de registo junto do BdP terem sido reguladas no Aviso n.º 3/2021 do BdP, que apenas entrou em vigor a 14 de abril de 2021 – conforme se pode inferir na Nota Justificativa ao Projeto de Aviso.

O Aviso traduz, assim, dois principais objetivos, na sua articulação com o enquadramento legislativo com vista ao combate do BCFT:

- Clarificar o modo de aplicação das disposições da Lei de PBCFT e da Lei n.º 97/2017 ao setor dos VASP, tendo em conta os seus riscos concretos e as particularidades técnicas do setor, espelhando a regulamentação já prevista para as entidades financeiras no Aviso n.º 1/2022;
- Introduzir elementos inovadores no enquadramento legislativo, específicos à realidade operativa do setor dos VASP.

Em particular, este Aviso veio regulamentar a forma de execução dos deveres preventivos de BCFT por parte dos VASP sujeitos à supervisão do BdP para efeitos de PBCFT. A este propósito salientamos, em concreto, as seguintes disposições relevantes:

- O dever de definir e implementar uma função de controlo do cumprimento do quadro normativo preventivo do BCFT. Deve ainda garantir-se a segregação desta função das próprias funções que o controlo de cumprimento monitoriza, com exceção das entidades com um número de colaboradores inferior a seis (excluindo os administradores) e em que os proveitos operacionais no último exercício económico sejam inferiores a

1.000.000€ (cf. artigo 3.º do Aviso). Este acréscimo no que toca às funções de controlo para efeitos de prevenção do BCFT reflete-se ainda na necessária designação de um Responsável pelo Cumprimento Normativo, que deve exercer funções em regime de exclusividade (cf. artigo 5.º do Aviso, em conjugação com o artigo 16.º da Lei do BCFT);

- Embora seja agora admissível na generalidade, a subcontratação de processos, de serviços ou de atividades para cumprimento destes deveres encontra-se submetida a um conjunto de regras, incluindo a impossibilidade de excluir a responsabilidade do VASP, o impedimento de subcontratação quando esta possa diminuir a qualidade das medidas, o dever de analisar os riscos subjacentes à própria subcontratação, tendo em conta as políticas preventivas de BCFT e o enquadramento legislativo em que se insere a entidade subcontratada, entre outras (cf. artigo 16.º do Aviso);
- Foi também introduzida a possibilidade de os VASP recorrerem à videoconferência como possível meio de comprovação dos elementos identificativos recolhidos no âmbito do cumprimento do dever de identificação e de diligência nos termos do artigo 25.º da Lei de prevenção do BCFT, podendo agora ser utilizado tanto pelos próprios VASP como por via de entidades subcontratadas, nos casos admissíveis e mediante o cumprimento de várias salvaguardas e requisitos prévios, técnicos e gerais;
- O dever de identificação e diligência quanto a clientes é atualizado conforme a realidade particular do setor, sugerindo-se o uso de ferramentas adequadas para a determinação da origem e de destino dos fundos e ativos virtuais (tais como ferramentas de análise de redes ou históricos de operações associados a endereços ou *wallets*, por exemplo) (cf. artigo 24.º do Aviso). Limita-se ainda o tipo de operações que podem ser realizadas sem proceder à identificação do cliente a um elenco muito reduzido (cf. artigo 24.º do Aviso). Os meios comprovativos de elementos de identificação disponíveis são os mesmos que já se encontram previstos para o setor financeiro (cf. artigo 21.º do Aviso);
- Prescreve-se, além disso, um maior controlo sobre a origem e o destino dos ativos virtuais, sendo que certas informações sobre o ordenante e o

beneficiário devem agora, obrigatoriamente, acompanhar a transferência destes (cf. artigos 37.º a 40.º do Aviso), em aplicação da chamada *travel rule* proposta pelo GAFI na sua recomendação 15;

- A obrigação concreta de proceder à identificação e subsequente avaliação de fatores de risco específicos deste setor (cf. artigo 7.º do Aviso), com base na identificação feita pelo GAFI.

A violação dos deveres preventivos por parte dos VASP poderá constituir contraordenação, nos termos dos artigos 169.º e 169.º-A, punível com coima até 1.000.000€ (cf. artigo 170.º da Lei do BCFT).

O Aviso entrou em vigor no dia 15 de julho de 2023, com exceção da utilização de videoconferência como meio de comprovação de elementos identificativos (cf. subalínea i) da alínea c) do n.º 4 do artigo 25.º do Aviso), a qual pode, desde logo, ser utilizada.

Capítulo III - O crime de branqueamento através de criptoativos

1. Impulsionadores da prática do crime

Não há dúvidas que o alcance global, a rapidez com que as transações podem ser realizadas e a possibilidade de anonimato oferecidas pelos ativos virtuais os tornam particularmente vulneráveis ao uso indevido para fins criminosos.

A tecnologia *blockchain* permite que os utilizadores armazenem criptoativos nas suas carteiras digitais e realizem transferências P2P (*peer-to-peer*) sem limites pré-estabelecidos. A ausência de regulamentação e a preservação do anonimato reduzem a necessidade das técnicas tradicionais de ocultação de ativos ilícitos, uma vez que a aquisição de outros bens e valores pode ser efetuada diretamente com criptoativos, sem retorno ao sistema financeiro convencional (fase da integração do branqueamento de capitais).[114]

JOSÉ FONTES e NÉLSON DA CRUZ[115] sublinham que o desenvolvimento de software de anonimização, como as redes P2P (*peer-to-peer*) e o uso de criptoativos criaram um ambiente propício para organizações criminosas, facilitando o acesso aos mercados ilícitos na *darkweb*, mesmo para aqueles sem conhecimentos avançados de informática. Assim, as organizações criminosas têm migrado dos mercados ilícitos tradicionais para esses ambientes digitais, visando dificultar a deteção pelas autoridades e ampliar o seu alcance junto a potenciais clientes, estabelecendo simultaneamente uma relação de confiança.

Dessa forma, os principais facilitadores para a prática de crimes incluem a descentralização, o anonimato e a natureza global dos criptoativos.

[114] BARROS, Marco António de – Lavagem de capitais: Crimes de Lavagem, Procedimento Penal Especial, Protocolos Administrativos e Preventivos, p. 89 e 90.
[115] FONTES, José e CRUZ, Nelson da – Contributo para a Sustentabilidade dos Estados e das Democracias, p. 32 e 33.

A descentralização das criptomoedas significa que não existe uma entidade central responsável por controlar ou monitorizar as operações, o que impede a identificação e o reporte de transações suspeitas, exceto no caso das *exchanges*, onde há interação com o mundo “real” e, portanto, uma possibilidade de investigação. Nas transações entre os utilizadores, não há mecanismos para rastrear diretamente as operações. Com a ausência de uma autoridade central para emitir ou regular essas moedas, as transações e a criação de novas unidades ocorrem através de um sistema descentralizado.

As operações com criptomoedas proporcionam um alto grau de privacidade, o que é particularmente relevante no contexto da investigação de crimes como o branqueamento de capitais. Não é necessário que uma pessoa se identifique para criar uma conta e uma mesma pessoa pode possuir múltiplos endereços de criptomoedas, aumentando ainda mais o anonimato das transações.

Embora todas as transações sejam registadas na *blockchain*, o que possibilita rastrear todo o histórico de transações, a identificação dos titulares desses endereços só pode ser realizada por terceiros, como as *exchanges.* A globalidade das criptomoedas caracteriza-se pela capacidade de realizar transações sem barreiras ou controlo centralizado. Isso significa que as criptomoedas facilitam a transferência de fundos através de fronteiras internacionais sem a necessidade de intermediários financeiros, como os bancos. Consequentemente, o dinheiro ilícito pode ser movimentado rapidamente e de forma menos percetível entre países, o que torna a deteção e a investigação por parte das autoridades mais difícil.

2. Criptoativos e o procedimento do branqueamento de capitais

Como já discutido, a "lavagem de dinheiro" é um dos riscos potenciais do uso de criptoativos. A facilidade com que os criptoativos, especialmente criptomoedas, podem ser adquiridos com dinheiro de origem ilícita permite que a tecnologia blockchain seja explorada para "limpar" esses fundos.

Muitas operações envolvendo, por exemplo, a *bitcoin* (BTC) podem enquadrar-se na tipificação do crime de branqueamento, cumprindo as três fases

descritas no artigo 368º-A do Código Penal (colocação, circulação e integração das vantagens obtidas ilicitamente com o objetivo de ocultar bens, capitais ou produtos com a finalidade de lhes dar uma aparência final de legitimidade, procurando dissimular a sua origem criminosa). Em qualquer uma dessas etapas, pode ocorrer a ocultação dos fundos investidos em criptoativos, preenchendo o tipo objetivo do crime, que inclui: (1) converter, (2) transferir, (3) auxiliar ou facilitar a conversão ou transferência de vantagens (obtidas por si ou por terceiros, direta ou indiretamente), (4) ocultar ou dissimular a verdadeira natureza dessas vantagens, e (5) adquirir, deter ou utilizar vantagens provenientes de um facto ilícito típico cometido por outrem.

Ao analisar o tipo legal mencionado, podemos enquadrar a aquisição de criptoativos como uma estratégia para "esconder" dinheiro de origem ilícita. Isso ocorre quando o agente utiliza esses fundos para adquirir uma quantidade de, por exemplo, BTC que corresponda ao valor das vantagens obtidas de forma ilícita, tentando assim ocultá-las. Neste contexto, as criptomoedas podem efetivamente romper qualquer vínculo entre os proventos ilícitos e o crime antecedente, representando uma transição do mundo físico para o virtual.

Com base na proteção do bem jurídico, que neste caso é a administração da justiça, dado que o objetivo do branqueamento é dificultar ou impedir a ação judicial e considerando que o crime de branqueamento é um crime de perigo abstrato, conclui-se que a utilização de ativos virtuais para dificultar a ação da justiça coloca em perigo esse bem jurídico protegido.

Assim, o crime de branqueamento pode ser considerado consumado a partir do momento em que a continuidade da *blockchain* é interrompida, impossibilitando a vinculação de um grupo específico de determinada criptomoeda a uma operação concreta. Mesmo que não haja uma lesão concreta ao bem jurídico, a conduta que impede a administração da justiça já configura o crime.

O tipo penal de branqueamento de capitais exige que as condutas recaiam sobre um objeto originado de crimes antecedentes e uma interpretação teleológica do termo "objeto" pode levar a entender as criptomoedas como equivalentes ao dinheiro. Além disso, o pseudo-anonimato dessas transações é

compatível com a ausência da necessidade de identificação dos autores ou do local da prática do crime antecedente para que exista a punição do crime de branqueamento.

Na fase de colocação, de acordo com TEICHMANN e FALKER[116], os criminosos adquirem criptomoedas com os lucros obtidos de atividades ilícitas. Para realizar essa aquisição de forma anónima é comum utilizarem mercados de câmbio situados em jurisdições com legislação insuficiente contra o BCFT, bem como ATMs (máquinas automáticas) que, por serem amplamente disponíveis, facilitam as transações e permitem a criação de novas carteiras virtuais.

Daqui resulta uma outra grande dificuldade do combate ao BCFT, que é a facilidade de movimentação dos fundos entre países e a escolha do local para praticar o crime, consoante a legislação que lhe for mais favorável. Arthur Budovsky, fundador da *Liberty Reserve*[117]*,* renunciou à sua cidadania norte-americana e mudou-se para a Costa Rica, onde criou o seu negócio intencionalmente fora dos Estados Unidos, com o objetivo de contornar a legislação americana.

Outras práticas incluem a aquisição de criptomoedas através de *exchanges* ou transações diretas entre usuários, além da venda direta de bens obtidos de atividades criminosas em troca de criptomoedas ou ainda a compra de criptomoedas com o produto do crime[118].

Na fase de circulação, o criminoso realiza transações para ocultar a origem dos fundos. Embora a blockchain garanta a rastreabilidade das transações, a identificação dos usuários é dificultada pelo facto de os endereços se resumirem

---

[116] TEICHMANN, Fabian Maximilian Johannes & FALKER, Marie-Christin – "Cryptocurrencies and financial crime: solutions from Liechtenstein" *in* Journal of Money Laundering Control, p. 775-788.

[117] A *Liberty Reserve* foi um processador de pagamentos e troca de moeda que não utilizava ferramentas anti-BCFT, como os processos de *Know Your Customer* (KYC). A plataforma apenas solicitava informações básicas como nome, morada e data de nascimento dos seus usuários, permitindo transações sem uma verificação rigorosa. Este cenário facilitou a utilização da plataforma para atividades ilícitas, o que resultou no seu encerramento pelas autoridades em 2013 e numa condenação de 20 de prisão para o fundador. Disponível em: https://www.publico.pt/2016/05/07/economia/noticia/fundador-da-liberty-reserve-condenado-a-20-anos-de-prisao-1731261 e https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years [consultados em 18.08.2023].

[118] ESTELLITA, Heloísa – Criptomoedas e lavagem de dinheiro, *in* "Revista Direito GV", 2020, [disponível em https://www.academia.edu/51716693/Criptomoedas_e_lavagem_de_dinheiro, consultado em 18.08.2024].

a algoritmos, tornando mais difícil a identificação dos titulares. Existem vários métodos que aumentam o nível de ocultação das operações com BTC, como os *mixers* (também conhecida como *tumbler* ou serviço de mistura de criptomoedas), onde as criptomoedas obtidas de forma ilícita são trocadas por outras "limpas".[119]

Segundo Teichmann & Falker[120], o processo de circulação pode ser realizado usando navegadores focados na privacidade, como o *Tor Browser*, e redes virtuais privadas (VPNs), o que adiciona outra camada de anonimato e dificulta a identificação do autor das transações.

Na fase de integração, as criptomoedas são convertidas diretamente em moeda fiduciária ou utilizadas para comprar bens e serviços. Essa etapa final goza das mesmas vantagens da fase de integração, pois a venda das criptomoedas pode ser feita pelos mesmos meios utilizados para a sua aquisição, como *exchanges* e ATMs.

Uma das maiores dificuldades na investigação do crime de branqueamento de capitais surge quando os crimes subjacentes ou as etapas do processo de branqueamento ocorrem através de redes digitais específicas no ambiente cibernético. Na atual situação de quase total liberdade no ambiente virtual, apesar de muitas transações legítimas ocorrerem, a falta de regulamentação em certas atividades tecnológicas prejudica a fiscalização, investigação e aplicação da justiça, além de dificultar a recuperação de valores obtidos ilegalmente.[121]

[119] FONTES, José e CRUZ, Nelson da – Contributo para a Sustentabilidade dos Estados e das Democracias, p. 38.
[120] TEICHMANN, Fabian Maximilian Johannes & FALKER, Marie-Christin – "Cryptocurrencies and financial crime: solutions from Liechtenstein" *in* Journal of Money Laundering Control, p. 775-788.
[121] BARROS, Marco António de – Lavagem de capitais: Crimes de Lavagem, Procedimento Penal Especial, Protocolos Administrativos e Preventivos, p. 88 e 89.

3. Deveres preventivos

No sentido de evitar a ocorrência do crime de branqueamento através de criptoativos, foram instituídos deveres preventivos, entre os quais:

Dever de controlo

O dever de controlo vem previsto entre os artigos 12º a 22º da Lei e consiste no dever de as entidades obrigadas definirem e aplicarem, de forma eficaz e em permanência, as políticas, procedimentos e controlos que se mostrem adequados para:

- gerir os riscos de BCFT a que entidade obrigada esteja ou venha a estar exposta;
- dar cumprimento às normas legais e regulamentares em matéria de prevenção do BCFT;
- assegurar o cumprimento das medidas restritivas de congelamento de bens e recursos económicos, adotadas pelo Conselho de Segurança das Nações Unidas ou pela União Europeia e relacionadas com o terrorismo, com a proliferação de armas de destruição em massa e com o respetivo financiamento.

Tais políticas, procedimentos e controlos devem ser:

- proporcionais à natureza, dimensão e complexidade da entidade obrigada e da atividade por esta prosseguida;
- no caso de entidades obrigadas que façam parte de um grupo, aplicadas transversalmente ao nível do grupo, com partilha, no seio do mesmo, de toda a informação relevante para a prevenção e combate ao BCFT.

Na *Luso Digital Assets*, este dever era exercido logo no momento do *onbording*, que era obrigatório para todos os clientes e permitia, através de procedimentos de KYC (*Know Your Customer*) e CDD (*Customer Due Diligence*), avaliar o cliente como de alto ou baixo risco. A partir desta avaliação, eram aplicadas as medidas e diligências adequadas que se justificassem. Esta

informação fica gravada e pode ser encontrada em qualquer momento, bastando para isso pesquisar pelo nome do cliente ou filtrar consoante o que se pretenda encontrar.

Dever de identificação e diligência

A Lei n.º 83/2017 unificou o que na Lei n.º 25/2008, de 5 de junho, eram os deveres autonomizados de identificação e diligência, regulando agora nos seus artigos 23º a 42º um dever único de identificação e diligência.

Este dever estipula que as entidades obrigadas devem observar procedimentos de identificação e diligência – relativamente aos clientes, aos respetivos representantes e aos beneficiários efetivos – quando:

a) Estabeleçam relações de negócio;

b) Efetuem transações ocasionais:

i) de montante igual ou superior a 15.000€ (independentemente de a transação ser realizada através de uma única operação ou de várias operações aparentemente relacionadas entre si);

ii) que constituam uma transferência de fundos de montante superior a 1 000 euros;

iii) de montante igual ou superior a 2.000€ (independentemente de a transação ser realizada através de uma única operação ou de várias operações aparentemente relacionadas entre si), no caso específico dos concessionários de exploração de jogo em casinos, (concessionários de exploração de salas de jogo do bingo, entidades pagadoras de prémios de apostas e lotarias e entidades abrangidas pelo Regime Jurídico dos Jogos e Apostas Online, aprovado pelo Decreto-Lei n.º 66/2015, de 29 de abril;

c) Se suspeite que as operações, independentemente do seu valor e de qualquer exceção ou limiar, possam estar relacionadas com o branqueamento de capitais ou com o financiamento do terrorismo;

d) Existam dúvidas sobre a veracidade ou a adequação dos dados de identificação dos clientes previamente obtidos.

Em complemento dos procedimentos de identificação, as entidades obrigadas devem ainda:

- obter informação sobre a finalidade e a natureza pretendida da relação de negócio;
- obter informação sobre a origem e o destino dos fundos movimentados no âmbito de uma relação de negócio ou na realização de uma transação ocasional, quando o perfil de risco do cliente ou as características da operação o justifiquem;
- manter um acompanhamento contínuo da relação de negócio, a fim de assegurar que as operações realizadas no decurso dessa relação são consentâneas com o conhecimento que a entidade tem das atividades e do perfil de risco do cliente e, sempre que necessário, da origem e do destino dos fundos movimentados.

Adequando esta questão à realidade da *Luso Digital Assets*, importa mencionar que o facto de a contratação ser sempre feita à distância (artigo 38.º da LBCFT) implica a adoção de medidas reforçadas, segundo o artigo 36.º, n.º 2 da LBCFT. No n.º 6 do referido artigo, é dado um elenco de exemplos – não taxativo – de medidas reforçadas, que podem ser aplicadas pelas entidades obrigadas e que nos parece, de certa forma, um corolário do dever específico de identificação e diligência.

Desta forma, todos os clientes eram assumidos como de alto risco, pelo que eram implementadas medidas de conformidade mais intensas, de forma a garantir a segurança de todo o sistema. Não era apenas verificada a identidade dos clientes (que incluía nome, morada, profissão, dados do documento de identificação e informações empresariais relevantes), como eram muitas vezes requeridas informações adicionais sobre estes, os seus representantes ou beneficiários efetivos, bem como sobre as operações planeadas ou realizadas.

Algo que constatamos, infelizmente com alguma frequência, era a pretensão de pessoas da terceira idade (mais de 80 anos) de realizar transferências para compra e/ou venda de ativos virtuais. Quando isto acontecia, era agendada uma

videochamada com o cliente no sentido de apurar se seria sua a verdadeira intenção de fazer aquela transferência e se estava consciente do que se tratava e dos respetivos riscos.

As transações dos clientes eram monitorizadas e acompanhadas pelos membros do departamento de *compliance* numa base contínua, de forma a verificar sinais de atividade criminosa. A título de exemplo, levantava suspeitas quando uma ou várias transferências rondavam valores perto dos 10.000€, não chegando a alcançar este valor (como 9.990€ ou 9.950€), pois poderiam indicar que, talvez por ter origem ilícita, o cliente não queria indicar *Source of Funds*.

Dentro deste dever, é importante salientar as dificuldades na identificação de duas categorias de indivíduos: as Pessoas Politicamente Expostas (PEP) e os Beneficiários Efetivos (BEF) de pessoas coletivas[122].

Constatamos um reforço de zelo do dever de identificação e diligência, tanto para o caso dos PEP's, como para os membros próximos da família e pessoas reconhecidas como estreitamente associadas.

O artigo 19º, para o qual se remete, impõe às entidades obrigadas a aplicação de procedimentos e sistemas de informação adequados e baseados no risco, que permitam aferir ou detetar a qualidade de PEP antes do estabelecimento da relação de negócio ou no decurso da mesma. Isto tem muita relevância prática, porque quer dizer que a Lei encarrega as entidades obrigadas a adotarem procedimentos ou sistemas de informação adequados para elas próprias detetarem que um cliente seu é PEP.

Por último, é importante referir que na realidade da *Luso Digital Assets*, o que acontece é que um programa de *software* faz o encontro automático de possíveis PEP's com o nome do cliente, aquando do *onbording*. É necessário, posteriormente, fazer uma averiguação de se de facto o cliente corresponde à pessoa detetada como PEP, passando este processo, muitas vezes, por fazer pesquisa na internet e por perguntar ao cliente. Tal como é estipulado na Lei, há depois a intervenção de um elemento da direção de topo para aprovação e,

[122] COSTA, João Neves da e NEVES, Mário – "Dificuldades e impossibilidades: Algumas notas práticas à aplicação da Lei n.º 83/2017, de 18 de junho, no contexto da atividade de *Compliance*" *in* "Novos Estudos sobre *Law Enforcement*, *Compliance* e Direito Penal", p. 202.

quando o valor que o cliente pretende transacionar é superior a 10.000 €, são adotadas medidas necessárias para conhecer e comprovar a origem do património e dos fundos (é pedida *Source of Funds* e comprovativo da *wallet*, o que também é criticável, mas desenvolveremos esta questão a seguir).

Dever de comunicação

O dever de comunicação está consagrado nos artigos 43º a 46º da LBCFT e é o dever de as entidades obrigadas, por sua própria iniciativa, informarem de imediato a Unidade de Informação Financeira (UIF) e o Departamento Central de Investigação e Ação Penal (DCIAP) sempre que saibam, suspeitem ou tenham razões suficientes para suspeitar que certos fundos ou outros bens, independentemente do montante ou valor envolvido, provêm de atividades criminosas ou estão relacionados com o financiamento do terrorismo, comunicando, para o efeito, todas as operações propostas, tentadas, em curso ou executadas.

Segundo a política da *Luso Digital Assets*, aquando da deteção de uma operação suspeita, o Responsável pelo Cumprimento Normativo recebe e avalia os relatórios internos sobre atividades suspeitas[123], decidindo se devem ou não ser formalmente comunicadas às autoridades. Em caso afirmativo, o mesmo realiza a comunicação formal (Comunicação de Operações Suspeitas - COS) em nome da *Luso Digital Assets*.

Em sentido mais lato, o dever de comunicação consagrado na Lei abrange ainda a comunicação, numa base regular:

- à UIF e ao DCIAP, das tipologias de operações definidas em portaria do ministro responsável pela área da justiça (comunicação sistemática de operações);
- ao Instituto dos Mercados Públicos do Imobiliário e da Construção (IMPIC), de informação sobre a atividade das entidades obrigadas

[123] Um exemplar do Relatório de Atividade Suspeita da *Luso Digital Assets* consta nos Anexos Documentais para consulta.

relacionada com (i) mediação imobiliária, (ii) compra, venda, compra para revenda ou permuta de imóveis, (iii) arrendamento e (iv) promoção imobiliária (comunicação de atividades imobiliárias).

Relativamente ao dever de comunicação, NUNO BRANDÃO[124] oferece uma perspetiva que nos parece relevante assinalar. O autor defende que, apesar de todas as obrigações visarem, naturalmente, o sucesso de programas de prevenção de branqueamento de capitais, é no cumprimento de um conjunto de deveres específicos que se joga o papel decisivo desse sucesso. Esses deveres são, no seu ponto de vista, o dever de exame, de informação e o de comunicação de operações suspeitas. O autor assinala ainda que para ele é, especificamente, no cumprimento do dever de comunicação que as instituições melhor contribuirão para a PBCFT, distinguindo-o do dever de informação, como melhor explicaremos adiante.

O dever de denúncia de operações suspeitas (que equivale, grosso modo, ao dever de comunicação) impõe também o dever de colaboração com as autoridades de luta contra o BCFT, que é outro dever assinalado na Lei e traduz-se na obrigação às entidades obrigadas de colaborar com as autoridades competentes, em contraposição a este dever de denúncia que impõe a obrigação de lhes comunicar, por iniciativa própria, quaisquer factos que indiciam operações de branqueamento de capitais[125].

Segundo NUNO BRANDÃO[126], existem três modelos de obrigação de comunicação. O primeiro é o da obrigação geral de comunicação, praticado nos EUA, pelo qual as instituições ficam vinculadas ao dever de comunicar todas as operações realizadas em numerário acima de determinado montante. No exemplo americano esse valor é de 10.000 dólares. É um sistema que acarreta custos elevados para pôr em prática, pois implica uma máquina administrativa que receba e processe todas as comunicações. O elevado número de

[124] BRANDÃO, Nuno - Branqueamento de Capitais: O Sistema Comunitário de Prevenção, p. 38 e 39.
[125] Cfr. artigo 6º-1/a) da Diretiva 91/308/CE – que, apesar de se dirigir às entidades financeiras, o seu conteúdo é agora passível de ser aplicável a outras a outras entidades adstritas a essas mesmas obrigações, como é o caso das entidades não financeiras e, em particular, às entidades que exercem atividades com ativos virtuais.
[126] BRANDÃO, Nuno - Branqueamento de Capitais: O Sistema Comunitário de Prevenção, p. 38 e 39.

comunicações torna esta tarefa de procurar sinais de operações de BCFT em algo semelhante a procurar uma agulha no palheiro, sendo esta a principal crítica que se faz a este modelo.

Por esta razão, num segundo modelo, procurou-se filtrar as comunicações a montante, por parte das autoridades, consoante houvesse ou não a suspeita de BCFT. Foi este o caminho apontado pela Diretiva e é o modelo o que foi adotado em Portugal, na Alemanha, na França e no Reino Unido. É o designado modelo de obrigação de comunicação de operações suspeitas.

Pode haver, contudo, um terceiro modelo (sistema misto), aquele que nos parece mais razoável, pois combina-se as características dos dois modelos anteriores. Neste modelo, as entidades, além de ficarem obrigadas a comunicar operações suspeitas que tenham detetado, devem dar também conhecimento às autoridades de todas as transações em numerário acima de determinado montante. É o sistema adotado, por exemplo, na Itália e na Espanha.

NUNO BRANDÃO[127] distingue ainda o dever de comunicação do de informação, defendendo que é no cumprimento do primeiro que melhor se contribuirá para a PBCFT, pois é através deste dever que as entidades desempenham um papel ativo na deteção de operações de BCFT e colocam as autoridades no trilho dos esquemas de BCFT e das atividades criminosas a ele associadas. Este é um contributo cuja importância não pode ser ignorada, pois, na maior parte dos casos, será só através desta intervenção das entidades que os órgãos de investigação criminal tomarão conhecimento dessas operações, devendo, por isso, este contributo ser tanto quanto possível promovido e estimulado. Por seu turno, o cumprimento do dever de informação traduz já uma situação em que é a autoridade que se dirige à entidade, no sentido de recolher dados e elementos que permitam confirmar ou infirmar as suspeitas de BCFT que já recaiam sobre determinado indivíduo ou organização. Neste caso, a entidade já está numa posição passiva, aparecendo a imposição deste dever de informação como o instrumento que permite derrubar o obstáculo que se interpõe entre os investigadores e as informações, o segredo profissional. No entanto,

[127] BRANDÃO, Nuno - Branqueamento de Capitais: O Sistema Comunitário de Prevenção, p. 48 e 49.

nem esta distinção, nem o próprio dever de informação foram consagrados na Lei n.º 83/2017, parecendo-nos antes corresponder ao previsto dever de colaboração.

Dever de abstenção

Relativamente ao dever de abstenção, este vem previsto nos artigos 47º a 49º e impõe que as entidades obrigadas se abstenham de executar qualquer operação ou conjunto de operações, presentes ou futuras, que saibam ou que suspeitem poder estar associadas a fundos ou outros bens provenientes ou relacionados com a prática de atividades criminosas ou com o financiamento do terrorismo.

Dever de recusa

Quanto ao dever de recusa, consagrado no artigo 50º da Lei, é o dever de as entidades obrigadas recusarem iniciar relações de negócio, realizar transações ocasionais ou efetuar outras operações, quando não obtenham:

- os elementos identificativos e os respetivos meios comprovativos previstos para a identificação e verificação da identidade do cliente, do seu representante e do beneficiário efetivo, incluindo a informação para a aferição da qualidade de beneficiário efetivo e da estrutura de propriedade e de controlo do cliente; ou
- a informação prevista no artigo 27.º da Lei, sobre a natureza, o objeto e a finalidade da relação de negócio.

Dever de conservação

Este dever resultou, primeiramente, das Recomendações do GAFI de 2012[128] que estipulam um dever de conservação de, no mínimo, cinco anos, para todos os documentos referentes aos clientes e às transações efetuadas, tanto internas como internacionais, a fim de poderem responder rapidamente aos pedidos de informação das autoridades competentes. No documento mencionado exige-se ainda que estes documentos sejam "suficientes para permitir reconstituir as transações individuais (inclusive os montantes e tipos de divisa em causa, se for caso disso), de modo a fornecerem, se necessário, provas em processo de natureza criminal".

Dever de exame

Nas palavras de NUNO BRANDÃO[129], ao lado do dever de denúncia, tem de vir o dever de exame, pois não basta que sobre as entidades recaia um dever de comunicar operações suspeitas, se este dever, por si só, de pouco servirá se só as operações de tal modo evidentes é que acabariam por ser detetadas. Assim, deve recair também sob as entidades, a obrigação de analisar criteriosamente as operações em que intervêm. Não devem ser todas analisadas, sob pena de o cumprimento do dever de exame se conduzir ao imobilismo, mas pelo menos aquelas que possam ser idóneas a constituir operações de BCFT.

De facto, é neste sentido que o artigo 52º define o dever de exame como o dever de as entidades obrigadas analisarem com especial cuidado e atenção – intensificando o grau e a natureza do seu acompanhamento – quaisquer condutas, atividades ou operações cujos elementos caraterizadores as tornem suscetíveis de poderem estar relacionadas com fundos ou outros bens que provenham de atividades criminosas ou que estejam relacionados com o financiamento do terrorismo.

[128] Disponível em https://irn.justica.gov.pt/Portals/33/Internacional/Recomendacoes_GAFI_fev_2012.pdf?ver=2019-03-06-161917-790, p. 15.

[129] BRANDÃO, Nuno - Branqueamento de Capitais: O Sistema Comunitário de Prevenção, p. 39 e 40.

Contudo, também esta disposição, que mesmo já tendo sofrido alterações no sentido de ser mais clara, na nossa opinião, ainda é passível de críticas. Conforme aponta NUNO BRANDÃO[130], a propósito da anterior redação, a forma como esta norma foi redigida e os termos em que este dever de exame se deve verificar, pode dar origem a grandes incertezas.

Efetivamente, o facto de não se definir exatamente os termos e os elementos caraterizadores que tornam as tais operações suscetíveis de poderem estar relacionadas com BCFT, gera confusão, principalmente no plano prático. Parece já ter havido esforços no sentido de tornar a norma menos vaga, mas sabendo que o incumprimento deste dever de exame constitui um ilícito penal ou administrativo em todos os Estados-Membros, por via da Diretiva 2001/97/CE, importa questionar se continua a prevalecer o argumento de que se está a violar o princípio da legalidade pela indeterminação dos conceitos usados. Em que consiste o "especial cuidado e atenção"?

Na nossa visão, não constitui uma violação do princípio da legalidade e temos sérias dúvidas se seria benéfico o legislador consagrar algumas situações que, quando verificadas, caíam neste dever de exame. É certo que não se pode cair no exagero oposto de tentar fazer um catálogo exaustivo de situações suspeitas de BCFT, até porque o caráter volátil deste crime não o permite, uma vez que estão sempre a surgir novas formas de BCFT. Porém, a consagração de alguns exemplos de movimentos seria uma possibilidade, a nosso ver, para que as entidades obrigadas ganhassem alguma noção de formas usualmente utilizadas para efeitos de BCFT e despertassem a sua sensibilidade para outras. Contudo, pesando os prós e contras, não nos parece ser um argumento suficientemente forte para as consagras. Se assim fosse, as transações constantes dessa lista passariam a fazer parte da secção de "operações a evitar" de qualquer "manual de BCFT", pelo que poderia levar os branqueadores a procurarem ser mais criativos.

[130] BRANDÃO, Nuno - Branqueamento de Capitais: O Sistema Comunitário de Prevenção, p. 40 e 41.

MIGUEL DA CÂMARA MACHADO[131], a este propósito, admite que enquadrar estas situações torna-se necessário "para que, dentro do princípio da legalidade, seja possível punir e sancionar determinados comportamentos relacionados com BCFT". Contudo, reconhece que "esta vontade e necessidade de definir conceitos pode ser uma armadilha no combate ao BCFT, reveladora de alguns dos maiores paradoxos em que os desenhadores, intérpretes e aplicadores do Direito se encontram nestas matérias".

Parece-nos que a solução passa então, em primeiro lugar, por um efetivo conhecimento do cliente e das atividades a que ele se dedica e não pela tipificação das situações que podem revelar-se operações de BCFT. Na *Luso Digital Assets*, por exemplo, é pedida informação relativa à profissão do cliente. Em caso de suspeita de BCFT, são pedidos os extratos bancários do cliente, de forma a conhecer melhor a sua situação financeira, bem como a origem dos capitais que pretende usar nas transações.

Outro exemplo que era praticado regularmente na *Luso Digital Assets* relativo a este dever de exame é que quando o cliente tem mais do que 65 anos é feita uma vídeo chamada, no sentido de examinar a intenção do cliente, como é que ele teve conhecimento da atividade com ativos virtuais e procurar entender se o cliente está ciente do que está a fazer. O objetivo é tentar perceber se, de facto, é a vontade daquele cliente transacionar os ativos virtuais, ou se há outro beneficiário por detrás daquela transação que, talvez por estar sinalizado em "listas negras", não possa "aparecer" no sistema, que teria a sua transação recusada.

Noutra vertente, NUNO BRANDRÃO[132] adota uma posição com a qual já concordamos totalmente. O autor defende que o dever de exame deve dar lugar à denúncia sempre que as entidades saibam ou suspeitem da prática de operações BCFT. No fundo, é a concretização do segundo modelo de obrigação de comunicação que vimos a respeito do dever de comunicação. Conjugado este dever com o dever de exame, é possível adotar um sistema que, em relação ao

[131] MACHADO, Miguel da Câmara – "4G na prevenção do branqueamento de capitais: problemas, paradoxos e principais deveres" *in* "Estudos de Direito Bancário I", p. 78.
[132] BRANDÃO, Nuno - Branqueamento de Capitais: O Sistema Comunitário de Prevenção, p. 42 e 43.

modelo de obrigação geral de comunicação, tem a vantagem de evitar um fluxo exagerado de comunicações e de dar azo à quebra do sigilo profissional apenas quando sobre o cliente recaia uma suspeita fundada da realização de operações de BCFT. Há, porventura, o grande inconveniente que se prende com o problema de determinar em que casos se está perante uma transação suspeita. Quais os factos que podem configurar indícios de operações de BCFT? Se as entidades estão obrigadas a comunicar esses factos e podem ser punidas se não o fizerem, esta é uma questão que se impõe. A doutrina maioritária, embora identificando o problema, não adianta nenhuma via de solução, constatando que não há maneira de ultrapassar essa indeterminação, em virtude da extrema variedade de formas que podem assumir as operações de BCFT. A descrição de algumas técnicas habituais seria contraproducente; mas é, em todo o caso, pela divulgação dessas técnicas que tem passado o esforço de concretização do que é uma transação suspeita. A este respeito e visando colmatar esta problemática, a Diretiva 2001/97/CE consagrou um dever para os Estados-Membros de proporcionar às pessoas e entidades vinculadas ao sistema de prevenção o acesso a informações atualizadas sobre as práticas de BCFT e sobre os indícios que permitam identificar transações suspeitas[133].

Dever de colaboração

Já o dever de colaboração vem definido no artigo 53º da Lei e é o dever de as entidades obrigadas prestarem, de forma pronta e cabal, toda a colaboração que lhes for requerida pelo *Departamento Central de Investigação e Ação Penal* (DCIAP), pela *Unidade de Informação Financeira* (UIF) pelas demais autoridades judiciárias e policiais, pelas autoridades setoriais ou pela *Autoridade Tributária e Aduaneira*.

Já vimos que este dever está intimamente relacionado com o dever de comunicação, distinguindo-se deste no sentido em que são estipuladas obrigações específicas às entidades em matéria de colaboração, sendo exemplos: a resposta, de forma completa, aos pedidos de informação; a

[133] Cfr. artigo 11º-2 da Diretiva.

disponibilização de todas as informações que sejam requeridas; conferir, se for requerido, acesso remoto a essas informações; colaborar, plena e prontamente com as autoridades setoriais no exercício da sua atividade inspetiva, nomeadamente abstendo-se de qualquer recusa, facultando a inspeção de quaisquer instalações utilizadas, facultando cópias, extratos ou traslados de toda a documentação requerida, cumprindo integralmente as ordens ou instruções que lhes sejam dirigidas, entre outras.

No nº 4 o legislador faz uma ressalva de que o cumprimento deste dever não pressupõe o exercício prévio do dever de comunicação do artigo 43º, sem prejuízo da solicitação de quaisquer informações complementares.

Dever de não divulgação

O dever de não divulgação vem previsto no artigo 54º da Lei e consubstancia-se no dever de as entidades obrigadas - bem como os membros dos respetivos órgãos sociais, os que nelas exerçam funções de direção, de gerência ou de chefia, os seus empregados, os mandatários e outras pessoas que lhes prestem serviço a título permanente, temporário ou ocasional - não revelarem ao cliente ou a terceiros:

- que foram, estão a ser ou irão ser efetuadas comunicações ao abrigo dos artigos 43.º, 45.º, 47.º e 53.º da Lei n.º 83/2017, de 18 de agosto;
- quaisquer informações relacionadas com aquelas comunicações;
- que se encontra em curso, ou pode vir a encontrar-se, uma investigação ou inquérito criminal, bem como quaisquer outras investigações, inquéritos, averiguações, análises ou procedimentos legais a conduzir pelas autoridades judiciárias, policiais ou setoriais;
- quaisquer outras informações ou análises, de foro interno ou externo, que possam pôr em causa (i) o exercício das funções legalmente conferidas às entidades obrigadas e às autoridades judiciárias, policiais e setoriais ou (ii) a preservação de quaisquer investigações, inquéritos,

averiguações, análises ou procedimentos legais e a prevenção, investigação e deteção do BCFT, em geral.

Dever de formação

Por último, o dever de formação está previsto no artigo 55º da Lei e é o dever de as entidades obrigadas proporcionarem aos seus dirigentes, trabalhadores e demais colaboradores, cujas funções sejam relevantes para efeitos da PBCFT, um conhecimento adequado das obrigações decorrentes da Lei do BCFT e da respetiva regulamentação, através da realização de ações específicas e regulares de formação, adequadas a cada sector de atividade, que habilitem os mesmos, a todo o momento, a reconhecer operações que possam estar relacionadas com o BCFT e a atuar de acordo com o quadro normativo vigente.

Foi ao abrigo deste dever que preparámos diversas formações aquando do estágio na *Luso Digital Assets*.

3.1. Problemática da violação do dever de segredo e das denúncias anónimas

Para NUNO BRANDÃO[134], o cumprimento do dever de comunicação implica a violação do dever de segredo a que as entidades estão adstritas. Em virtude da enorme diversidade dos ordenamentos jurídicos dos Estados-Membros no que diz respeito à regulação do sigilo profissional, sua exoneração e exclusão de responsabilidade, esta norma[135] pretende impor expressamente a proibição de ser imputada aos destinatários do sistema de PBCFT qualquer responsabilidade pela divulgação às autoridades, realizada de boa-fé, de informações relativas a suspeitas de práticas de BCFT.

No entanto, segundo o autor, esta transposição da Diretiva para o nosso ordenamento não seria, em princípio, necessária, pois essa exoneração da responsabilidade decorreria já do princípio da unidade da ordem jurídica, pelo que a quebra do dever de segredo dever-se-ia considerar justificada em face do cumprimento de um dever legal que exclui a ilicitude penal e contraordenacional do facto. Não há, portanto, qualquer violação de um dever de segredo, pois nestas situações a entidade está obrigada a dar a conhecer factos relativos ao cliente, não devendo, por isso, guardar sigilo sobre eles. Existindo uma obrigação de denúncia, é óbvio que o cumprimento desses deveres não se pode traduzir na "violação de qualquer dever de segredo", porque esse dever nem sequer existe. A exclusão da responsabilidade funda-se numa exclusão da ilicitude[136].

Não obstante, o legislador português optou por deixar clara a exclusão de qualquer tipo de responsabilidade, apesar deste preceito já vir a ser criticado pela doutrina há vários anos. OLIVEIRA ASCENSÃO[137] define-o como "rigorosamente inútil" e acrescenta que "é claro que o cumprimento de um dever legal não pode implicar a violação de um dever de segredo; e que se não há

[134] BRANDÃO, Nuno - Branqueamento de Capitais: O Sistema Comunitário de Prevenção, p. 49-52.
[135] Que advém do artigo 9º da Diretiva 2001/97/CE.
[136] Cfr. alínea c) do n.º 2 do artigo 31º do CP.
[137] ASCENSÃO, José de Oliveira – "Branqueamento de Capitais: Reacção Criminal" *in* "Estudos de Direito Bancário", p. 353.

ilícito não pode haver responsabilidade". De facto, e ainda bastante atual, o autor referiu que "não há hoje qualquer tipo de segredo profissional que prevaleça sobre o combate ao branqueamento de capitais; pelo contrário, são as preocupações desta ordem que prevalecem sempre".

Noutra nota, o n.º 2 do artigo 56º da Lei n.º 83/2017 faz depender a exclusão da responsabilidade de uma atuação de boa-fé na disponibilização das informações[138]. Mais uma vez, segundo NUNO BRANDÃO, mesmo que esta exigência não tivesse sido expressamente imposta, resultaria já dos princípios gerais. Além disso, a justificação não é prejudicada pelo facto de uma vez levada a cabo a investigação da operação objeto de denúncia, se chegar à conclusão de que a transação não constituía, na verdade, uma operação de BCFT ou subsistirem fortes dúvidas em relação a isso. Suspeitando fundadamente da licitude da proveniência dos bens, a entidade tem o dever de comunicar esse facto às autoridades, constituindo isso fundamento bastante para que seja exonerada de qualquer responsabilidade pela revelação do segredo, mesmo que essa ilicitude não se venha efetivamente a provar ou se desconheça a concreta atividade criminosa em causa. Efetivamente, não seria razoável, nem compatível com a eficácia do sistema de PBCFT a defesa de outra solução.

Problemática diferente é a das denúncias anónimas (ou *whistleblowing*, cujos mecanismos tantas vezes se cruzam com o *Compliance*).

O *whistleblowing* é, nas palavras de NUNO BRANDÃO[139], "o termo, de origem norte-americana, com que, há longo tempo, é cunhada a actividade daquele que sinaliza um comportamento ilegal ou irregular ocorrido no quadro de uma organização, pública ou privada, com a qual tem ou teve algum vínculo". Os mecanismos de proteção dos *whistleblowers* foram sendo instituídos em vários países, um movimento que, no espaço da União Europeia, culminou na publicação da Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União.

[138] Este pressuposto tem a sua origem na Recomendação 16 do GAFI, p. 4.
[139] BRANDÃO, Nuno – O *whistleblowing* no ordenamento jurídico português, p. 99.

O termo foi utilizado pela primeira vez em 1963 por Otto Opeka, antigo membro do Departamento do Estado dos EUA, que foi demitido após entregar documentos confidenciais a um conselheiro do Senado, relativamente ao sistema de segurança interna do país[140].

O *whistleblowing* pode ocorrer no interior do ente coletivo em que o *whistleblower* se integra, mediante reporte de suspeitas de ilegalidades ou irregularidades à pessoa ou ao órgão internamente incumbido de receber participações dessa natureza (denúncia interna) ou pode o *whistleblower* comunicar a entidades externas, judiciárias ou administrativas, com competência para a investigação dos factos participados (denúncia externa), não havendo, em Portugal, um escalonamento das formas preferíveis de denúncia e não obstante qualquer pessoa que tenha conhecimento de um crime poder denunciá-lo ao Ministério Público (artigo 244º do CPP)[141]. O denunciante deve, em todo o caso, agir de boa-fé, perfilhando-se aqui a opinião de ANDRÉ ALFAR RODRIGUES[142] que defende que, quando haja de má-fé ou utilize os canais de denúncia para fins contrários aos que se destinam, o agente deveria ser responsabilizado.

Estes mecanismos relacionam-se com o *compliance* na medida em que surgiram como um meio de deteção de infrações penais ou administrativas. O *whistleblowing* é visto quer como um mecanismo para prevenir a prática de crimes da empresa, quer como um meio para aferir da existência e efetiva aplicação de um programa de *compliance* e, assim, decidir da sua eventual responsabilidade criminal[143].

A questão é que, na prática, esta figura não tem grande expressão e relevo em Portugal. O legislador e as autoridades públicas portuguesas estão, em larga medida, alheados à figura do *whistleblower*, a legislação é escassa, fragmentária e lacunosa e o seu *enforcement* pelas autoridades é débil e limitado. Para NUNO BRANDÃO[144], isto acontece por tratar-se de uma figura sem qualquer tradição

[140] RODRIGUES, André Alfar – Inteligência Artificial, *Compliance* e Responsabilidade das Pessoas Coletivas, p. 89.
[141] BRANDÃO, Nuno – O *whistleblowing* no ordenamento jurídico português, p. 102-110.
[142] RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 175.
[143] BRANDÃO, Nuno – O *whistleblowing* no ordenamento jurídico português, p. 107.
[144] BRANDÃO, Nuno – O *whistleblowing* no ordenamento jurídico português, p. 112 e 113.

na experiência portuguesa e pelo facto de nunca ter havido uma interiorização de que o *whistleblower* deveria ser acolhido e estimulado como um meio útil, virtuoso e desejável de prevenção e deteção de crimes.

Segundo MIGUEL DA CÂMARA MACHADO[145], esta questão das denúncias anónimas na Europa assume um cariz marcadamente filosófico e é resultado da História das ditaduras no nosso continente. Os portugueses, os alemães, os franceses e os fióis são avessos às denúncias anónimas pelos "traumas" resultantes do período pré- e pós-Segunda Guerra Mundial. Pelo contrário, nos EUA e em Inglaterra admite-se, aceita-se e fomenta-se denúncias anónimas (vejamos o caso *Enron*[146], nos EUA, que reforçou a necessidade deste mecanismo, pois acredita-se que só foi possível "desmontar" aquela estrutura criminosa com recurso a este instrumento). A experiência europeia aponta no sentido de que as denúncias anónimas são utilizadas para delatar vizinhos e familiares, talvez por, nestes países, se ter vivido ditaduras até há pouco tempo, pelo que há uma certa cultura europeia "continental" contra as denúncias anónimas.

De facto, aquando da experiência de estágio na *Luso Digital Assets*, constatou-se a existência de um canal para este efeito[147], mas que nunca tinha sido ativado. A nosso ver, trata-se de uma boa arma de apoio na luta contra o BCFT embora, na realidade laboral, praticamente não tenha sido ainda utilizada.

Estamos em crer que a simples existência deste canal de denúncia, além de servir o propósito de denunciar possíveis comportamentos ilegais e contrários aos regulamentos da empresa, serve como dissuasor de futuros comportamentos erróneos. Também o facto de o canal de denúncias poder ser instituído através de uma plataforma *web* comporta vantagens, desde logo

---

[145] MACHADO, Miguel da Câmara – "Contexto, evolução e tendências do *compliance* em Portugal e na Europa, em especial a partir do Aviso n.º 3/2020, de 15 de julho, do Banco de Portugal" *in* "Estudos sobre *Law Enforcement*, *Compliance* e Responsabilidade Empresarial", p. 176-177.

[146] BRATTON, William Wilson – Enron and the Dark Side of Shareholder Value. Artigo disponível em SSRN: https://ssrn.com/abstract=301475 or http://dx.doi.org/10.2139/ssrn.301475 [consultado em 19.04.2024].

[147] As entidades obrigadas têm o dever de criar canais específicos, independentes e anónimos que internamente assegurem, de forma adequada, a receção, o tratamento e o arquivo das comunicações de irregularidades relacionadas com eventuais violações em matéria de PBCFT, nos termos do artigo 20º da LBCFT.

porque a plataforma é separada e protegida de forma a não ter qualquer ligação aos sistemas informáticos da organização que recebe a denúncia, o que garante o anonimato e a confidencialidade, bem como a proteção do denunciante[148]. Concordamos, pois, que os canais de denúncia se afiguram extremamente vantajosos e relevantes para reduzir os riscos de *compliance* e de BCFT.

O que já não é consensual e suscita dúvidas quanto à sua razoabilidade é relativamente a exigir essa denúncia sobre colegas. Há relatos de empresas nos EUA onde os trabalhadores são sancionados por não terem denunciado colegas que estão a violar Códigos de Conduta na sua presença. Esta situação gera alguma polémica, pois um ambiente onde os trabalhadores são os polícias uns dos outros parece inconciliável com um bom ambiente de trabalho. No entanto, ao contrário do que defende MIGUEL DA CÂMARA MACHADO[149], não nos parece que, nesta questão, os regimes de combate ao BCFT tenham ido longe demais. Tratando-se da deteção de atividades de BCFT, um flagelo tão grande e de difícil deteção, parece-nos razoável exigir aos agentes responsáveis por "cumprir" os procedimentos no âmbito das suas empresas que sejam os primeiros a dar o exemplo e a fazer tudo o que tiver ao seu alcance para combater este problema, incluindo a denúncia de colegas, se tal for necessário, que eventualmente não estejam a cumprir deveres de PBCFT.

[148] RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 173.
[149] MACHADO, Miguel da Câmara – "Contexto, evolução e tendências do *compliance* em Portugal e na Europa, em especial a partir do Aviso n.º 3/2020, de 15 de julho, do Banco de Portugal" *in* "Estudos sobre *Law Enforcement*, *Compliance* e Responsabilidade Empresarial", p. 177.

4. Reporte de operações suspeitas: um valor aquém do esperado

Já vimos que sobre certas entidades recaem obrigações de reporte de operações suspeitas, entidades essas sujeitas a registo junto do Banco de Portugal. No entanto, se é verdade que cabe a estas entidades, em primeira linha, a denúncia dessas operações, também é verdade que tais denúncias são raras, havendo uma clara disfunção entre aquilo que devia ser o dever de denúncia e o uso cada vez mais frequente dos ativos virtuais para efeitos de BCFT.

A Quinta Diretiva AML veio, pela primeira vez, alargar o âmbito da sua aplicação de modo a incluir os prestadores cuja atividade consiste na realização de serviços de câmbio entre ativos virtuais e moedas fiduciárias, bem como os prestadores de serviços de custódia de carteiras digitais, criando obrigações de reporte às UIFs nacionais de operações suspeitas que, por via desse reporte, devem ser capazes de obter informações que lhes permitam associar endereços do ativo virtual à identidade do seu detentor[150].

Atualmente, a PBCFT está cometida, *prima facie*, ao DCIAP, junto do qual funciona a UIF. Em tempos, o regime jurídico que vigorava em Portugal era um sistema dual de comunicação de operações suspeitas, que implicava a comunicação para as duas entidades. Este sistema era criticado pela sua ineficácia e por forçar as entidades obrigadas a um esforço redobrado, razão pela qual foi desenvolvida uma plataforma digital que permite a comunicação simultânea ao DCIAP e à UIF[151], simplificando o procedimento[152].

[150] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 255.
[151] Esta comunicação digital única surgiu no seguimento do disposto no artigo 126º da Lei 83/2017, que impõe a cooperação entre o DCIAP e a UIF "no sentido de estabelecerem um canal único, seguro e fiável" para as entidades obrigadas efetuarem as suas comunicações de operações suspeitas e outras informações solicitadas.
[152] NUNES, Carlos Casimiro – O Ministério Público na prevenção do branqueamento e do financiamento do terrorismo, p. 109.

Cabe às UIFs processar e analisar as informações recebidas, bem como repassar essas informações aos órgãos de prossecução penal, no caso de constarem a prática de algum ilícito penal[153], conforme artigo 82.º da LBCFT.

Apesar dos esforços no sentido de otimizar a comunicação de operações suspeitas, o reporte destas entidades é fraca ou quase inexistente. A cooperação em sede de investigação criminal com vista à obtenção de dados referentes ao titular da conta ou de informações sobre transações, depende quase sempre de pedidos informais, efetuados por plataformas próprias, pois a alternativa de recurso a meios tradicionais de cooperação judiciária internacional é quase sempre morosa, esbarrando muitas vezes no facto das sedes daqueles prestadores, muitas vezes instáveis, se encontrarem em jurisdições que não cooperam com as investigações criminais[154].

Estas circunstâncias culminam num número anormalmente baixo de reporte à UIF nacional de transações suspeitas usando ativos virtuais.

Segundo o relatório anual da UIF referente ao ano de 2021[155], das 10.059 comunicações suspeitas recebidas, apenas 6 transações suspeitas foram reportadas por entidades que se dedicam a atividades com ativos virtuais.

Em 2022, não obstante o aumento verificado das comunicações de operações suspeitas pelas entidades do setor não financeiro (um aumento de 140,5% em comparação ao ano de 2021), continuou a verificar-se a existência de entidades obrigadas que pouco ou nada reportaram. O maior número de comunicações de operações suspeitas que a UIF recebeu continuou a ser proveniente das entidades financeiras e as entidades que exercem atividade com ativos virtuais reportaram apenas 15 transações (mais 9 do que no ano anterior)[156].

Em contrapartida, é cada vez mais frequente a descoberta, em processos criminais e nomeadamente em processos relacionados com fraude fiscal e

[153] TEIXEIRA, Adriano – "A relevância processual dos relatórios de inteligência financeira" *in* "Estudos sobre *Law Enforcement*, *Compliance* e Responsabilidade Empresarial", p. 130.
[154] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 261.
[155] Disponível em https://uif.policiajudiciaria.pt/wp-content/uploads/2022/11/UIFRelatorioAnual2021-3.pdf.
[156] Disponível em https://uif.policiajudiciaria.pt/relatorio-anual-2022/.

BCFT, da existência de carteiras de ativos virtuais, normalmente custodiadas em operadores financeiros nacionais e internacionais que, não obstante estarem obrigados a políticas de KYC e de obrigações de reporte, não haviam comunicado qualquer transação suspeita às autoridades nacionais. A deteção da existência daquelas carteiras destinadas a BCFT, ocorre, usualmente após a realização de diligências intrusivas (como buscas domiciliárias e não domiciliárias, apreensão de computadores e dispositivos móveis) aos suspeitos. A sua posterior análise forense, financeira e contabilística revela, quase sempre, um volume e uma frequência de transações que, se tivesse ocorrido no setor bancário tradicional, teria certamente gerado obrigações de reporte, permitindo de imediato o acionamento dos mecanismos previstos na Lei do BCFT, particularmente os deveres de abstenção e de comunicação, com a consequente avaliação da necessidade de suspensão temporária da operação, consagrada no artigo 48º do referido diploma[157].

[157] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 261 e 262.

Capítulo IV – O caminho para a normalização das transações com ativos virtuais

1. Vantagens

Revela-se importante reconhecer as principais vantagens decorrentes da utilização dos ativos virtuais e da tecnologia *blockchain,* vantagens essas que são até apontadas pelas autoridades preocupadas com os riscos inerentes à sua utilização[158].

Configura-se uma grande vantagem, desde logo, a eficiência e a rapidez na realização de operações transfronteiriças, principalmente quando comparado com o tradicional sistema de transferências bancárias internacionais. Adicionalmente, e devido à desnecessidade de intermediários ou de um sistema de monitorização, o custo de transação de ativos virtuais também é muito baixo. Uma transferência leva, em média, menos de 8 segundos e menos de 30 cêntimos a ser executada[159].

Existem também movimentos de autorregulação, portanto alguns operadores que impuseram aos seus utilizadores deveres de identificação e diligência próprios do sistema de PBCFT, com o objetivo de conquistar uma vantagem competitiva face aos outros concorrentes que se vão mantendo indiferentes às manifestações de preocupação das autoridades, procurando assim ganhar reputação e credibilidade no mercado e atrair aqueles clientes que não pretendem fazer uma utilização ilegítima da tecnologia. É o caso da *Luso Digital Assets* e consubstancia uma vantagem no sentido em que é possível esta autorregulação.

Além disso, a transição para o mundo digital é inevitável, está cada vez mais presente nos nossos dias, por isso a facilidade em fazer transações é algo que,

[158] BRITO, João Rodrigues – "Da sujeição dos *Virtual Asset Service Providers* ao Cumprimento de Deveres de Prevenção do Branqueamento de Capitais" *in* "Novos Desafios da Prova Penal", p. 376 e 377.
[159] PACHECO, António Vilaça – Bitcoin: Tudo o que precisa de saber sobre o mundo das criptomoedas, p. 293.

com certeza, se procurará generalizar e, idealmente, espera-se que sejam feitas em segurança (o que nos parece possível, uma vez que tudo fica gravado na *blockchain*).

Através desta tecnologia e no momento da conversão dos criptoativos em dinheiro governamental - como o euro ou o dólar - é possível identificar quem fez a conversão e, a partir daí, ver de onde vieram todas as transações de todas as carteiras anteriores e, um a um, investigar os seus intervenientes. Para PACHECO[160], também não parece razoável eliminar a tecnologia, uma vez que não é a mesma a praticar os crimes de BCFT, mas sim os criminosos, que usam qualquer forma de dinheiro e não são proibidas essas formas nas quais transitam ainda maiores volumes de dinheiro ilícito. O autor refere ainda que trocar notas e moedas é e será sempre muito mais anónimo do que qualquer outra forma informática. O autor admite que há espaço para melhoria, mas precisamos primeiro de aceitar a mudança.

Assim, os ativos virtuais podem assegurar funções monetárias, de acordo com a vontade das partes, sem a necessidade de intervenção de um terceiro (descentralização), o que permite ganhos de eficiência, rapidez, segurança, escassez, polivalência, inovação e autonomia sistémica[161].

A eficiência é adquirida pela redução dos custos de transação, como as comissões de depósito e as taxas de transação, que ocorrem nas moedas fiduciárias. A rapidez traduz-se numa elevada velocidade da transação, o que permite garantir a ocorrência de pagamentos ou transferências, que se fossem realizadas por uma instituição financeira, poderia demorar dias. A segurança é outro ponto forte uma vez que o sistema de registo descentralizado não é passível de ser corrompido com facilidade, o que a torna de certa forma imune a fraudes, furtos, falsificação, destruição, entre outras limitações que ocorrem em moedas físicas. A escassez é outro ponto determinante e especialmente válido para a *Bitcoin*, dada a predefinição máxima de 21 milhões de moedas, o que lhe confere uma natureza deflacionária. Além do seu valor enquanto moeda, esta também assume uma elevada polivalência, uma vez que as criptomoedas

[160] PACHECO, António Vilaça – Bitcoin: Tudo o que precisa de saber sobre o mundo das criptomoedas, p. 292 e 293.
[161] ANTUNES, José Engrácia – As criptomoedas, p. 124.

podem desempenhar funções de investimento e financiamento, como são exemplos as "*utility tokens*" e as "*security tokens*". A sua existência é também fomento para plataformas de *crowdfunding* e financiamento de *startups*, tendo assim caráter inovatório e distinguindo-se do sistema financeiro atual, ao abrir novas possibilidades de negócio. A privacidade é outra vantagem das criptomoedas, na medida em que os endereços das moedas virtuais, que consistem em chaves públicas e privadas, não contém, normalmente, a identificação pessoal do titular. A autonomia sistémica é conferida pela independência destas moedas face à intervenção dos Estados[162].

[162] RODRIGUES, André Alfar – Manual de Inovação Financeira: Uma Introdução ao Universo das Criptomoedas e da Blockchain, p. 38 e 39.

2. Desvantagens

Ao nível das desvantagens convém entender que, se por um lado, a independência das criptomoedas face à intervenção de um Estado pode ser uma vantagem, por outro, confere-lhe uma ausência de estatuto legal próprio, o que desprotege os utilizadores, no que aos seus direitos diz respeito[163].

Como já expusemos, também constituem motivo de preocupação as condutas de utilização e dissimulação da origem ilícita, nomeadamente, de *bitcoins*, através de operações financeiras virtuais de *mixing* – que são, não obstante o seu propósito de ocultação, muitas vezes lícitas[164].

Já vimos que, quando alguém realiza uma transação com criptomoedas, essa transação é registada na *blockchain* e fica visível para qualquer pessoa. Através de análises à *blockchain* é possível, na maior parte das vezes, rastrear o histórico de transações de um endereço, por exemplo, de *Bitcoin* e potencialmente associá-la a uma identidade real[165]. O problema está na existência de *mixers* ou *tumblers* que, embora associados e vendidos como ferramentas de privacidade, estão a ser associados à prática de crimes cometidos no espaço cibernético, como a *ransomware*[166]*.* Um *mixer* de *Bitcoin* é um serviço que permite aos usuários baralharem ou misturarem as suas *Bitcoins* com as de outros utilizadores, com o objetivo de dificultar o rastreamento e a associação das transações a endereços específicos[167].

O processo ocorre com o envio de *Bitcoins* para o *mixer* que, por sua vez, redistribui os fundos para diferentes endereços, geralmente aleatoriamente, antes de os enviar de volta para os utilizadores. Ao usar um *mixer* de Bitcoin, é

[163] RODRIGUES, André Alfar – Manual de Inovação Financeira: Uma Introdução ao Universo das Criptomoedas e da Blockchain, p. 39.
[164] RAMALHO, David Silva e MATOS, Nuno Igreja – Branqueamento e *Bitcoin*: uma introdução, p. 78.
[165] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 262.
[166] *Ransomware* ou *ransom malware* é um tipo de *malware* (software malicioso) que impede os utilizadores de aceder ao seu sistema ou ficheiros pessoais e exige-lhes o pagamento de um resgate [*ransom*] para devolver o acesso. Atualmente, os autores do *ransomware* exigem que o pagamento seja enviado através de criptomoedas ou cartão de crédito. Mais informações podem ser encontradas em https://pt.malwarebytes.com/ransomware/.
[167] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 262 e 263.

possível obscurecer o rasto das transações, tornando mais difícil para terceiros identificar a origem das *Bitcoins* e relacioná-las a uma pessoa específica. Ainda que o valor estimado do uso de *mixers* para ocultar o rasto de transações por atores criminais seja apenas de 10% do valor total estimado de transações usando esta tecnologia, não é menosprezível, considerando o valor total de transações destes ativos virtuais diretamente relacionado a BC e se tivermos em conta que a Quinta Diretiva AML, como já vimos, não se aplica a estes fornecedores de serviços[168].

É por este motivo que o principal foco de riscos de BCFT apontado pelo GAFI reside, atualmente, nos mecanismos de reforço de anonimização, de obscurecimento e de dispersão de ativos virtuais transacionados, ou seja, nas entidades prestadoras de serviços de mistura (*mixers*/*tumblers*) e estes constituem uma clara desvantagem da utilização para os ativos virtuais[169].

Entre outras desvantagens, também é possível apontar que o propósito para o qual os ativos virtuais foram criados se está a perder (rapidez, simplicidade, segurança, baixo custo, etc.). Neste momento, as entidades que exercem atividade com ativos virtuais estão sujeitas a vários procedimentos, cuja utilidade é discutível. São exemplos: a questão do print da *wallet*; a falta de especificação na lei do que é aceite como *Source of Funds*; a falta de formação; e até os testes de eficácia – que nenhuma consultora sabe bem como fazer e, por isso, cobram valores altíssimos; a questão dos TIN's – e de como isso não é uma realidade praticável noutros países, como é em Portugal.

Tudo isto é explicado com a crescente preocupação em legislar esta matéria, mas que acaba por resultar numa verdadeira confusão de diplomas, nacionais e internacionais. O facto de, até este ano, se ter optado por Diretivas europeias, em vez de Regulamentos, também fez com que a informação na União Europeia não fosse consensual e fosse diferente de país para país, o que resulta num autêntico caos e permite a escolha da jurisdição mais favorável por parte do

[168] SANTOS, Nuno Serdoura dos – "Prevenção do Branqueamento e Criptoativos" *in* "I Congresso Inteligência Artificial e Direito – Atas da Conferência", p. 263.
[169] RAMALHO, David Silva e MATOS, Nuno Igreja – Branqueamento e *Bitcoin*: uma introdução, p. 97 e 98.

criminoso. Também a informação sobre ativos virtuais disponibilizada não é clara, acessível e completa.

Quanto à obrigatoriedade da SOF, sentimos tendência a concordar com a posição de NUNO BRANDÃO[170], de que pedir este tipo de informação sobre a origem dos fundos e a justificar a operação, obtida por escrito através do próprio cliente, não parece suficiente para atingir o seu propósito. De facto, parece-nos que esta obrigação carece de sentido, pois o seu cumprimento não garante nada e terá ainda como consequência pôr os potenciais autores de operações de BCFT imediatamente alerta, mostrando-lhes que estão perante uma entidade atenta a possíveis esquemas de BCFT e levando-os a procurar outras paragens.

Além destas desvantagens, as moedas virtuais são ainda extremamente voláteis e instáveis, sendo esta instabilidade decorrente da maior falta de liquidez e menor dimensão de mercado. Têm também uma elevada facilidade em serem manipuladas e sofrerem ataques especulativos. Isto porque, não obstante a capacidade de fortificar a sua segurança através de encriptação de última tecnologia, a verdade é que estas moedas podem ser bastante vulneráveis e suscetíveis a ataques informáticos caso os "atacantes" disponham de um poder computacional superior. Isto pode resultar em falhas de autenticidade e operacionalidade. Outra desvantagem é que, com exceção de moedas com maior poder de mercado, como o *Bitcoin* ou a *Ether*, a grande maioria das criptomoedas não são diretamente convertíveis em moedas fiduciárias, como o euro ou o dólar.[171]

Porém, mesmo quando são convertíveis e uma vez que os ativos virtuais não têm curso legal em Portugal, a sua aceitação pelo valor nominal não é obrigatória. Ademais, ao usar moedas virtuais como meio de pagamento, o consumidor encontra-se desprotegido. Isto porque não existe, atualmente, 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. Consequentemente, em caso de desvalorização parcial ou total dos ativos virtuais, não existe um fundo que cubra

[170] BRANDÃO, Nuno - Branqueamento de Capitais: O Sistema Comunitário de Prevenção, p. 42.
[171] RODRIGUES, André Alfar – Manual de Inovação Financeira: Uma Introdução ao Universo das Criptomoedas e da Blockchain, p. 39.

eventuais perdas dos seus utilizadores, que terão de suportar o risco associado às operações com estes instrumentos, podendo perder todo o seu dinheiro na plataforma de negociação.[172]

Por último, e pese embora a baixíssima taxa de reporte de operações suspeitas, verifica-se que os crimes com mais impacto entre os inquéritos abertos pela UNC3T[173] da PJ em 2022, foram, precisamente, o branqueamento de capitais, a *sextortion* e o o *ransomware*[174].

Com conclusão semelhante, também o *Crypto Crime Report 2023* da *Chainanalysis* dá conta de que o volume de transações de ativos virtuais diretamente relacionado a branqueamento de capitais ascendeu a 22 biliões de dólares, tendo subido exponencialmente face aos anos anteriores.

Vejamos, a título de exemplo, a recente operação global que desmantelou uma rede ilícita de lavagem de dinheiro relacionada com a Rússia, que utilizava criptomoedas para evadir sanções internacionais[175]. Embora fossem utilizadas *exchanges* ilícitas, este caso demonstra como a tecnologia pode ser desvirtuada dos seus propósitos originais, podendo-se tirar proveito do anonimato e da falta de regulamentação rigorosa, o que permite que indivíduos ou entidades contornem sanções económicas impostas, neste caso à Rússia, decorrentes da guerra atual.

O BCFT é, portanto, uma prática frequentemente associada aos ativos virtuais, dado o seu caráter tendencialmente anónimo, o que não pode deixar de constituir uma das principais desvantagens desta tecnologia.

---

[172] Disponível em https://www.bportugal.pt/comunicado/banco-de-portugal-reitera-alertas-aos-consumidores-sobre-riscos-associados-aos-ativos [consultado em 18.08.2024].
[173] Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica.
[174] Esta informação consta na página 17 do Relatório do Centro Nacional de Cibersegurança em Portugal (CNCS), de junho de 2023. Na página 18 também é possível ler-se "Os cibercriminosos realizaram principalmente ataques de *phishing*/*smishing*/*vishing*, *ransomware*, intrusões (algumas na forma tentada), diversos tipos de burla e **branqueamento de capitais**". Este relatório está disponível em https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs15m.pdf [consultado em 20.04.2024].
[175] Disponível em https://www.coindesk.com/pt-br/policy/2024/09/27/global-effort-disrupts-russia-linked-network-using-crypto-to-evade-sanctions-us-charges-two-russians/amp/ [consultado em 29.09.2024]

3. Criação de uma entidade reguladora específica

Seria, a nosso ver, importante a criação de uma entidade reguladora específica para a atividade com ativos virtuais. Porque não haver uma entidade supervisora específica que, além de regular e inspecionar, também possa ajudar os prestadores de serviços de criptoativos com uma componente formativa e pedagógica, nas questões interpretativas da lei e nas melhores formas para concretizar essas mesmas exigências?

A entidade reguladora atualmente é o Banco de Portugal e, para as questões que lhe são colocadas, nem sempre tem uma resposta adaptada à realidade dinâmica dos ativos virtuais, além de ter a seu cargo muitas outras entidades financeiras para supervisionar. Não deixa de ser algo contraditório que uma entidade financeira regule e supervisione uma entidade não financeira.

Como também aponta CARLOS CASIMIRO NUNES[176], Portugal necessitava de uma entidade que coordenasse os esforços efetuados no âmbito da PBCFT. A existência de uma autoridade ou mecanismo de coordenação das políticas nacionais de combate ao BCFT era um imperativo desde a revisão das Recomendações do GAFI em 2012 e da publicação da Diretiva (UE) n.º 2015/849, do Parlamento Europeu e do Conselho, de 20 de maio de 2015 (artigo 7º).

O que aconteceu, ao invés, foi a criação da Comissão de Coordenação das Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo (CCPPCBCFT)[177] cuja principal missão é acompanhar e coordenar a identificação, avaliação e resposta aos riscos de BCFT a que Portugal está ou venha a estar exposto. Estando sob dependência do Ministério das Finanças, o objetivo desta Comissão é contribuir para a melhoria contínua da conformidade técnica e da eficácia do sistema nacional de combate ao BCFT, propondo as medidas legislativas, regulamentares e

[176] NUNES, Carlos Casimiro – O Ministério Público na prevenção do branqueamento e do financiamento do terrorismo, p. 97.
[177] Esta Comissão foi criada a partir da Resolução de Conselho de Ministros 88/2015, de 01/10 (DR n.º 195/2015, Série I de 06/10/2015).

operacionais necessárias para assegurar a boa execução da estratégia e das políticas nacionais[178].

É certo que esta Comissão de Coordenação representa um importante avanço na PBCFT, considerando que até um dos seus primeiros trabalhos foi a conclusão da primeira Avaliação Nacional de Risco (ANR)[179] em matéria de PBCFT. Este primeiro relatório serviu não só para percecionar os riscos concretos, como para compreender, orientar e adequar as medidas tomadas e aquelas que eram necessárias, em cada setor. Foi, ainda, um auxiliar importante na quarta avaliação do GAFI a Portugal[180].

No entanto, nem esta Comissão, nem a nova Autoridade Europeia específica para o combate ao BCFT resolvem o problema, uma vez que, mesmo que esta última vise supervisionar o cumprimento dos deveres de PBCFT por parte de algumas entidades obrigadas, não é dotada da *expertise,* nem focada na realidade dos ativos virtuais.

Sendo esta uma matéria muito complexa, com conceitos técnicos e específicos, uma entidade reguladora própria, com recursos técnicos, humanos, financeiros e formação apropriada em ativos virtuais, traria inúmeras vantagens. Dada a dificuldade em acompanhar a rápida evolução deste mercado, esta entidade específica teria uma maior perícia na matéria dos ativos virtuais, traria maior eficiência na aplicação das medidas regulatórias e uma maior coordenação entre as diferentes autoridades competentes. Esta entidade, que poderia assumir a denominação de ERACAV (Entidade Reguladora da Atividade Com Ativos Virtuais), deveria funcionar em estreita articulação com a CCPPCBCFT e o Banco de Portugal.

Embora o GAFI não recomende, de uma forma explícita, a criação de uma entidade reguladora específica em cada país para os ativos virtuais, são várias as recomendações a sugerir, ainda que implicitamente, que é este o caminho a trilhar. Olhemos, a título de exemplo, para a Recomendação 25, onde o GAFI solicita aos países que cooperem entre si de modo a partilhar informações e a

[178] RODRIGUES, André Alfar – Manual Teórico-Prático de *Compliance*, p. 158 (nota de rodapé).
[179] A imposição da realização periódica de ANR vem prevista no artigo 8.º da Lei 83/2017.
[180] NUNES, Carlos Casimiro – O Ministério Público na prevenção do branqueamento e do financiamento do terrorismo, p. 97.

investigar conjuntamente casos de BCFT. A criação de uma entidade reguladora específica para ativos virtuais poderia ser uma forma eficaz de concretizar, assim, as Recomendações do GAFI, que alertam frequentemente para a necessidade de os países executarem medidas regulatórias robustas, de modo a prevenir e a detetar o uso indevido de ativos virtuais.

De facto, já existem entidades específicas que regulam e supervisionam a atividade com ativos virtuais noutros países, com o objetivo de prevenir o BCFT, como é o caso dos EUA (que tem o *Financial Crimes Enforcement* Network - FinCEN) e do Japão (*Financial Services Agency* - FSA). A regulamentação de ativos virtuais, além de multifacetada, varia de país para país. Ora, a criação de uma entidade reguladora específica permitiria uma maior cooperação, articulação e eficácia na PBCFT, a nível nacional e internacional.

Admitimos, porém, que a criação de uma entidade reguladora específica para ativos virtuais, também pode acarretar algumas desvantagens, como o aumento dos custos e uma eventual duplicação de esforços regulatórios, quando há já um universo muito vasto e confuso de diplomas e, além disso, está para breve a AMLA.

Conclusão

A crescente adoção e utilização de ativos virtuais têm gerado uma série de desafios legais, inclusivamente no que toca a questões relacionadas com a PBCFT.

Para enfrentar esses desafios é essencial desenvolver um ambiente jurídico adequado. Ora, o que acontece é que a regulamentação desta matéria deixa de fora importantes questões, como os NFT's.

Além disso, a cooperação internacional e a harmonização regulatória são fundamentais de modo a garantir a segurança e a integridade do mercado de ativos.

Verificamos também que o regime de PBCFT aplicável às VASP é praticamente idêntico ao das entidades financeiras, o legislador não foi muito "original" e não se adequou, nalgumas circunstâncias, às especificidades desta atividade em franca expansão.

Dado o caráter eminentemente internacional e o facto de se utilizar a tecnologia associada aos ativos virtuais para BCFT a uma escala global, só uma política de cooperação internacional permitiria um combate mais eficaz a este tipo de crimes.

O regime atual de PBCFT é considerado bastante ambicioso, mas contém algumas caraterísticas que, por vezes, culminam em verdadeiras impossibilidades práticas de cumprimento e, noutras situações, não abrange todas as realidades passíveis de operações de BCFT. Noutros casos ainda, o cumprimento até é possível, mas mostra sérias dificuldades práticas de interpretação legislativa potencialmente geradoras de confusão.

Ao nível europeu, pese embora os esforços recentes que têm vindo a ser feitos nesse sentido, são manifestamente insuficientes, pois deixaram de fora produtos e tecnologia que facilmente podem ser usados no cometimento de crimes de BCFT, como os serviços de câmbio entre ativos virtuais e os *mixers*/*tumblers*.

Apesar de a tecnologia *blockchain* ser, à partida, uma alternativa mais confiável, inteligente, segura e acessível por baixo custo, também acarreta riscos, nomeadamente porque permite o anonimato de certas transações e pode,

assim, ser utilizada com o propósito de BCFT. Esta utilização tem vindo a aumentar e já assume alguma expressão nos inquéritos criminais em investigação em Portugal.

Os riscos deste uso não se circunscrevem unicamente à mera detenção dos ativos virtuais, mas também ao desenvolvimento de novas moedas.

Urge a criação de uma disciplina específica no ensino superior, que aborde a legislação e as várias incidências destas atividades, em virtude da impossibilidade de integrar o conceito dos ativos virtuais nas figuras existentes na nossa ordem jurídica. Seria também uma oportunidade para investigar, aprofundar e publicar estudos científicos sobre estas matérias, que rapidamente sofrem transformações.

Além desta componente académica e científica, torna-se imperativa a criação de uma entidade reguladora específica, que supervisione as entidades que exercem atividade com ativos virtuais. Entidade essa que poderia assumir a denominação de ERACAV (Entidade Reguladora da Atividade Com Ativos Virtuais).

Por último, o ideal será dotar o sistema de PBCFT com um filtro suficientemente apertado de modo a detetar operações suspeitas de BCFT e denunciá-las logo na primeira fase.

Não obstante o crescente reporte desta utilização, os mecanismos de prevenção existentes com vista à comunicação de transações suspeitas são muito deficitários, quer pelo atual quadro legal, quer pela falta de cumprimento de obrigações de reporte.

É, por isso, necessário repensar o quadro legislativo atendendo às especificidades destes ativos e a dotação de meios técnicos e humanos nas entidades reguladoras e de controlo, que assumirão cada vez mais protagonismo na área da PBCFT relacionada com ativos virtuais. Só desta forma se prevenirá a ocorrência destas operações e poderemos combater este flagelo.

A AMLA veio acautelar uma necessidade que foi por nós identificada ao longo da elaboração deste trabalho. A natureza transfronteiriça da maioria das investigações sobre BCFT, a disparidade dos formatos utilizados para o combate a este flagelo, as dificuldades no tratamento dos registos de transações e a dificuldade de intercâmbio de informações entre as autoridades competentes dos Estados-Membros, já há muito que requeria uma solução como a que agora foi

apresentada. Resta-nos saber se os países estarão aptos a adequar os seus procedimentos e se se saberá retirar o melhor proveito desta ideia.

Ao abrigo deste novo pacote legislativo foram também acrescentados requisitos adicionais para as empresas que, seguramente, contribuirão para que o combate ao BCFT seja mais eficaz e que seja mais difícil branquear dinheiro e financiar o terrorismo através de ativos virtuais.

Referências bibliográficas

1. ANTUNES, José Engrácia – "As criptomoedas" *in* Revista da Ordem dos Advogados, Vol. 81, n.º 1-2, 2021.
2. ASCENSÃO, José de Oliveira – "Branqueamento de Capitais: Reacção Criminal" *in* "Estudos de Direito Bancário", coord. António Menezes Cordeiro… [et al.], Coimbra Editora, 1999, ISBN 972-32-0911-X.
3. BARROS, Marco António de – Lavagem de capitais: Crimes de Lavagem, Procedimento Penal Especial, Protocolos Administrativos e Preventivos, 6ª edição, Editorial Juruá, Porto, 2022, ISBN 978-989-712-892-9.
4. BRANDÃO, Nuno - Branqueamento de Capitais: O Sistema Comunitário de Prevenção. 1ª ed. Coimbra: Coimbra Editora, 2002, ISBN 972-32-1110-6.
5. BRANDÃO, Nuno – O *whistleblowing* no ordenamento jurídico português, Revista do Ministério Público n.º 161, janeiro-março, 2020, p. 99-113.
6. BRATTON, William Wilson – "Enron and the Dark Side of Shareholder Value", in "Public Law and Legal Theory Working Paper" n. º 035, The George Washington University Law School, 2002. Artigo disponível em SSRN: https://ssrn.com/abstract=301475 ou http://dx.doi.org/10.2139/ssrn.301475 [consultado em 19.04.2024].
7. BRITO, João Rodrigues – "Da sujeição dos Virtual Asset Service Providers ao Cumprimento de Deveres de Prevenção do Branqueamento de Capitais" *in* "Novos Desafios da Prova Penal", v. I, coord. Paulo de Sousa Mendes e Rui Soares Pereira, Almedina, 2020, ISBN 978-972-40-8950-8.
8. CANAS, Vitalino – «Branqueamento de Capitais»: Noções elementares do regime jurídico de prevenção e repressão e evolução previsível. Coimbra Editora, 2004. Separata da Revista da Faculdade de Direito da Universidade de Lisboa, Suplemento.
9. CANAS, Vitalino - O Crime de Branqueamento: Regime de Prevenção e de Repressão. 1ª ed. Coimbra: Almedina, 2004, ISBN 972-40-2245-5.
10. COSTA, João Neves da e NEVES, Mário – "Dificuldades e impossibilidades: Algumas notas práticas à aplicação da Lei n.º 83/2017,

de 18 de junho, no contexto da atividade de Compliance" *in* "Novos Estudos sobre Law Enforcement, Compliance e Direito Penal", v. I, coord. Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes, Almedina, 2020, ISBN 978-972-40-8451-0.

11. DUARTE, Diogo Guerreiro – "An Introduction to Blockchain Technology from a Legal Perspective and its Tensions with the GDPR" *in* "Direito e Ciberespaço – Coletânea de Artigos da Revista Digital CyberLaw by CIJIC", cood. Eduardo Vera-Cruz Pinto e Marco Antonio Marques da Silva, São Paulo, Editora Quartier Latin, 2023, ISBN 978-65-5575-206-9.
12. ESTELLITA, Heloísa – "Criptomoedas e lavagem de dinheiro" *in* "Revista Direito GV", 2020, [disponível em https://www.academia.edu/51716693/Criptomoedas_e_lavagem_de_dinheiro, consultado em 18.08.2024], ISSN 2318-6172.
13. ETCHEBERRY, Jaime Winter – "La regulación internacional del lavado de activos y el financiamento del terrorismo" *in* "Lavado de Activos y Compliance – Perspectiva internacional y Derecho comparado", coord. Kai Ambos, Dino Carlos Caro Coria e Gustavo Urquizo, 2ª edición, Lima – Perú, Gaceta Jurídica S.A., 2019, ISBN 978-612-311-686-6.
14. FLYVBJERG, Bent – "Quality Control and Due Diligence in Project Management: Getting Decisions Right by Taking the Outside View", 2013, *in* "International Journal of Project Management", vol. 31, n. º 5. Artigo disponível em SSRN: https://ssrn.com/abstract=2229700 [consultado em 22.04.2024].
15. FONTES, José e CRUZ, Nelson da – Contributo para a Sustentabilidade dos Estados e das Democracias, Almedina, 2021, ISBN 978-972-409-980-4.
16. GODINHO, Jorge Alexandre Fernandes – Do crime de «Branqueamento» de Capitais: Introdução e Tipicidade. 1ª ed. Coimbra: Almedina, 2001. ISBN 972-40-1454-1.
17. LAVRADOR, Jasmine Souto – "Benefícios da Coleta e Armazenamento de Evidências Eletrônicas Disponíveis na Internet Através da Tecnologia Blockchain em Comparação com as Provas Tradicionalmente Disponíveis aos Particulares em Portugal" *in* "Novos Desafios da Prova Penal", v. I,

coord. Paulo de Sousa Mendes e Rui Soares Pereira, Almedina, 2020, ISBN 978-972-40-8950-8.

18. MACHADO, Miguel da Câmara – "4G na prevenção do branqueamento de capitais: problemas, paradoxos e principais deveres" *in* "Estudos de Direito Bancário I", coord. António Menezes Cordeiro… [et al.], Coimbra, Almedina, 2019, reimpressão, ISBN 978-972-40-7312-5.
19. MACHADO, Miguel da Câmara – "Contexto, evolução e tendências do compliance em Portugal e na Europa, em especial a partir do Aviso n.º 3/2020, de 15 de julho, do Banco de Portugal" *in* "Estudos sobre Law Enforcement, Compliance e Responsabilidade Empresarial", coord. Paulo de Sousa Mendes, Teresa Quintela de Brito, [et. al], Coimbra, Almedina, 2023, ISBN 978-989-40-1093-7.
20. MACHADO, Miguel da Câmara – "Deveres antibranqueamento de capitais: De onde vieram, quais são e como vão evoluir (do "4G" ao "5G")" *in* "Novos Estudos sobre Law Enforcement, Compliance e Direito Penal", coord. Maria Fernanda Palma, Augusto Silva Dias e Paulo de Sousa Mendes, Coimbra, Almedina, 2020, ISBN 978-972-40-8451-0.
21. MACHADO, Miguel da Câmara – Regimes da Prevenção do Branqueamento de Capitais e Compliance Bancário, Lisboa, AAFDL Editora, 2017, ISBN 978-972-629-163-3.
22. MATA, Paulo Saragoça da - Política e corrupção: branqueamento e enriquecimento, 1ª ed., Lisboa, Chiado Editora, 2015.
23. MELO, Júlio César Machado Ferreira de – Crime organizado e delação premiada: com as alterações do pacote anticrime (Lei 13.964/2019), Porto, Editorial Juruá, 2020, ISBN 978-989-712-897-4.
24. MENDES, Paulo de Sousa – "Regulação responsiva, autorregulação regulada e responsabilidade empresarial" in "Estudos sobre Law Enforcement, Compliance e Responsabilidade Empresarial", coord. Paulo de Sousa Mendes, Teresa Quintela de Brito, [et. al], Coimbra, Almedina, 2023, ISBN 978-989-40-1093-7.
25. NUNES, Carlos Casimiro – O Ministério Público na prevenção do branqueamento e do financiamento do terrorismo, Revista do Ministério Público n.º 153, Lisboa, 2018.

26. OGUNBADEWA, Ajibola – "The Bitcoin Virtual Currency: A Safe Haven for Money Launderers?", 2013. Artigo disponível em SSRN: https://ssrn.com/abstract=2402632 ou http://dx.doi.org/10.2139/ssrn.2402632 [consultado em 22.04.2024].
27. PACHECO, António Vilaça – Bitcoin: Tudo o que precisa de saber sobre o mundo das criptomoedas, Self PT, 12ª edição, 2023, ISBN 978-989-903-283-5.
28. PAÚL, Jorge Patrício – "A Legislação Portuguesa sobre Branqueamento de Capitais e as suas Repercussões no Exercício da Actividade Bancária" *in* "Estudos de Direito Bancário", coord. António Menezes Cordeiro… [et al.], Coimbra Editora, 1999.
29. RAMALHO, David Silva e MATOS, Nuno Igreja – Branqueamento e Bitcoin: uma introdução, Revista do Ministério Público n.º 162 (abr.-jun. 2021), p. 113-127, ISSN 0870-6364.
30. RAMALHO, David Silva – "Corrupção e Compliance na Nova Lei Portuguesa de Prevenção do Branqueamento e Financiamento do Terrorismo: Lições da Experiência Norte-Americana" *in* "Estudos sobre Law Enforcement, Compliance e Responsabilidade Empresarial", coord. Paulo de Sousa Mendes e Teresa Quintela de Brito, Coimbra, Almedina, 2023, ISBN 978-989-40-1093-7.
31. RAMALHO, David Silva – Comentário ao Regime de Prevenção do Branqueamento de Capitais e do Financiamento do Terrorismo, 2ª ed., Coimbra, Almedina, 2023, ISBN 978-972-40-9059-7.
32. RAPOSO, Gonçalo Matias – Branqueamento de Capitais e Actividade Bancária: Enquadramento Legal Nacional e Internacional. 1ª ed. Coimbra: Coimbra Editora, 2002, ISBN 972-32-1105-X.
33. SCHNEIDER, Friedrich – "The Financial Flows of Transnational Crime and Tax Fraud in OECD Countries: What Do We (Not) Know?", 2010. Artigo disponível em SSRN: https://ssrn.com/abstract=1617119 ou http://dx.doi.org/10.2139/ssrn.1617119 [consultado em 18.08.2024].
34. SILVA, Jorge Godinho – "Caminhos e cruzamentos: O branqueamento de capitais e o financiamento do terrorismo no século XXI" *in* "Estudos sobre Direito Penal Internacional", coord. Paulo Pinto de Albuquerque e Jorge Godinho Silva, Lisboa, AAFDL, 2023, ISBN 978-972-629-548-8.

35. TORRES, Miguel Amaral – Criptomoedas e a sua influência no branqueamento de capitais, Almedina, 2022, ISBN 978-989-40-1025-8.
36. VEIGA, Francisco Pereira e VEIGA, Pedro C. – Combate ao Branqueamento de Capitais: A Experiência Portuguesa, 1ª ed. Coimbra, Almedina, 2019, ISBN 978-972-40-7712-1.
37. ZAGARIS, Bruce – "U.S. and International Cooperation Against Transnational Organized Crime and Money Laundering" *in* "Fordham International Law Journal", vol. 35, n. º 3, 2012.

Anexos documentais

LUSO DIGITAL ASSETS	**Relatório de Atividade Suspeita**
Supervisor: RCN	Aprovado pela Gerência a 12-08-2022
N.º do Doc.: LDA-1-003	Data de Revisão: 12-08-2023

Detalhes da Atividade Suspeita	
Nome e contatos da pessoa/empresa envolvida	
Quando é que ficou alerta pela primeira vez de atividade suspeita?	
Qual a natureza da atividade da empresa? Ou profissão do indivíduo?	
Natureza da atividade suspeita	
Montante da transação/transações em causa	
Discutiu esta situação com alguém? Se sim, com quem?	

Assinatura:	Data:

Para uso do RCN - Exclusivamente		
Nome:	Função:	
Notas especiais:	Assinatura:	Data: