FACULDADE DE DIREITO

CRYPTO ASSETS: O EQUILÍBRIO ENTRE A NECESSIDADE DE REGULAMENTAÇÃO AML/CFT E A PROTEÇÃO DE DADOS

Rafaela Pinheiro de Andrade Machado

Dissertação de Mestrado em Direito e Prática Jurídica
Especialidade em Direito Civil

Lisboa
2024

FACULDADE DE DIREITO

CRYPTO ASSETS: O EQUILÍBRIO ENTRE A NECESSIDADE DE REGULAMENTAÇÃO AML/CFT E A PROTEÇÃO DE DADOS.

Rafaela Pinheiro de Andrade Machado

Orientador: Professor Doutor Diogo Neves Pereira Duarte

Dissertação de Mestrado em Direito e Prática Jurídica
Especialidade em Direito Civil

Lisboa

2024

AGRADECIMENTOS

Primeiramente, sou grata a Deus por conceder-me a graça de viver com fé e poder desafiar-me em prol do meu propósito de vida.

Ao meu marido, Felicio, pelo apoio incondicional em todos os momentos da minha vida, especialmente para que fosse possível a elaboração desta dissertação, e por acreditar tanto na minha capacidade de realização.

À minha filha, Vitoria, que, apesar de tenra idade, é capaz de ensinar-me que a dedicação faz-me melhor.

À minha mãe, Fatimamiris, que, quando em vida, sempre incentivava-me a estudar e progredir na vida académica e profissional.

Ao professor Dr. Diogo Duarte, pela orientação que tornou possível a elaboração desta dissertação.

PRINCIPAIS ABREVIATURAS E SIGLAS UTILIZADAS

5AML/CFT – 5.ª Diretiva *Anti-Money Laundering and Combating the Financing of Terrorism*
6AML/CFT – 6.ª Diretiva *Anti-Money Laundering and Combating the Financing of Terrorism*
Ac. – Acórdão
AEPD - Autoridade Europeia para a Proteção de Dados
Al. – Alínea
AML – *Anti-Money Laundering*
AML/CFT – *Anti-Money Laundering and Combating the Financing of Terrorism*
Art.º – Artigo
Art.ºs – Artigos
BIS - *Bank for International Settlements*
CASPs - *Crypto-Asset Service Providers*
CEPD - Comité Europeu para a Proteção de Dados
CDD – *Customer Due Diligence*
CFT – *Combating the Financing of Terrorism*
COM – Comissão Europeia
DLT – *Distributed Ledger Technology*
DPIA - *Data Protection Impact Assessments*
EBA - *European Banking Authority*
EMD - *Electronic Money Directive*
ESMA - *European Securities and Markets Authority*
FATF - *Financial Action Task Force*
GAFI – Grupo de Ação Financeira Internacional
ICO - *Information Commissioner's Office*
KYC – *Know Your Costumer*
MiCA - *Markets in Crypto-Assets*
MiFID – *Markets in Financial Instruments Directive*
RGPD – Regulamento Geral de Proteção de Dados
UE – União Europeia
UIF – Unidade de Inteligência Financeira
VASPs - *Virtual Asset Service Providers*

ÍNDICE

RESUMO

Esta dissertação de mestrado oferece uma análise acerca dos *cryptoassets*, com foco especial em criptomoedas, na regulamentação AML/CFT (*Anti-Money Laundering / Combating the Financing of Terrorism*) e na proteção de dados. Inicialmente, aborda a natureza dos *cryptoassets*, mencionando suas categorias, como moedas virtuais, *tokens* de utilidade e *tokens* de segurança, bem como aspectos da tecnologia *blockchain*. As implicações dos *cryptoassets* no branqueamento de capitais e no financiamento do terrorismo são discutidas, com uma análise das respostas regulatórias, na União Europeia e em Portugal. A dissertação investiga as regulamentações AML/CFT, avaliando como elas afetam o mercado de *cryptoassets* e as práticas das instituições financeiras. Para além disso, a pesquisa aborda a questão da proteção de dados, enfatizando a relevância do Regulamento Geral de Proteção de Dados (RGPD) da UE, e como isso interage com a regulamentação dos *cryptoassets*.

Palavras-chave: *cryptoassets*; criptomoedas; *blockchain*; proteção de dados; branqueamento de capitais; financiamento ao terrorismo; RGPD; AML/CFT

ABSTRACT

This master's thesis offers an analysis of cryptoassets, with a special focus on cryptocurrencies, AML/CFT (Anti-Money Laundering / Combating the Financing of Terrorism) regulation and data protection. Initially, it addresses the nature of cryptoassets, mentioning their categories, such as virtual currencies, utility tokens and security tokens, as well as aspects of blockchain technology. The implications of cryptoassets for money laundering and terrorist financing are discussed, with an analysis of regulatory responses, in the European Union and in Portugal. The dissertation investigates AML/CFT regulations, evaluating how they affect the cryptoassets market and the practices of financial institutions. Furthermore, the research addresses the issue of data protection, emphasizing the relevance of the EU General Data Protection Regulation (GDPR), and how this interacts with the regulation of cryptoassets.

Keywords: cryptoassets; cryptocurrencies; blockchain; data protection; money laundering; terrorist financing; GDPR; AML/CFT

“É justo que muito custe o que muito vale”.

Santa Teresa de Ávila

Introdução

Neste trabalho, destaca-se a ascensão meteórica dos *cryptoassets*, uma inovação que transformou profundamente o cenário financeiro e económico global, que desafia as normas tradicionais e introduz novos paradigmas no comércio e investimento digital. Estes ativos digitais, que vão além das moedas tradicionais, representam uma mudança fundamental na forma como são concebidas as transações financeiras, abrindo caminho para uma era de inovações tecnológicas e desafios regulatórios. A análise dos *cryptoassets* neste contexto é primordial, pois eles não apenas remodelam o sistema financeiro, mas também levantam questões importantes sobre segurança, privacidade e estabilidade económica.

Os *cryptoassets* são diversos, suas categorias, incluem moedas virtuais como o *Bitcoin*, *tokens* de utilidade que oferecem acesso a serviços específicos e *tokens* de segurança que representam ativos reais ou direitos financeiros. Esta diversidade provoca desafios regulatórios e operacionais, visto que cada tipo de *cryptoasset* interage de maneira diferente com os mercados financeiros e os sistemas legais existentes. Esta dissertação foca-se no entendimento das criptomoedas.

A tecnologia *blockchain* é o fundamento sobre o qual os *cryptoassets* são construídos, fornecendo uma infraestrutura descentralizada, segura e transparente. Esta tecnologia não só viabiliza as transações de *cryptoassets*, mas também tem o potencial de revolucionar diversas outras indústrias, fornecendo soluções para problemas de transparência e eficiência. A *blockchain* é mais do que uma tecnologia; é uma inovação disruptiva que desafia o *status quo,* oferecendo novas formas de realizar e registar transações em um ambiente digital.

O surgimento dos *cryptoassets* trouxe desafios significativos para os reguladores globais, que se esforçam para adaptar os sistemas legais existentes a um cenário financeiro em rápida mudança. A natureza descentralizada e muitas vezes anónima ou pseudónima dos *cryptoassets* dificulta os esforços de regulação e supervisão, exigindo uma abordagem inovadora que consiga equilibrar a regulamentação e a promoção da inovação. As complexidades inerentes a esse tema são exploradas nesta dissertação, ao

abordar os meios como os reguladores respondem (e podem responder) efetivamente a esse fenómeno emergente.

Os desafios que os *cryptoassets* apresentam no contexto de políticas *Anti-Money Laundering* (AML) e *Combating the Financing of Terrorism* (CFT) devem-se, sobretudo, à sua natureza descentralizada, anónima e à ausência de fronteiras internacionais. Por consequência, eles podem ser utilizados para atividades ilícitas, como branqueamento de capitais e financiamento ao terrorismo. Esta dissertação aborda como as estruturas regulatórias existentes estão sendo adaptadas para mitigar esses riscos e examina a eficácia dessas medidas no contexto dinâmico dos *cryptoassets*.

A União Europeia tem tratado o tema de forma proativa e desenvolvido regulamentos específicos acerca da matéria, que visam promover a integridade do mercado financeiro, proteger os consumidores e prevenir atividades ilícitas. Nesse sentido, é feito um estudo sobre essas políticas e diretrizes da UE, com destaque para as suas estratégias com vistas a integrar os *cryptoassets* no sistema financeiro regulamentado.

A questão da proteção de dados no contexto dos *cryptoassets* é um tema sensível a ser trabalhado, uma vez que a natureza descentralizada e anónima das transações de *cryptoassets* levanta dúvidas significativas sobre privacidade e segurança de dados. A aplicação do Regulamento Geral de Proteção de Dados (RGPD) e a complexidade na efetiva proteção dos dados no contexto das criptomoedas, sem inibir a inovação tecnológica, são temas de destaque nesta dissertação. São analisados exemplos específicos que ilustram como esses ativos estão sendo implementados na realidade e aplicações práticas dos *cryptoassets*, enfatizando tanto os sucessos quanto os desafios.

Foi feita uma análise crítica das abordagens regulatórias atuais para os *cryptoassets*. Destaca-se os potenciais caminhos futuros para esses ativos digitais e as tendências emergentes no campo. A discussão se concentra em avaliar a adequação das medidas regulatórias atuais e especular sobre as dificuldades e oportunidades que podem surgir com a evolução dos *cryptoassets*.

Finalmente, as conclusões principais dessa dissertação são apresentadas, oferecendo uma visão geral do tema proposto, com a finalidade de guiar a análise do

tema, cobrindo os aspectos teóricos e práticos dos *cryptoassets*, sua regulamentação e repercussão na proteção de dados.

I – Conceitos básicos de *Cryptoassets* e dos crimes de branqueamento de capitais e financiamento ao terrorismo

Antes de adentrarmos profundamente na análise do equilíbrio entre a necessidade de regulamentação AML/CFT no contexto de *cryptoassets* e a proteção de dados, é crucial estabelecer uma sólida compreensão dos conceitos fundamentais envolvidos. Serão abordadas três áreas principais: *cryptoassets*, regulamentação AML/CFT, e a proteção de dados.

O primeiro subtema, 1.1, dedica-se à definição e classificação de *cryptoassets*, bem como à explanação acerca da tecnologia por detrás das criptomoedas, a *blockchain*. *Cryptoassets*, ou criptoactivos em português, são um fenómeno relativamente recente que tem desafiado as concepções tradicionais de dinheiro e activos. Dada a importância deste conceito para a análise, é fundamental fornecer uma visão geral detalhada do quê são os *cryptoassets*, como são categorizados e o contexto do seu surgimento.

A seguir, no subtema 1.2, será voltada para os conceitos dos crimes de branqueamento de capitais e de financiamento do terrorismo. Serão abordados os conceitos, a legislação e como as criptomoedas são utilizadas como ferramentas para atingir a finalidade do cometimento desses crimes.

Esta seção visa criar uma base conceitual para a análise subsequente dos desafios e oportunidades que a intersecção desses conceitos apresenta. A análise desses conceitos é relevante, uma vez que é fundamental compreendê-los para ser possível conciliar os bens jurídicos que devem ser protegidos.

1.1. *Cryptoassets*: Surgimento, definição e classificação

Cryptoassets, um termo que abrange um espectro de activos digitais que utilizam a criptografia, surgiram como um subproduto da revolução digital, desafiando as perceções tradicionais de dinheiro e activos. O mais conhecido destes, o *Bitcoin*, foi

introduzido em 2008 através de um documento, chamado *white paper*[1], publicado por um indivíduo ou grupo conhecido como Satoshi Nakamoto. Este *white paper* propunha uma forma descentralizada de dinheiro digital que, em vez de depender de uma entidade centralizada como um banco ou governo, depende de uma rede de pares, cada um dos quais mantém um registo de todas as transacções realizadas. Esta rede de pares e o seu registo de transacções é conhecido como uma *blockchain*.

Como Don Tapscott e Alex Tapscott[2] exploram em seu livro *Blockchain Revolution*, esta tecnologia "não apenas desafia as estruturas tradicionais de moeda, mas também tem o potencial de revolucionar diversos setores além das finanças, redefinindo a forma como é feita a interação com o mundo digital". William Mougayar[3], em *The Business Blockchain*, discute com mais detalhe as propostas desta inovação tecnológica, dando destaque ao seu "impacto potencial e profundo no futuro da Internet". A introdução do *Bitcoin* acarretou em uma significativa evolução dos *cryptoassets*, que atualmente abrangem diferentes categorias, cada uma com as suas próprias características e usos: moedas virtuais, *tokens* de utilidade e *tokens* de segurança.

As moedas virtuais, também conhecidas como criptomoedas, são a categoria mais conhecida de *cryptoassets*. Elas são essencialmente versões digitais do dinheiro, que têm como objectivo proporcionar um meio de troca seguro, eficiente e descentralizado. *Bitcoin* e *Ethereum* são exemplos de moedas virtuais.

Os *tokens* de utilidade representam acesso a um serviço específico fornecido por uma rede *blockchain*. Eles não se destinam a ser utilizados como moeda, mas, em vez disso, oferecem aos utilizadores a capacidade de interagir com uma plataforma *blockchain* de uma determinada maneira. Um exemplo seria o *token BAT* do navegador *Brave*, que pode ser usado para compensar os criadores de conteúdo na plataforma.

Os *tokens* de segurança, por outro lado, representam uma participação em um activo subjacente, tal como ações de uma empresa ou direitos a fluxos de receita futura. Estes *tokens* são frequentemente sujeitos à regulamentação financeira, dado o seu

[1] NAKAMOTO, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Consultado em 24 de janeiro de 2024. Disponível aqui: https://bitcoin.org/bitcoin.pdf
[2] TAPSCOTT, Don, & TAPSCOTT, Alex, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. 1.ª Edição, Senai-SP, São Paulo-SP, 2017, p. 238.
[3] MOUGAYAR, William. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, 1.ª Edição, Wiley, New Jersey, 2016, p. 137.

carácter semelhante ao dos instrumentos financeiros tradicionais. Zetzsche, Buckley, Arner e Föhr[4], em *The ICO Gold Rush*, abordam os desafios regulatórios apresentados pelas Ofertas Iniciais de Moedas (ICOs), com enfoque nas "complexidades e os riscos associados a estes instrumentos financeiros emergentes".

A classificação dos *cryptoassets* tem um papel significativo na análise subsequente da necessidade de regulamentação AML/CFT e da proteção de dados, uma vez que cada categoria tem sua peculiaridade do ponto de vista regulatório.

1.1.1. Contexto do surgimento – A 4.ª Revolução Industrial

Pode até passar despercebido por alguns, mas a realidade é que estamos a viver um momento divisor de águas no mundo. As transformações que estamos a assistir e experienciar no âmbito tecnológico refletem em todos os setores da vida humana e impactam na existência de todos. Claramente, trata-se de uma transição muito relevante que está a quebrar paradigmas e alterar profundamente as relações humanas.

O conceito de Quarta Revolução Industrial foi proposto em 2016 por Klaus Schwab, alemão fundador do Fórum Económico Mundial, que afirma que "ao permitir 'fábricas inteligentes', a quarta revolução industrial cria um mundo onde os sistemas físicos e virtuais de fabricação cooperam de forma global e flexível[5]". Schwab ainda ratifica que "as mudanças são tão profundas que, na perspectiva da história da humanidade, nunca houve um momento tão potencialmente promissor ou perigoso[6]".

O escopo desta atual revolução é muito abrangente. As novas descobertas decorrentes do avanço tecnológico pairam sobre todos os setores da sociedade e em todos os campos de trabalho. No âmbito jurídico, a evolução tecnológica tem trazido alterações profundas. As novas relações que surgem juntamente com o avanço tecnológico provocam a necessidade de regulamentá-las.

---

[4] ZETZSCHE, Dirk, BUCKLEY, Ross P., ARNER, Douglas W., & FÖHR, Linus, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, UNSW Sydney Australia, 2018, pp. 15-29. Consultado em 20 de Janeiro de 2024. Disponível aqui: https://dx.doi.org/10.2139/ssrn.3072298

[5] SCHWAB, Klaus, *A quarta revolução industrial*, Edipro, São Paulo: Edipro, 2016, p. 20.

[6] SCHWAB, A quarta.... Op. Cit.

O surgimento de novas tecnologias, produtos e serviços relacionados na última década representa uma das principais mudanças no sistema financeiro global. Essas novas tecnologias têm o potencial de estimular a inovação e a eficiência financeiras e melhorar a inclusão financeira, porém, em contrapartida, também criam novas oportunidades para criminosos e terroristas branquearem seus lucros ou financiarem suas atividades ilícitas.

Em 2008, o programador Santoshi Nakamoto em seu artigo intitulado "*Bitcoin: A Peer-to-Peer Electronic Cash System*[7]", descreveu um novo tipo de moeda exclusivamente assente numa rede direta de participantes baseada numa nova tecnologia (*blockchain*) descentralizada e criptográfica de registo, tratamento e armazenamento eletrónico de dados que permite assegurar um sistema de emissão e circulação de moeda e de pagamentos. Mais tarde, os *cryptoassets* estariam difundidos.

Os *cryptoassets*, nas palavras do Sindicato dos Magistrados do Ministério Público (SMMP)[8], "são representações digitais de ativos baseadas numa tecnologia de registo criptográfico e descentralizada de dados digitais (*blockchain*), não emitidas por um banco central, instituição de crédito ou instituição de moeda eletrónica, que são aceites no âmbito de uma comunidade virtual e são suscetíveis de desempenhar uma pluralidade de funções monetárias e financeiras. O termo engloba as nomenclaturas que normalmente lhe são associadas, como *tokens*, *coins*, criptomoedas ou moedas virtuais. Os criptoativos têm sido muitas vezes associados a atividades como a lavagem de dinheiro e ao comércio de mercadorias proibidas, devido às suas caraterísticas de anonimato, ausência de regulação e natureza global.".

---

[7] "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone." NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*, p. 20. Consultado em 26 de abril de 2022. Disponível aqui: https://bitcoin.org/bitcoin.pdf

[8] CARVALHO, Adão, *O aumento da criminalidade associada às moedas virtuais*, 2021. Consultado em 07 de fevereiro de 2024. Disponível aqui: https://smmp.pt/smmp-na-imprensa/prova-digital-e-correio-eletronico-2/

1.1.2. Natureza dos *cryptoassets* - *Blockchain* e o caráter anónimo

O *Blockchain*, em breves linhas e de forma simplista, é uma tecnologia de banco de dados descentralizado, seguro, irretratável e incorruptível que se transformou numa ferramenta para criação de valor ponto-a-ponto (*peer-to-peer* – P2P) e transações onde não é necessário confiar nos entes envolvidos e em uma autoridade central[9].

O registo de todas as transações já realizadas permanece em todos os nós da rede de forma praticamente imutável, publicamente acessível a todos, e são validadas não por uma autoridade central, como um banco ou um cartório, mas pelos próprios componentes da rede por meio de "provas-de-trabalho" (*proof-of-work*) realizadas através de cálculos criptográficos que levam em consideração também a identidade criptográfica das partes da transação presentes nas suas assinaturas digitais. Ao final, a transação é efetivamente registada em todos os nós do sistema, e é possível identificar as assinaturas digitais utilizadas, mesmo que não se conheça os seus titulares[10].

O *Blockchain* evoluiu de tal forma que não apenas transações e arquivos eletrónicos estáticos podem ser registados nos nós, mas também algoritmos auto-executáveis de acordo com variáveis e condições pré-determinadas. Tal procedimento recebeu o nome de "*smart contracts*" (contratos inteligentes): trata-se de protocolo de tomada de decisões automatizadas, que não se confunde com contratos no significado literal e jurídico do termo, mas sim com obrigações de qualquer natureza, seja a venda de uma casa ou promessas de campanha verbalizadas por candidatos durante o pleito eleitoral, que são acordadas entre diferentes partes e, como mencionado, não precisam se conhecer ou confiar uma na outra. O algoritmo registado no *Blockchain* permite que, no advento da realização de uma condição, ou da não realização, a obrigação escrita no código seja auto-executada, sem qualquer intervenção humana, de uma entidade central ou mesmo imposição pelo Estado, que poderia se valer de formas coercitivas *ex post* para obrigar o cumprimento do contrato. Nesse contexto, alguns afirmam que "o

[9] DE FILIPPI, Primavera, HASSAN, Samer. *Blockchain technology as a regulatory technology: From code is law to law is code*. First Monday, 2016, p. 2. Consultado em 02 de abril de 2021. Disponível aqui: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097430

[10] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*, p. 2. Consultado em 02 de abril de 2021. Disponível aqui: https://bitcoin.org/bitcoin.pdf

Blockchain irá fazer para transações de qualquer natureza o que a *Internet* fez para as telecomunicações"[11].

Blockchain se mostra uma tecnologia tida como anárquica[12] e considerada por muitos revolucionária, que em tese não precisaria se adequar às normas Estatais[13], e que poderia até mesmo substituir qualquer forma de regulação[14]. Todavia, não são poucas as tentativas, privadas e estatais, de regular o seu funcionamento para que seja possível exercer um maior nível de controlo sobre as transações[15]. Alguns autores, no entanto, defendem que o *Blockchain* permitiria um tipo totalmente novo de regulação por meio de código[16] denominada de "*Law is Code"*[17], conceito que trata de leis transpostas para códigos e aplicadas por meio de algoritmos, sem a necessidade de autoridade central, privada ou estatal[18].

Essa tecnologia, aparentemente, ao utilizar algoritmos criptográficos e de assinaturas digitais geradas pelo próprio sistema para validar e individualizar as transações, garantiria, se assim for desenhado, o anonimato das partes, que não

---

[11] ROMETTY, Ginni, *From Yelp reviews to mango shipments: IBM's CEO on how blockchain will change the world*. Business Insider, 2017. Consultado em 31 de março de 2021. Disponível aqui: http://www.businessinsider.com/ibm-ceo-ginni-rometty-blockchain-transactions-internet-communications-2017-6

[12] CACHIN, Christian. *Blockchain-From the Anarchy of Cryptocurrencies to the Enterprise (Keynote Abstract*), 2017. Consultado em 31 de março de 2021. Disponível aqui: https://doi.org/10.4230/LIPIcs.OPODIS.2016.2

[13] DE FILIPPI, Primavera, *Bitcoin: A Regulatory Nightmare to a Libertarian Dream*. Internet Policy Review, 3(2).. 2018, p. 5. Consultado em 25 de março de 2021. Disponíve aqui: https://ssrn.com/abstract=2468695

[14] "Some proponents suggest that blockchain technology could lead to a society where self-enforcing rules would supplant traditional laws (Nakamoto, 2008). Indeed, with the advent of blockchain technology and the introduction of smart contract capabilities on top of it, it becomes increasingly appealing for people to bypass the traditional legal framework of contract law, and to rely on the underlying technical infrastructure provided by the blockchain instead", p. 11, in DE FILIPPI. *Blockchain technology as* ….Op.Cit.

[15] KIVIATT, Trevor I. *Beyond Bitcoin: Issues in Regulating Blockchain Tranactions*. 2015, pp. 20-21. Consultado em 28 de março de 2022. Disponível aqui: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3827&context=dlj

[16] O Parlamento Europeu especificamente já tratou da possibilidade de transformar leis em código por meio de *Blockchain*, vide: *Smart contracts: if code were law*. European Parliament. *How blockchain technology could change our lives*, 2017, pp. 14-15. Consultado em 28 de março de 2021. Disponível aqui: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

[17] Lawrence Lessig cunhou o conceito de "*Code is Law*", ao tratar de como o código, algoritmos, tem o mesmo efeito de leis, permitindo entidades centrais controlarem o ambiente virtual com base em interesses particulares, comerciais ou não, ao ponto de moldar comportamentos. Atualmente se discute uma evolução desse conceito, em que as leis seriam transpostas, também, para código, vide: DE FILIPPI, Primavera. *Blockchain technology as*, p. 2….Op.Cit

[18] WRIGHT, Aaron; DE FILIPPI, Primavera, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 2015, p. 39. Consultado em 28 de março de 2021. Disponível aqui: https://ssrn.com/abstract=2580664

precisariam se identificar para poder realizar qualquer operação[19]. Entretanto, a não identificação do indivíduo por trás da transação não garante totalmente o seu anonimato, muito menos a sua privacidade[20], uma vez que: (i) o conteúdo das transações que serão registradas no *Blockchain* poderá ser acessado, monitorado e analisado por qualquer um da rede[21], dando ensejo a um paradoxo entre transparência e privacidade, por vezes chamado de "*radical transparency*[22]"; e (ii) vários são os casos em que foi possível reidentificar titulares de dados por meio de cruzamento de informações estruturadas e não estruturadas que se valem de metodologias de *big data* para atingir este fim[23], algo que já vem sendo feito, inclusive, em *Blockchain*[24]. Ademais, o fato de os dados e as informações ficarem registadas eternamente no *Blockchain*[25], dificultando o seu apagamento, cancelamento e/ou ofuscamento, pode violar, a princípio, direitos básicos

[19] ZYSKIND, Guy, NATHAN, Oz, PENTLAND, Alex Sandy, *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, IEEE Security and Privacy Workshops, San Jose, CA, 2015, p. 2. Consultado em 28 de março de 2021. Disponível aqui: https://doi.org/10.1109/SPW.2015.27

[20] "Regardless of how careful a person has been to hide his or her identity in the past, once the identity of the person owning that Bitcoin address has been established, it then becomes possible for anyone to retroactively associate to that person all the transactions which have previously been made to and from that address". In DE FILIPPI, Primavera, *The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies*, Journal of Peer Production, 2016, pp. 11-12. Consultado em 01 de abril de 2021. Disponível aqui: https://ssrn.com/abstract=2852689

[21] "The other major problem that blockchains have is privacy. As seductive as a blockchain's other advantages are, neither companies or individuals are particularly keen on publishing all of their information onto a public database that can be arbitrarily read without any restrictions by one's own government, foreign governments, family members, coworkers and business competitors". BUTERIN, Vitalik. *Privacy in the Blockchain*. The Ethereum Blog. Consultado em 29 de março de 2021, Disponível aqui: https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

[22] BRADBURY, Danny, *The problem with Bitcoin*. Computer Fraud & Security, 2013. Consultado em 30 de março de 2021. Disponível aqui: https://doi.org/10.1016/s1361-3723(13)70101-5

[23] "Does privacy of Netflix ratings matter? The privacy question is not "Does the average Netflix subscriber care about the privacy of his movie viewing history?", but "Are there any Netflix subscribers whose privacy can be compromised by analyzing the Netflix Prize dataset?" The answer to the latter question is, undoubtedly, yes. As shown by our experiments with cross-correlating non-anonymous records from the Internet Movie Database with anonymized Netflix records (seebelow), it is possible to learn sensitive non-public information about a person's political or even sexual preferences. We assert that even if the vast majority of Netflix subscribers did not care about the privacy of their movie ratings (which is not obvious by any means), our analysis would still indicate serious privacy issues with the Netflix Prize dataset." NARAYANAN, Arvind, SHMATIKOV, Vitaly. *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset).* The University of Texas at Austin, 2008, p. 11. Consultado em 29 de março de 2021. Disponível aqui: http://arxiv.org/pdf/cs/0610105v2.pdf

[24] "the transparency inherent to these networks is such that anyone can retrieve the history of all transactions performed on a blockchain and rely on big data analytics in order to retrieve potentially sensitive information." In DE FILIPPI, Primavera, *The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies*, Journal of Peer Production, 2016, p. 1. Consultado em 29 de março de 2021. Disponível aqui: https://ssrn.com/abstract=2852689

[25] "In order to prevent anyone from tampering with past transactions, the blockchain acts as an append-only ledger —i.e. once information has been recorded onto the blockchain, it can no longer be edited or deleted.", in DE FILIPPI. The Interplay …. p. 6. Op. Cit.

de proteção de dados pessoais, como os direitos ARCO (*access, rectification, cancelation and opposition*).

Os *cryptoassets*, ativos eletrónicos assentes na tecnologia *blockchain*, carregam o carácter – relativamente – anónimo inerente à tecnologia, o que os tornam uma ferramenta atrativa para o cometimento de crimes, nomeadamente o branqueamento de capitais e o financiamento ao terrorismo.

1.2. Branqueamento de capitais e financiamento ao terrorismo

A estabilidade financeira e a segurança da sociedade são bens valiosos que são atacados diretamente pelos crimes de branqueamento de capitais e financiamento ao terrorismo. Não por acaso esses crimes têm recebido cada vez mais atenção e regulamentação rigorosa na União Europeia (UE), que tem adoptado medidas concretas de combate a essas atividades ilícitas, promovendo uma abordagem unificada entre os Estados membros. Nesta dissertação, serão analisados os desafios, regulamentações e estratégias da UE para prevenir e combater o branqueamento de capitais e o financiamento do terrorismo em seu território.

1.2.1. Branqueamento de capitais: conceito e legislação

O crime de branqueamento de capitais é o processo de tornar ativos financeiros obtidos de atividades ilegais ou ilícitas, como corrupção, tráfico de drogas ou fraude, "limpos" ou aparentemente legais[26], que envolve a ocultação da origem criminosa dos fundos por meio de transações financeiras complexas, na tentativa de dificultar a deteção e a persecução dos crimes subjacentes.

O crime de branqueamento de capitais é uma ameaça significativa à integridade do sistema financeiro na União Europeia, que tem trabalhado na implementação de

[26] CHATAIN, Pierre-Laurent, MCDOWELL, John, MOUSSET, Cedric, SCHOTT Paul Allan, VAN DER DOES DE WILLEBOIS, Emile. *Preventing Money Laundering and Terrorist Financing – A Practical Guide for Bank Supervisors.* The World Bank, Washington, DC. 2009.

rigorosas regulamentações e diretrizes para combater esse crime. A 5ª Diretiva *Anti-Money Laundering and Combating the Financing of Terrorism* (5AML/CFT) é a Diretiva em vigor mais atual que trata do assunto na União Europeia. Há uma proposta de alteração, porém ainda não está vigente, que passará a ser a 6AML/CFT. A 5AML/CFT estabelece requisitos rigorosos para identificação de clientes, *due diligence* e relatórios de transações suspeitas. Para além disso, a UE promove a cooperação internacional por meio do Grupo de Ação Financeira Internacional (GAFI) e busca alinhar suas políticas com os padrões globais de combate ao branqueamento de capitais.

Na União Europeia e em Portugal, as legislações relacionadas ao crime de branqueamento de capitais são extensas e detalhadas, abrangendo medidas preventivas e repressivas. Em Portugal, a Lei n.º 83/2017, de 18 de agosto, estabelece medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo. Esta lei transpõe parcialmente as Diretivas 2015/849/UE e 2016/2258/UE do Parlamento Europeu e do Conselho, além de alterar o Código Penal e o Código da Propriedade Industrial. A Lei n.º 58/2020, de 31 de agosto, que transpõe a Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, também tem relevândia para o tema. Esta diretiva altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para fins de branqueamento de capitais ou de financiamento do terrorismo, bem como a Diretiva (UE) 2018/1673 relativa ao combate ao branqueamento de capitais através do direito penal.

No âmbito da União Europeia, diversas diretivas e regulamentos são fundamentais para a legislação contra o branqueamento de capitais. Entre elas, destacam-se a Diretiva (UE) 2015/849 4AML/CFT, a Diretiva (UE) 2018/843 5AML/CFT, que altera a anterior, e a Diretiva (UE) 2018/1673, todas voltadas para a prevenção da utilização do sistema financeiro para o branqueamento de capitais e o financiamento do terrorismo. Além disso, o Regulamento (UE) 2018/1672 trata do controlo das somas em dinheiro líquido que entram ou saem da União Europeia.

O Banco de Portugal desempenha um papel crucial na supervisão e verificação do cumprimento das obrigações de prevenção do branqueamento de capitais e do financiamento do terrorismo, conforme estabelecido na Lei n.º 83/2017 e em legislação complementar. A Instituição também participa na elaboração do quadro normativo nacional e internacional referente à prevenção do branqueamento de capitais e financiamento ao terrorismo. Essas legislações representam um esforço conjunto para

combater o branqueamento de capitais e o financiamento do terrorismo, tanto em Portugal como em toda a União Europeia.

Relativamente ao crime de branqueamento de capitais, a doutrina destaca as fases que o envolvem, no objectivo de obscurecer a trilha do dinheiro "sujo". São as seguintes[27]:

Colocação (*Placement*)[28]: Nesta fase, o dinheiro ilegal é introduzido no sistema financeiro, muitas vezes através de pequenas transações, com o intuito de ocultar o montante.

Estratificação (*Layering*)[29]: Os valores são movidos e ocultados por meio de transações mais complexas (transferências internacionais e investimentos em ativos), a fim de que a sua origem seja obscurecida.

Integração (*Integration*): Nesta etapa final, o capital, com a aparência de "limpo" pode ser reintroduzido na economia legal, e geralmente o fazem sob a forma de ativos ou investimentos.

Os *cryptoassets* são utilizados comumente nas fases iniciais do crime.

1.2.1.1. Utilização de *cryptoassets* no crime de branqueamento de capitais

As criptomoedas podem ser utilizadas para a colocação e estratificação de dinheiro oriundo do crime, para fins de branqueamento. Durante a fase da colocação, descrita anteriormente, o dinheiro obtido por meio ilegal é introduzido no sistema financeiro através de depósitos bancários, compras de criptomoedas, compras de ítens de valor (como arte ou joias), ou usando-o em negócios que lidam com grandes volumes de numerário (como casinos, bares, ou lavandarias), de modo que o dinheiro não possa ser rastreado ao crime que o originou.

É possível comprar criptomoedas nos caixas eletrónicos criptografados, específicos para o efeito, ou em casas de *exchange* de criptomoedas. Uma organização de tráfico de drogas, por exemplo, pode utilizar um caixa eletrónico criptografado para trocar dinheiro por *Bitcoins*. Os caixas eletrónicos criptografados estão localizados em

[27] BRAGUÊS, José Luis. *O Processo de Branqueamento de Capitais*, Edições Húmus & OBEGEF, 2009, pp. 9-16. Consultado em 10 de janeiro de 2024. Disponível aqui: https://obegef.pt/wordpress/wp-content/uploads/2009/02/wp0021.pdf

[28] CHOO, Kim-Kwang Raymond. *New payment methods: A review of 2010–2012 FATF mutual evaluation reports*, Computers & Security, Volume 36, 2013, p. 8. Consultado em 10 de Janeiro de 2014. Disponível aqui: https://doi.org/10.1016/j.cose.2013.01.009.

[29] DUARTE, Jorge Manuel Vaz Monteiro Dias. *Branqueamento de Capitais - O Regime do D.L 15/93, de 22 de Janeiro, e a Normativa Internacional*. Coimbra Editora, 2002, pp. 35-39

quase todas as jurisdições e podem ser encontrados *online*, através de uma aplicação a ser instalada no telemóvel.

A depender da localização e das regulamentações locais, nem sempre exigem identificação do indivíduo aquando da aquisição das criptomoedas. Quando são necessários, exigem um número de telefone ou podem exigir a verificação de identidade, que seria um procedimento mais complexo de identificação, o *Know Your Costumer* (KYC). Nesse caso, o crime organizado pode, portanto, providenciar um "testa de ferro", ou seja, alguém que faça as transações para ele, através de um telefone pré-pago descartável, para usar um caixa eletrónico criptografado; caso seja requisitada a identificação, o "testa de ferro" usará seu próprio passaporte. Essa pessoa depositaria numerário, que a máquina converteria automaticamente em *Bitcoin* ou outra criptomoeda. Se o indivíduo não tiver uma carteira criptografada, o caixa eletrónico criará uma para ele. O recibo da transação pode ser descartado, de forma que não haverá rastro digital nem em papel conectando os traficantes à criptomoeda emitida.

Indivíduos que tencionam branquear o capital oriundo de ilícitos podem enviar e receber criptomoedas entre diferentes carteiras criptografadas, bem como podem trocá-las por outras moedas digitais. Os chamados "misturadores[30]" oferecem este serviço em troca de 1% a 3% do montante que está sendo "misturado". Para o método *mixer*, os lavadores de dinheiro exigem uma carteira *clearnet*[31] e pelo menos duas carteiras *darknet*[32]. As moedas adquiridas são transferidas da carteira *clearnet* para uma carteira *darknet*; esse chamado "salto" pode ser realizado várias vezes, e cada novo salto adiciona-se outra camada de opacidade às moedas. Assim que as moedas forem colocadas em uma carteira *darknet*, pode-se começar a usar o serviço *mixer*, que consiste em dividir automaticamente as moedas e as transferir para diferentes endereços *darknet*, dificultando assim a conexão delas ao endereço *Bitcoin* original ou entre si.

[30] "Bitcoin mixers (also known as 'tumblers') purportedly clean dirty cryptocurrency by bouncing it between various addresses, before recombining the full amount through a Bitcoin wallet hosted on the dark web. Mixing services split up Bitcoin, only to reassemble it". CANELLIS, David. *Here's how criminals use Bitcoin to launder dirty money*. Consultado em 24 de janeiro de 2024. Disponível aqui: https://thenextweb.com/news/bitcoin-money-laundering-2

[31] "The term 'Clearnet' was coined, which refers to the normal, publically accessible Internet at large". AKED, Symon, BOLAN, Christopher, BRAND, Murray. *Determining What Characteristics Constitute a Darknet*, 2013, p. 14. Consultado em 25 de janeiro de 2024. Disponível aqui: https://doi.org/10.4225/75/57b561bfcd8e0

[32] "The usage of 'Darknet' has evolved over time to refer collectively to all encrypted communication networks that allow anonymous participation, and do so using a de-centralised, peer-to-peer network topology, running inside the Internet". AKED, Symon, BOLAN, Christopher, BRAND, Murray. *Determining What Characteristics Constitute a Darknet*. 2013, p. 4. Consultado em 25 de janeiro de 2024. Disponível aqui: https://doi.org/10.4225/75/57b561bfcd8e0

Quando o processo termina, as moedas são agrupadas novamente em uma carteira *darknet* e transferidas de volta para a carteira *clearnet* original. O dinheiro agora está "limpo" e pode ser trocado de volta por moeda fiduciária ou mantido como um ativo digital. Uma troca por moeda fiduciária acrescentaria mais um grau de opacidade.

Também é possível utilizar *exchanges* de criptomoedas não regulamentadas que não aplicam protocolos KYC ou AML, que não exigiriam a identificação do beneficiário efetivo,[33] para o cometimento do crime de branqueamento de capitais.

[33] Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, 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, que altera o Regulamento (UE) n.° 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão (Texto relevante para efeitos do EEE), 4AML/CFT. Consultado em 30 de abril de 2021. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015L0849 .
Art.º 3.º
6) «Beneficiário efetivo»: a pessoa ou pessoas singulares que, em última instância, detêm a propriedade ou o controlo do cliente e/ou a pessoa ou pessoas singulares por conta de quem é realizada uma operação ou atividade, incluindo pelo menos:
a) No caso das entidades societárias:
i) a pessoa ou pessoas singulares que, em última instância, detêm a propriedade ou o controlo, direto ou indireto, de uma percentagem suficiente de ações ou dos direitos de voto ou de participação no capital de uma pessoa coletiva, incluindo através da detenção de ações ao portador, ou que exercem controlo por outros meios sobre essa pessoa coletiva, que não seja uma sociedade cotada num mercado regulamentado sujeita a requisitos de divulgação de informações consentâneos com o direito da União ou sujeita a normas internacionais equivalentes que garantam suficiente transparência das informações relativas à propriedade.
A detenção, por uma pessoa singular, de uma percentagem de 25 % de ações mais uma ou de uma participação no capital do cliente superior a 25 % é um indício de propriedade direta. A detenção de uma percentagem de 25 % de ações mais uma ou de uma participação no capital do cliente de mais de 25 % por uma entidade societária que está sob o controlo de uma ou várias pessoas singulares, ou por várias entidades societárias que estão sob o controlo da mesma pessoa ou pessoas singulares é um indício de propriedade indireta. Esta disposição é aplicável sem prejuízo do direito dos Estados-Membros a decidirem que uma percentagem mais baixa pode indiciar propriedade ou controlo. O controlo através de outros meios pode ser determinado, inter alia, segundo os critérios estabelecidos no artigo 22.o, n.os 1 a 5, da Diretiva 2013/34/UE do Parlamento Europeu e do Conselho (29);
ii) se, depois de esgotados todos os meios possíveis e na condição de não haver motivos de suspeita, não tiver sido identificada nenhuma pessoa nos termos da subalínea i), ou se subsistirem dúvidas de que a pessoa ou pessoas identificadas sejam os beneficiários efetivos, a pessoa ou pessoas singulares que detêm a direção de topo; as entidades obrigadas conservam registos das ações levadas a cabo para identificar os beneficiários efetivos nos termos da subalínea i) e da presente subalínea;
b) No caso dos fundos fiduciários (*trusts*):
i) o fundador (*settlor*),
ii) o administrador ou administradores fiduciários (*trustees*) de fundos fiduciários,
iii) o curador, se aplicável,
iv) os beneficiários ou, se as pessoas que beneficiam do centro de interesses coletivos sem personalidade jurídica ou da pessoa coletiva não tiverem ainda sido determinadas, a categoria de pessoas em cujo interesse principal o centro de interesses coletivos sem personalidade jurídica ou a pessoa coletiva foi constituído ou exerce a sua atividade,
v) qualquer outra pessoa singular que detenha o controlo final do trust através de participação direta ou indireta ou através de outros meios;
c) No caso das pessoas coletivas como as fundações e centros de interesses coletivos sem personalidade jurídica similares a fundos fiduciários (trusts), a pessoa ou pessoas singulares com posições equivalentes ou similares às mencionadas na alínea b).

Através dessas *exchanges*, não é preciso utilizar a figura do misturador, de modo que é possível branquear capitais ao realizar diversas *exchanges* envolvendo diferentes moedas. Importa salientar que a eficácia deste método está condicionada ao grau de regulamentação AML/CFT ao qual aquelas *exchanges* estão submetidas.

Repetidamente, dados publicados[34] por especialistas, pesquisadores e empresas de *blockchain* ilustram que grandes proporções de criptomoedas são desviadas para crimes financeiros. Fabian Maximilian Johannes Teichmann e Marie-Christin Falker[35], em *Money laundering via cryptocurrencies – potential solutions from Liechtenstein* mencionam que "as dificuldades na regulamentação das criptomoedas podem ser atribuídas ao fato de as criptomoedas serem alimentadas por *blockchain*. Devido à sua descentralização, este livro público está fora do alcance dos governos, o que também o torna adequado para contornar sanções ou outros crimes financeiros. Como o *blockchain* é uma rede descentralizada, não há nenhum responsável pela rede que possa ser sancionado por atividades ilícitas que ocorram nela."

1.2.2. Financiamento ao terrorismo: conceito e legislação

O crime de financiamento ao terrorismo na União Europeia (UE) está regulamentado na 4AML/CFT, em seu atigo 1.º, n.º 5, o que preleciona que se trata de "o fornecimento ou a recolha de fundos, por qualquer meio, direta ou indiretamente, com a intenção de os utilizar, ou com conhecimento de que serão utilizados, no todo ou em parte, para praticar uma das infrações previstas nos artigos 1.º a 4.º da Decisão-Quadro 2002/475/JAI do Conselho". Também encontra-se determinado no art.º 11.º da Diretiva 2017/541, que afirma que "1. Os Estados-Membros tomam as medidas necessárias para assegurar que seja punível como infração penal, quando cometido com dolo, o fornecimento ou a recolha de fundos, seja por que meio for, direto ou indireto,

[34] "Cryptocurrencies are increasingly used to launder the proceeds of drug trafficking. In recent years, EU law enforcement authorities carried out several investigations into the laundering of drug trafficking proceeds using cryptocurrencies. These large-scale laundering activities normally involve specialised criminal networks that provide professional crypto money laundering services". *Cryptocurrencies: Tracing the Evolution of Criminal Finances*. Europol Spotlight, 2021, p. 15. Consultado em 25 de Janeiro de 2024. Disponível aqui: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

[35] MAXIMILIAN JOHANNES TEICHMANN, Fabian and FALKER, Marie-Christin. *Money laundering via cryptocurrencies – potential solutions from Liechtenstein*. 2020, p. 99. Consultado em 25 de Janeiro de 2024. Disponível aqui https://doi/10.1108/JMLC-05-2020-0060

com a intenção de serem utilizados, ou com conhecimento de que serão utilizados, total ou parcialmente, para cometer qualquer das infrações referidas nos artigos 3.º a 10.º ou para contribuir para a sua prática. 2. Caso o financiamento do terrorismo a que se refere o n.º 1 do presente artigo diga respeito a qualquer das infrações previstas nos artigos 3.º, 4.º e 9.º, não é necessário que os fundos sejam efetivamente utilizados, no todo ou em parte, para cometer uma dessas infrações ou para contribuir para a sua prática, nem é necessário que o autor do financiamento saiba para que infração ou infrações específicas os fundos serão utilizados.".

A definição de grupo terrorista está disposta no art.º 2,º 3 da Diretiva 2017/541, que determina como sendo "uma associação estruturada de mais de duas pessoas, que se mantém ao longo do tempo e atua de forma concertada com o objetivo de cometer infrações terroristas; entende-se por «associação estruturada» uma associação que não é constituída de forma fortuita para a prática imediata de uma infração e que não tem necessariamente funções formalmente definidas para os seus membros, nem continuidade na sua composição nem uma estrutura elaborada".

Pode-se dizer, portanto, que o crime de financiamento ao terrorismo refere-se à ação de fornecer recursos financeiros (transferências de capitais ou qualquer apoio financeiro direto ou indireto) ou os materiais (armas, bombas, etc.) para organizações terroristas ou indivíduos envolvidos em atividades terroristas, que possa contribuir para a execução de atos terroristas.

As infrações terroristas e infrações relacionadas com um grupo terrorista estão definidas nos artigos 3.º e 4.º da Diretiva 2017/541, e passam por ofensa contra a vida humana suscetíveis de causar a morte, rapto, ameaça, etc.

1.2.2.1. Utilização de *cryptoassets* no crime de financiamento ao terrorismo

O uso de criptomoedas no financiamento ao terrorismo na União Europeia é um tema de crescente preocupação para os órgãos reguladores e de aplicação da lei. As criptomoedas, devido à sua natureza descentralizada e, em alguns casos, ao anonimato que oferecem, podem ser utilizadas para facilitar atividades ilícitas, incluindo o financiamento ao terrorismo.

O crime de financiamento ao terrorismo e o de branqueamento de capitais, quanto à vertente financeira, podem ter aspetos similares, uma vez que a origem do capital a ser branqueado ou utilizado para fins de terrorismo pode ser objeto de ilícito. O

facto é que, em ambos os crimes, o dinheiro precisa ser movimentado de maneira oculta. Relativamente ao crime de financiamento ao terrorismo, o capital em causa não necessariamente oriunda de crimes, porém, para que o fim seja alcançado (aquisição de armas, bombas, contratação de pessoas, etc.), é necessário que o capital chegue até ao destino sem que as autoridades consigam rastreá-lo.

As características das criptomoedas beneficiam que seja alcançado esse objetivo ilícito. Algumas criptomoedas oferecem maior anonimato nas transações, o que pode dificultar o rastreamento do fluxo de fundos. O caráter descentralizado permite que os utilizadores façam transações sem passar por instituições financeiras tradicionais, que têm protocolos de AML/CFT estabelecidos. As criptomoedas podem ser transferidas facilmente através das fronteiras nacionais, o que pode dificultar a aplicação da lei e a supervisão regulatória.

Em contrapartida, a União Europeia tem implementado várias diretivas AML/CFT que incluem medidas para lidar com o uso de criptomoedas em atividades ilícitas. A 5AML/CFT, por exemplo, expandiu o escopo das regulamentações para incluir provedores de serviços de câmbio de criptomoedas e carteiras digitais. Nesse sentido, as plataformas de câmbio de criptomoedas e provedores de carteiras digitais devem submeter-se ao registo junto às autoridades competentes e cumprir as regras de AML/CFT, tais como a realização de verificações de *Due Diligence* do Cliente (KYC). A UE tem trabalhado no sentido de rastrear e combater o uso de criptomoedas nessas atividades.

Apesar dessas medidas, a natureza das criptomoedas e o seu dinamismo apresentam-se como entraves significativos para a regulamentação e aplicação da lei. A identificação e o rastreamento de transações ilícitas em uma rede descentralizada exigem conhecimento técnico avançado e colaboração internacional. Conforme explana relatório da Europol, em *Terrorism Situation and Trend Report*[36] "A forma como as organizações terroristas *jihadistas* movimentam fundos está a evoluir. Mais camadas são usadas para cobrir as transações, que ocorrem globalmente. Por exemplo, as criptomoedas são pagas para uma conta num país onde são retiradas, o montante é dividido e enviado via *hawala* para outros países e posteriormente transferido através de serviços de transferência de dinheiro. Quando enviado para zonas de conflito, o dinheiro

[36] Europol. *European Union Terrorism Situation and Trend Report 2023*, 2023, p. 21. Consultado em 25 de Janeiro de 2024. Disponível aqui: https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf

é normalmente retirado dos escritórios de transferência de dinheiro por mulas monetárias que o entregam ao beneficiário final.".

As criptomoedas acabam por ser uma alternativa para a sociedade, no que importa à facilidade de circulação internacional da moeda, mesmo que não haja algum ilícito envolvido. Isso ocorre principalmente em países onde há uma maior carência da sociedade por serviços financeiros mais eficazes, como é o caso da Venezuela e da Palestina, citados na sequência por Fabian Maximilian Johannes Teichmann e Marie-Christin Falker[37], em *Money laundering via cryptocurrencies – potential solutions from Liechtenstein*: "Embora existam dados limitados disponíveis sobre a utilização de criptomoedas para atividades ilícitas, os volumes de negociação de *Bitcoin* sugerem que a utilização de criptomoedas é mais predominante em países que têm restrições financeiras. A evidência do fenómeno pode ser observada na Palestina, onde os serviços convencionais de transferência de dinheiro, como o *PayPal*, não estão disponíveis, ou na Venezuela, que sofre de uma inflação muito elevada. Na Palestina, a conscientização sobre *Bitcoin* e *Ethereum* entre cidadãos cumpridores da lei e financiadores do terrorismo aumentou desde 2018, principalmente porque os serviços bancários regulares estão em grande parte indisponíveis."

[37]MAXIMILIAN JOHANNES TEICHMANN, Fabian and FALKER, Marie-Christin. *Money laundering via cryptocurrencies – potential solutions from Liechtenstein*, 2020, p. 93. Consultado em 25 de janeiro de 2024. Disponívelaqui: https://doi/10.1108/JMLC-05-2020-0060

2. A Necessidade de Regulamentação AML/CFT para *Cryptoassets*

Os avanços provocados pelos cryptoassets no cenário financeiro global, proporcionando inovação e inclusão financeira, também apresentam desafios significativos, especialmente no que diz respeito à prevenção de branqueamento de capitais e ao financiamento do terrorismo.

Várias jurisdições no mundo têm reconhecido a necessidade de regulamentação AML/CFT para criptoativos. Organizações internacionais como o GAFI têm tomado medidas para estabelecer diretrizes e padrões globais, todavia, os países implementam as recomendações de forma variada.

A importância da implementação de regulamentações eficazes e harmonizado entre os Estados membros com vistas a AML/CFT reflete no crescimento sustentável do setor de criptoativos, tornando possível estabelecer uma base sólida para o setor, capaz de melhorar a confiança dos consumidores e investidores.

2.1. Regulamentação AML/CFT

A legislação AML/CFT da UE é composta por uma série de diretivas e regulamentações destinadas a prevenir a lavagem de dinheiro e o financiamento do terrorismo. As Diretivas AML/CFT da UE estabelecem obrigações para instituições financeiras, incluindo verificações rigorosas de identidade do cliente, relatórios de transações suspeitas e medidas de diligência devidamente aprimoradas. Para além dessas medidas, a UE promove a cooperação internacional e busca alinhar suas políticas com padrões globais, como os do GAFI, para garantir uma abordagem eficaz na luta contra essas atividades ilícitas.

2.1.1. Visão geral

A União Europeia adotou uma legislação de combate ao branqueamento de capitais e financiamento ao terrorismo, que precisa estar em constante evolução. O branqueamento de capitais e o financiamento ao terrorismo representam uma séria ameaça à integridade da economia e do sistema financeiro da União Europeia e à segurança dos seus cidadãos. A Europol estimou que cerca de 1% do Produto Interno

Bruto anual da União Europeia é detetado como estando envolvido em atividades financeiras suspeitas[38], razão pela qual são necessárias reformas no regime da União Europeia AML/CFT.

Em 7 de maio de 2020, a Comissão apresentou um plano de ação[39] para uma política global da União Europeia em matéria de prevenção do branqueamento de capitais e do financiamento do terrorismo. Nesse plano de ação, a Comissão comprometeu-se a tomar medidas para reforçar as regras da União Europeia em matéria de combate ao branqueamento de capitais e ao financiamento do terrorismo e a sua aplicação, com seis prioridades ou pilares:

- Garantir a implementação eficaz do atual quadro AML/CFT da UE;
- Estabelecer um livro único de regras da UE sobre AML/CFT;
- Promover a supervisão AML/CFT a nível da UE;
- Estabelecer um mecanismo de apoio e cooperação para as Unidades de Inteligência Financeira (UIFs), que são responsáveis pela receção e análise de informações relevantes no que toca ao branqueamento de capitais e ao financiamento do terrorismo, nomeadamente sob a forma de relatórios das entidades obrigadas;
- Aplicação das disposições de direito penal a nível da UE e intercâmbio de informações;
- Reforçar a dimensão internacional do quadro AML/CFT da UE.

Em 18 de janeiro de 2024, foi feito o comunicado à comunicação social sobre o acordo feito entre o Conselho e o Parlamento Europeu acerca de regras mais estritas no combate ao branqueamento de capitais. A expetativa, segundo o ministro das Finanças da Bélgica, Vincent Van Peteghem, é a de que esse acordo "melhorará a forma como os

[38] Tribunal de Contas Europeu. *Os esforços da UE para combater o branqueamento de capitais no setor bancário são fragmentados e a aplicação é insuficiente*, 2021, p. 5. Consultado em 25 de janeiro de 2024. Disponível aqui: https://www.eca.europa.eu/Lists/ECADocuments/SR21_13/SR_AML_PT.pdf

[39] Comissão Europeia. *Comissão intensifica a luta contra o branqueamento de capitais e o financiamento do terrorismo*. Bruxelas, 2020. Consultado em 25 de janeiro de 2024. Disponível aqui: https://ec.europa.eu/commission/presscorner/detail/pt/ip_20_800

sistemas nacionais de combate ao branqueamento de capitais e ao financiamento do terrorismo são organizados e cooperam entre si. Garantir-se-á desse modo que os autores de fraudes, a criminalidade organizada e os terroristas não terão margem de manobra para legitimar os seus produtos através do sistema financeiro[40].”

O referido acordo aumenta a lista de entidades que ficam obrigadas à submissão das novas regras, que abrangerão a maior parte do setor dos criptoativos e obrigarão todos os prestadores de serviços desse mercado a exercer o dever de diligência relativo aos seus clientes, o que significa proceder à verificação de factos e informações sobre os seus clientes, nomeadamente as diligências de KYC, bem como comunicar qualquer atividade suspeita.

As medidas de diligência que os prestadores de serviços de criptoativos terão de aplicar referem-se a operações de valor igual ou superior a 1 000 euros efetuadas pela clientela. São ainda acrescidas algumas medidas para diminuir os riscos que envolvem as operações com carteiras sem guarda (*non-custodial wallets*)[41].

Também foram introduzidas, pelo Conselho e pelo Parlamento Europeu, medidas específicas de diligência reforçada para as relações transfronteiras de correspondência para os prestadores de serviços de criptoativos.

Nos termos do acordo, as UIF terão acesso imediato e direto a informações financeiras, administrativas e policiais, nomeadamente a informações fiscais, a informações sobre fundos e outros ativos congelados por força de sanções financeiras específicas, a informações sobre transferências de fundos e transferências de criptoativos, a registos nacionais de veículos a motor, de aeronaves e de embarcações, a dados aduaneiros e a registos nacionais de armas e armas, entre outros.

---

[40] Conselho da União Europeia. *Combate ao branqueamento de capitais: Conselho e Parlamento Europeu chegam a acordo sobre regras mais estritas*. 2024. Consultado em 25 de janeiro de 2024. Disponível aqui: https://www.consilium.europa.eu/pt/press/press-releases/2024/01/18/anti-money-laundering-council-and-parliament-strike-deal-on-stricter-rules/

[41] “Custodial wallets are a range of digital escrow wallets that store crypto assets externally, outside of a user’s device. Non-custodial wallets (carteira sem guarda), on the other hand, can be either software-based or hardware-based and can satisfy different preferences related to security and privacy”. BOWLER, Ryan, GOODELL, Geoffrey, REVANS, Joe, BIZAMA Gabriel, SPEED Chris. *A Non-Custodial Wallet for CBDC: Design Challenges and Opportunities*, 2023, p. 15. Consultado em 25 de janeiro de 2024. Disponível aqui: https://doi.org/10.48550/arXiv.2307.05167

As transferências de ativos virtuais estão hoje enquadradas no MiCA (*Markets in Cryptto Assets*), que começará a ser aplicado em dezembro de 2024. O branqueamento de capitais, o financiamento ao terrorismo e a criminalidade organizada continuam a ser problemas significativos que devem ser abordados uniformemente na União Europeia.

2.1.2. Evolução da legislação no mundo

O combate ao branqueamento de capitais e ao financiamento do terrorismo é um esforço global que tem evoluído ao longo das últimas décadas, à medida que novas ameaças e técnicas são identificadas. Aqui está um breve resumo de alguns dos marcos mais importantes na história da regulamentação AML/CFT.

1970 - Lei do Segredo Bancário (BSA) nos Estados Unidos da América

Pode-se afirmar que o combate moderno ao branqueamento de capitais teve início na década de 70 nos Estados Unidos, com a aprovação da Lei do Segredo Bancário (BSA) nos Estados Unidos, que determinou que as instituições financeiras começassem a manter registos de transações em dinheiro e a relatar certas transações ao governo dos EUA.

1988 - Convenção das Nações Unidas contra o Tráfico Ilícito de Narcóticos e Substâncias Psicotrópicas

Este tratado internacional foi pioneiro no sentido do reconhecimento do branqueamento de capitais como um problema a nível mundial, indicando aos demais países que o criminalizassem. É considerado um notável marco no combate ao branqueamento de capitais.

1989 - Criação do Grupo de Ação Financeira (GAFI)

Os países do G7 criaram o GAFI no intuito de desenvolvimento e promoção de políticas nacionais e internacionais a fim de combater branqueamento de capitais. O GAFI ainda mantem-se ativo e atualmente também atua no combate do financiamento ao terrorismo.

2001 - Lei Patriota dos EUA

Em resposta aos ataques de 11 de setembro, os EUA aprovaram a Lei Patriota, que significativamente aumentou os requisitos de AML/CFT para as instituições financeiras, incluindo novas regras sobre a verificação da identidade do cliente (KYC) e a obrigação de relatar atividades suspeitas.

2015-2023 - Diretivas AML da União Europeia

A União Europeia implementou uma série de diretivas para padronizar e reforçar as regulamentações AML/CFT entre os Estados-membros. Houve um aumento dos requisitos de diligência devida do cliente (*Customer Due Diligence* – CDD) e expansão do escopo das regulamentações para incluir provedores de serviços de criptomoedas.

Directiva 91/308/CEE[42] do Conselho, de 10 de Junho de 1991, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais

Trata-se da primeira legislação europeia sobre o tema branqueamento de capitais, elaborada em 1991. O legislador europeu já considerava que a abordagem penal não deveria ser a única estratégia para combater o branqueamento de capitais, uma vez que o sistema financeiro poderia desempenhar um papel altamente eficaz. Mais, também demonstrou uma preocupação com a identificação dos clientes dos estabelecimentos de créditos e instituições financeiras, "a fim de evitar que os branqueadores de capitais beneficiem do anonimato para desenvolver as suas actividades criminosas[43]".

A Diretiva 91/308/CEE exigia que os países membros da União Europeia implementassem legislação para identificar, prevenir e combater o branqueamento de capitais. Foi essa diretiva que determinou que os bancos e outras instituições financeiras têm a obrigação de implementarem internamente os procedimentos de diligência devida para verificação da identidade dos clientes, manter registos de transações suspeitas e relatar essas transações às autoridades competentes. Essa diretiva é considerada um marco importante na luta contra o branqueamento de capitais na Europa, sendo o

[42] Directiva 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. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31991L0308

[43] Directiva 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. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31991L0308

alicerce para a subsequente adoção de diretivas e regulamentos mais abrangentes sobre AML/CFT na União Europeia.

> Directiva 2001/97/CE[44] do Parlamento Europeu e do Conselho, de 4 de Dezembro de 2001, que altera a Directiva 91/308/CEE do Conselho relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais - Declaração da Comissão

A Diretiva 2001/97/CE foi adotada em 4 de dezembro de 2001 e teve o objetivo de fortalecer as medidas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo na União Europeia.

Essa diretiva trouxe diversas alterações e melhorias em relação à Diretiva 91/308/CEE. Ela ampliou o escopo das atividades e entidades financeiras cobertas pelas medidas de prevenção, incluindo, por exemplo, agentes imobiliários e auditores. Além disso, a Diretiva 2001/97/CE introduziu requisitos mais rigorosos para a identificação dos clientes, a manutenção de registros e a comunicação de transações suspeitas às autoridades competentes.

> Directiva 2005/60/CE[45] do Parlamento Europeu e do Conselho, de 26 de Outubro de 2005, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais e de financiamento do terrorismo (Texto relevante para efeitos do EEE)

A Terceira Diretiva AML (Diretiva 2005/60/CE) revogou e substituiu a Diretiva 2001/97/CE. Ela foi um marco importante no aprimoramento da legislação europeia de prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

Essa diretiva introduziu mudanças significativas, como a expansão do escopo das entidades e atividades abrangidas, aprimorando a diligência devida na identificação de clientes, exigindo a implementação de políticas e procedimentos internos robustos de

[44] Directiva 2001/97/CE do Parlamento Europeu e do Conselho, de 4 de Dezembro de 2001, que altera a Directiva 91/308/CEE do Conselho relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais - Declaração da Comissão Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32001L0097

[45] Directiva 2005/60/CE do Parlamento Europeu e do Conselho, de 26 de Outubro de 2005 , relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais e de financiamento do terrorismo (Texto relevante para efeitos do EEE) Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005L0060

combate à lavagem de dinheiro, além de fortalecer a cooperação entre as autoridades nacionais.

> Diretiva (UE) 2015/849[46] do Parlamento Europeu e do Conselho, 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, que altera o Regulamento (UE) n. 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão (4ª directiva AML)

O termo beneficiário efetivo surge nessa directiva com o intuito de identificar todas as pessoas singulares que detêm a propriedade ou o controlo de uma pessoa coletiva. O legislador considera "um fator essencial para rastrear os agentes do crime, que de outro modo poderão dissimular a sua identidade numa estrutura societária"[47]. Para o efeito, a directiva indica que "Estados-Membros deverão assegurar o armazenamento das informações sobre os beneficiários efetivos num registo central situado fora da sociedade, na plena observância do direito da União[48]".

Nesse sentido, Portugal aprova o Regime Jurídico do Registo Central do Beneficiário Efetivo, transpõe o capítulo III da Diretiva (UE) 2015/849, do Parlamento Europeu e do Conselho, de 20 de maio de 2015, e procede à alteração de Códigos e

[46] Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, 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, que altera o Regulamento (UE) n.° 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão (Texto relevante para efeitos do EEE), 4AML/CFT. Consultado em 30 de abril de 2021. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015L0849

[47] Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, 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, que altera o Regulamento (UE) n.° 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão (Texto relevante para efeitos do EEE), 4AML/CFT. Consultado em 30 de abril de 2021. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015L0849. Considerando 14, 4AML/CFT

[48] Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, 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, que altera o Regulamento (UE) n.° 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão (Texto relevante para efeitos do EEE), 4AML/CFT. Consultado em 30 de abril de 2021. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015L0849. Considerando 14, 4AML/CFT

outros diplomas legais[49], lei que tem como objeto "transposição para a ordem jurídica interna do capítulo III da Diretiva (UE) n.º 2015/849, do Parlamento Europeu e do Conselho, 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, e aprova o Regime Jurídico do Registo Central do Beneficiário Efetivo (RCBE)".

> Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE [50](Texto relevante para efeitos do EEE) (5ª directiva AML)

Essa directiva altera e expande a quarta Diretiva de Lavagem de Dinheiro e aumenta a transparência das informações de beneficiários efetivos, concede às unidades de inteligência financeira um acesso mais amplo às informações, melhora a cooperação entre supervisores e regula moedas virtuais e cartões pré-pagos para melhor prevenir a lavagem de dinheiro e o financiamento do terrorismo.

Salienta-se que a directiva em tela não menciona o termo "criptoativos", mas define moeda virtual como sendo "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 possa ser transferida, armazenada e comercializada por via eletrónica"

2.1.2.1. Proposta à 6.ª Directiva AML/CFT

[49] Lei n.º 89/2017, de 21 de Agosto, Regime Jurídico do Registo Central do Beneficiário Efetivo, Consultado em 01 de maio de 2021, Disponpivel aqui: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2755&tabela=leis&so_miolo=

[50] Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE (Texto relevante para efeitos do EEE), 5AML/CFT, Consultado em 30 de abril de 2021. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32018L0843

A Proposta de Diretiva do Parlamento Europeu e do Conselho, relativa aos mecanismos a criar pelos Estados-Membros para prevenir a utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que revoga a Diretiva (UE) 2015/849[51] será, caso aprovada, a 6ª Directiva AML/CFT.

Trata-se de uma proposta de diretiva, que traz, pela primeira vez, o termo criptoativos, a propor "uma reformulação do Regulamento (UE) 2015/847 no sentido de alargar os requisitos de rastreabilidade aos criptoativos".

A referida proposta faz alterações importantes à 5ª directiva, tais como:

- Amplia o escopo e fornece uma lista dos 22 crimes antecedentes que constituem branqueamento de capitais (ex: crime cibernético);
- Estende a responsabilidade criminal para permitir a punição de pessoas jurídicas, como empresas ou parcerias;
- Introduz uma pena mínima de prisão de 4 anos (a exigência de sentença mínima anterior era de 1 ano);
- Propõe a criação de uma nova autoridade da União Europeia para combater o branqueamento de capitais (AML).

Essa proposta de diretiva aplica-se às transferências de fundos, em qualquer moeda, ou criptoativos, que sejam enviados ou recebidos por um prestador de serviços de pagamento, um prestador de serviços de ativos criptográficos ou um prestador intermediário de serviços de pagamento estabelecido na União Europeia (inclui fichas de dinheiro electrónico).

Orienta preventivamente, no sentido de que as novas obrigações dos prestadores de serviços de criptoativos devem basear-se na aplicação do procedimento de conformidade na origem da transação; bem como na deteção, visto que o prestador de serviços de criptoativos do beneficiário deve implementar procedimentos eficazes para

[51] Proposta de DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO relativa aos mecanismos a criar pelos Estados-Membros para prevenir a utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que revoga a Diretiva (UE) 2015/849, 6AML-CFT, Consultado em 01 de maio de 2021. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0423

detetar se as informações do originador estão incluídas na operação de transferência de criptoativos. O prestador de serviços de criptoativos do beneficiário também deve implementar tais procedimentos (também se aplica ao pagador e ao beneficiário).

Quanto aos dados contidos na transação, o prestador de serviços de criptoativos do originador deve garantir que as transferências de criptoativos sejam acompanhadas dos dados do originador (nome; número da conta, quando uma conta é usada para processar a transação; o endereço do remetente, número do documento pessoal oficial, número de identificação do cliente ou data e local de nascimento) e do beneficiário (nome; o número da conta, caso exista e seja utilizada para processar a transação).

Surgem novas obrigações relacionadas aos criptoativos, tais como:

- O envio das informações do originador e do beneficiário deve ser fornecido antes da transferência ou no momento da conclusão da transação;
- As informações podem ser gravadas por 5 anos;
- Aplica-se a países terceiros: a transferência de criptoativos da União Europeia para fora da União deve conter informações completas sobre o ordenante e o beneficiário;
- Todas as transferências de ativos criptográficos devem ser tratadas como transferências eletrônicas transfronteiriças, sem regime simplificado de transferências eletrônicas domésticas.

As instituições financeiras precisarão adotar e manter uma estrutura de política baseada em risco que atenda às diretrizes regulatórias da proposta a 6AMLD. Estão obrigadas a identificar e abordar, quando necessário, vulnerabilidades percebidas em suas estruturas de políticas, garantindo que as verificações apropriadas sejam definidas e alinhadas com a proposta a 6AMLD quando uma abordagem baseada em risco indicar um nível mais alto de risco. Será necessário que as referidas instituições apliquem uma abordagem baseada em risco ao avaliar e categorizar clientes, relacionamentos e produtos de alto risco, particularmente aqueles associados a criptomoedas. Em virtude de as Instituições Financeiras terem obrigações relativamente aos dados do ordenante e beneficiário, devem ter atenção para evitar conflitos com as regras de proteção de dados.

A proposta a 6AMLD aborda a partilha de dados com base na confidencialidade e na necessidade. O envio de informações confidenciais deve ocorrer de forma imediata e segura; apenas haverá partilha de informações necessárias, tais como nome do remetente, número da conta do remetente e endereço do remetente, número do documento pessoal oficial, número de identificação do cliente ou data e local de nascimento (também se aplica ao beneficiário e ao pagador).

O prestador de serviços de criptoativos do originador deve garantir que as transferências de criptoativos sejam acompanhadas do nome do originador, o número da conta do originador, caso tal conta exista e seja usada para processar a transação; e o endereço do remetente, número do documento pessoal oficial, número de identificação do cliente ou data e local de nascimento; o provedor de serviços de criptoativos do originador também deve garantir que as transferências de criptoativos sejam acompanhadas do nome do beneficiário e do número da conta do beneficiário, caso tal conta exista e seja usada para processar a transação. (6AMLD)

2.1.2.2. MiCA (*Markets in Crypto-Assets*)

Em setembro de 2020, a Comissão Europeia (COM) adotou uma proposta legislativa sobre criptoativos[52], parte do Pacote Financeiro Digital, estabelecendo uma estrutura para um mercado de ativos criptográficos, na tentativa de regular tipos de ativos criptográficos atualmente fora do escopo, como *stablecoins* e fornecedor de serviços de ativos criptográficos. O MiCA entrou em vigor em 29 de junho de 2023 e será aplicável a partir de 30 de dezembro de 2024.

Os objetivos da Proposta de Regulamento passam por fornecer segurança jurídica para criptoativos não cobertos pela legislação de serviços financeiros da UE existente; estabelecer regras uniformes para fornecedores e emissores de serviços de criptoativos a nível da UE; substituir as estruturas nacionais existentes aplicáveis a

[52] Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo aos mercados de criptoativos e que altera a Diretiva (UE) 2019/1937, MiCA, Consultado em 01 de maio de 2021. Disponível aqui: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0006.02/DOC_1&format=PDF

criptoativos não cobertos pela legislação existente de serviços financeiros da UE; estabelecer regras específicas para as chamadas *stablecoins*, inclusive quando se trata de dinheiro eletrônico.

A proposta do MiCA apresenta várias definições em seu artigo 3.º, relacionadas a criptoativos, pelo que importam mencionar as descritas abaixo:

«Tecnologia de registo distribuído» ou «DLT», um tipo de tecnologia que permite o registo distribuído de dados cifrados;

«Criptoativo», uma representação digital de valor ou de direitos que pode ser transferida e armazenada eletronicamente, recorrendo à tecnologia de registo distribuído ou a outra tecnologia semelhante;

«Criptoficha referenciada a ativos», um tipo de criptoativo que procura manter um valor estável por referência ao valor de várias moedas fiduciárias com curso legal, uma ou várias mercadorias ou um ou vários criptoativos, ou a uma combinação desses tipos de ativos;

«Criptoficha de moeda eletrónica», um tipo de criptoativo cujo objetivo principal é ser utilizado como meio de troca e que procura manter um valor estável por referência ao valor de uma moeda fiduciária com curso legal;

«Criptoficha de consumo», um tipo de criptoativo destinado a fornecer acesso digital a um bem ou serviço, disponível através da DLT, e aceite apenas pelo emitente dessa criptoficha;

«Emitente de criptoativos», uma pessoa jurídica que oferece ao público qualquer tipo de criptoativos ou procura obter a admissão de tais criptoativos numa plataforma de negociação de criptoativos;

«Oferta pública», uma oferta a terceiros para que adquiram um criptoativo em troca de moeda fiduciária ou de outros criptoativos;

«Prestador de serviços de criptoativos», qualquer pessoa cuja ocupação ou atividade económica seja a prestação de um ou mais serviços de criptoativos a terceiros de forma profissional.

A proposta do MiCA tem como escopo regular todas as representações digitais de valor ou direitos, que podem ser compartilhadas ou armazenadas eletronicamente, utilizando tecnologia de contabilidade distribuída (Distributed Ledger Technology – DLT) ou similar.

Para fornecer serviços de criptoativos, as empresas precisarão receber autorização prévia dos governos dos estados membros competentes, que será válida em toda a União Europeia. Ficam convenientemente excluídas deste requisito as instituições de crédito e empresas cujos serviços já estejam autorizados pela *Markets in Financial Instruments Directive* (MiFID) como serviços financeiros:

- Semelhante aos requisitos do MIFID, os *Crypto-Asset Service Providers* (CASPs) estarão sujeitos (dependendo de seu tamanho e risco associado) a outros requisitos relacionados aos seus requisitos de capital, modelo de governança, treinamento de pessoal, cobertura de seguro e etc;
- A proteção dos investidores continua sendo um ponto focal e, portanto, outras obrigações sobre separação adequada de ativos, guarda de fundos, estrutura de negócios e qualificação da gestão terão de ser cumpridas.

O MiCA estabelece proibições e requisitos para evitar abusos de mercado envolvendo criptoativos. Como tal, todos os criptoativos com luz verde para negociação em uma plataforma de troca estarão sujeitos a medidas regulatórias que visam combater o abuso desenfreado de mercado há muito associado às trocas de criptomoedas. As autoridades competentes podem impor sanções monetárias na violação do regulamento.

Relativamente à proteção de dados, o MiCA apresenta-se de forma consistente com os princípios estabelecidos no Regulamento Geral de Proteção de Dados (RGPD, Regulamento (UE) 2016/679). Especificamente, o art.º 101.º do MiCA estipula que, "no que respeita ao tratamento de dados pessoais no âmbito do presente regulamento, as autoridades competentes exercem as suas atribuições para efeitos do presente regulamento nos termos do Regulamento (UE) 2016/679. O tratamento dos dados pessoais pela EBA e a ESMA para efeitos do presente regulamento deve ser efetuado nos termos do Regulamento (UE) 2018/1725.".

Este alinhamento assegura que as operações relacionadas com criptoativos, incluindo a coleta, o processamento e a partilha de dados pessoais por autoridades

competentes ou entidades reguladas pelo MiCA, respeitam os direitos fundamentais dos indivíduos à privacidade e à proteção de dados, o que significa que todas as atividades de processamento de dados dentro do escopo do MiCA devem ser justificadas, minimizadas, seguras e transparentes, garantindo aos titulares dos dados o acesso aos seus direitos, como o direito de acesso, retificação e apagamento dos dados, além do direito de objeção e à portabilidade dos dados.

2.2. *Cryptoassets* e Riscos de Branqueamento de Capitais e de Financiamento ao Terrorismo

Os *cryptoassets*, enquanto avanço significativo na tecnologia financeira, apresentam novos desafios em termos de regulamentação e segurança. Um dos riscos mais notórios associados aos *cryptoassets*, nomeadamente às criptomoedas, conforme visto, é o seu potencial uso no branqueamento de capitais e no financiamento ao terrorismo. Portanto, é de suma importância desenvolver e implementar regulamentações rigorosas e sistemas de monitoramento para mitigar esses riscos, garantindo que os avanços tecnológicos dos *cryptoassets* não sejam explorados para fins nefastos.

2.3. As dificuldades de uma Regulamentação AML/CFT para cryptoassets

O crescimento expressivo das criptomoedas e a sua crescente adoção por parte dos consumidores e empresas torna a regulamentação de *cryptoassets* na UE um tema de destaque. O desafio de regular os *cryptoassets* torna-se ainda mais complexo quando se trata de lidar com questões de AML/CFT, visto que a dinâmica única dos *cryptoassets* e a sua natureza descentralizada apresentam um novo conjunto de desafios para os reguladores na UE.

A UE tem trabalhado na criação de um quadro regulatório robusto para os *cryptoassets*. Não apenas para combater o branqueamento de capitais e o financiamento ao terrorismo, mas também com o objectivo de garantir que a inovação possa prosperar enquanto se mantém a integridade do sistema financeiro e se protege os consumidores e investidores.

A UE introduziu a 5AML/CFT, que entrou em vigor em janeiro de 2020. Esta diretiva estende a regulamentação AML/CFT aos prestadores de serviços de câmbio entre criptomoedas e moedas fiduciárias, bem como aos prestadores de carteiras de custódia.

No entanto, a implementação da 5AML/CFT tem sido desigual entre os Estados-membros, com alguns países a adotar uma abordagem mais estrita, enquanto outros têm sido mais lenientes. Esta falta de harmonização pode criar um ambiente regulatório fragmentado que pode desencorajar a inovação e a adoção de *cryptoassets* na região.

Para efetivamente abordar os desafios de regulamentação AML/CFT associados aos *cryptoassets*, é crucial uma cooperação internacional. Dada a natureza global dos cryptoassets, é imperativo que os reguladores da UE colaborem com as suas contrapartes internacionais para desenvolver um quadro regulatório harmonizado.

Países como Chipre e Malta têm sido considerados como melhores destinos para empresas de criptomoedas na UE, uma vez que possuem legislações favoráveis, regimes fiscais atraentes e uma regulamentação flexível. Como membros da UE, seguem as Diretivas AML/CFT da UE, porém ambos os países adotaram medidas estratégicas no intuito de serem reconhecidos mundialmente como referências de inovação e tecnologia financeira.

Malta, especificamente, tem se posicionado como a "*Blockchain Island*", visto que tem adoptado uma legislação atrativa para empresas de *blockchain* e criptomoedas, e, consequentemente, tem promovido a inovação e atraído capitais. Em 2018, foram aprovadas três leis importantes em Malta que são consideradas a base de sua legislação para a tecnologia *blockchain* e criptomoedas, que são *Malta Digital Innovation Authority Act*[53] (MDIA Act), *Innovative Technology Arrangements and Services Act* [54](ITAS Act) e *Virtual Financial Assets Act* (VFA Act)[55]. Importa mencionar que nessas

[53] Malta Digital Innovation Authority Act, Chapter 591. "AN ACT to provide for the establishment of an Authority to be known as the Malta Digital Innovation Authority, to support the development and implementation of the guiding principles described in this Act and to promote consistent principles for the development of visions, skills, and other qualities relating to technology innovation, including distributed or decentralised technology, and to exercise regulatory functions regarding innovative technology, arrangements and related services and to make provision with respect to matters ancillary thereto or connected therewith" Consultado em 26 de Janeiro de 2024, Disponível aqui: https://legislation.mt/eli/cap/591/eng

[54] Innovative Technology Arrangements And Services Act. Chapter 592. "AN ACT to provide for the regulation of designated innovative technology arrangements referred to in this Act, as well as of designated innovative technology services referred to in this Act, and for the exercise by or on behalf of the Malta Digital Innovation Authority of regulatory functions with regard thereto." Consultado em 26 de Janeiro de 2024, Disponível aqui: https://legislation.mt/eli/cap/592/eng/pdf

legislações há a tentativa de conciliação entre o fomento do mercado de criptomoedas, tornando o país atrativos para essas emrpesas, e a regulação AML/CFT, conforme está disposto nos textos das respetivas leis.

Há, por outro lado, iniciativas na tentativa de melhor uniformizar a nível global esses entendimentos sobre o tema. A FATF (Financial Action Task Force) é um organismo intergovernamental global que estabelece padrões internacionais para prevenir atividades financeiras ilícitas. A Iniciativa de Travel Rule da FATF[56] é um exemplo de como a cooperação internacional pode ajudar a abordar os desafios de AML/CFT associados aos cryptoassets. A *Travel Rule* é parte da Recomendação 16 da FATF, que originalmente se aplicava a bancos e outras instituições financeiras. A regra exige que os provedores de serviços de ativos virtuais (*Virtual Asset Service Providers* – VASPs) transmitam informações sobre os remetentes e destinatários durante as transações de criptomoedas, com o objetivo de garantir que as transações de criptomoedas passem a ser transparentes e, portanto, rastreáveis, com a finalidade de as autoridades detetarem o branqueamento de capitais e o financiamento do terrorismo. Assim, os países membros devem implementar regulamentos no sentido de obrigarem os prestadores de serviços de ativos virtuais a recolher e transmitir informações (dados) sobre os remetentes e destinatários de transações. Os desafios na implementação da *Travel Rule* no setor das criptomoedas passam pela dificuldade técnica relativamente à privacidade e à interoperabilidade entre diferentes plataformas e tecnologias. Na tentativa de obtenção de conformidades entre os diferentes países membros[57] da FATF, os mesmos foram encorajados a implementar essas regras em suas jurisdições, levando a uma variedade de abordagens regulatórias.

---

[55] Virtual Financial Assets Act, Chapter 590. "AN ACT to regulate the field of Initial Virtual Financial Asset Offerings and Virtual Financial Assets and to make provision for matters ancillary or incidental thereto or connected therewith." Consultado em 26 de Janeiro de 2024, Disponível aqui: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=NIM:202103962

[56] FATF, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation*, The FATF Recommendations, 2023. "Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available", 2023, p. 80. Consultado em 26 de Janeiro de 2024. Disponível aqui: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

[57] FATF, *Country Members*. "Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, European Commission, Finland, France, Germany, Greece, Gulf Co-operation Council, Hong Kong, China, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Malaysia, Mexico, Netherlands, New Zealand, Norway, Portugal, Russian Federation (suspended), Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Türkiye, United Kingdom, United States". Consultado em 26 de janeiro de 2024. Disponível aqui: https://www.fatf-gafi.org/en/countries/fatf.html

As jurisdições criam leis AML/CFT com três objectivos principais: reduzir a criminalidade geral, proteger os direitos violados pelos crimes e proteger a integridade do sistema financeiro. A definição legal exata de branqueamento de capitais varia entre as jurisdições, o que dificulta uma uniformização legal.

O Banco de Compensações Internacionais – *Bank for International Settlements* (BIS[58]), juntamente com FATF, são entidades que desempenham papéis fundamentais na padronização de modelos de regulamentação de AML/CFT. O FATF estabelece padrões de prevenção e avalia o progresso dos países membros, enquanto o BIS integra as recomendações do FATF em seu quadro geral de supervisão bancária.[59]

As medidas de AML/CFT e a supervisão relacionada nos bancos devem seguir uma abordagem baseada em risco, no sentido de diferenciar as classes pelo nível de risco e separá-las sua gestão. Mais, é essencial que as informações sejam geridas adequadamente pelas instituições bancárias para que seja possível garantir um rastreamento das informações para fins de auditoria, estimular uma correta comunicação de supervisão e, quando necessário, apoiar processos criminais

Percebe-se, portanto, que a regulamentação dos *cryptoassets* na União Europeia é um desafio contínuo, exigindo uma abordagem regulatória bem pensada e coordenada, tanto a nível nacional como internacional, a fim de que possa efetivamente regular os *cryptoassets*, proteger os consumidores e prevenir atividades ilícitas, sem prejuízo da inovação e da integração dos *cryptoassets* no sistema financeiro *mainstream*.

2.4. Formas eficazes de combate ao branqueamento de capitais e financiamento ao terrorismo através da legislação AML/CFT

Combater o branqueamento de capitais e o financiamento ao terrorismo é uma preocupação central das políticas AML/CFT. É possível obter êxito nessa luta, desde que as autoridades competentes trabalhem em prol deste fim, desde a elaboração de

[58] Bank for International Settlements - BIS, *History – overview*. "Established in 1930, the Bank for International Settlements is the oldest international financial institution. From its inception to the present day, the BIS has played a number of key roles in the global economy, from settling reparation payments imposed on Germany following the First World War, to serving central banks in their pursuit of monetary and financial stability." Consultado em 26 de janeiro de 2024. Disponível aqui: https://www.bis.org/about/history.htm?m=11

[59] Bank for International Settlements – BIS, *AML and CFT in banking – Executive Summary*, 2020, pp. 2-3. Consultado em 26 de janeiro de 2024. Disponível aqui: https://www.bis.org/fsi/fsisummaries/aml_cft_banking.pdf

normas eficazes até ao respetivo cumprimento, passando pelos meios adequados para que este propósito seja alcançado.

2.4.1. Meios tecnológicos

É necessário que seja exigida a identificação e verificação dos clientes por parte das instituições financeiras, bem como o monitoramento contínuo de transações suspeitas. As transações suspeitas devem ser relatadas às autoridades competentes e, para além disso; é necessário obter a cooperação internacional, no intuito de haver troca de informações financeiras entre países para rastrear e impedir fluxos financeiros ilícitos; essas medidas precisam estar aliadas à implementação de tecnologia avançada para deteção e análise de padrões de transações suspeitas.

O legislador tem em consideração essa necessidade de aliar a tecnologia no enfrentamentod essas atividades ilícitas, uma vez que destaca, no considerando 1 do MiCA[60] que "é importante assegurar que os atos legislativos da União em matéria de serviços financeiros sejam consentâneos com a era digital e contribuam para uma economia preparada para o futuro que esteja ao serviço dos cidadãos, nomeadamente permitindo a utilização de tecnologias inovadoras. A União tem um interesse estratégico no desenvolvimento e no incentivo à adoção de tecnologias transformadoras no sector financeiro, nomeadamente a adoção de tecnologia de registo distribuído (DLT, do inglês distributed ledger technology). Prevê-se que, no futuro, muitas das aplicações da tecnologia de registo distribuído que ainda não foram estudadas de forma exaustiva continuarão a resultar em novos tipos de atividades e modelos empresariais, que, em conjunto com o próprio sector dos criptoativos, conduzirão ao crescimento económico e criarão novas oportunidades de emprego para os cidadãos da União."

Para fins de legislação AML/CFT, é preciso considerar técnicas com soluções tecnológicas para conseguir acompanhar a inovação dos *cryptoassets*. Os métodos de anonimização e pseudonimização, por exemplo, podem trazer benefícios para aliar o AML/CFT em equilíbrio com a proteção de dados.

Por meio da anonimização, as informações pessoais são transformadas de forma que não possam ser atribuídas a um indivíduo específico, mantendo a utilidade para fins

[60] Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo aos mercados de criptoativos e que altera a Diretiva (UE) 2019/1937, MiCA, Consultado em 13 de fevereiro de 2024. Disponível aqui: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0006.02/DOC_1&format=PDF

de AML/CFT. Os dados pessoais são transformados ou embaralhados de tal forma que se tornam impossíveis de serem vinculados a um indivíduo específico. Por exemplo, em vez de armazenar nomes completos, os dados podem ser convertidos em códigos ou IDs únicos, removendo qualquer informação identificável. Dessa forma, as instituições podem continuar a realizar análises de risco e detecção de atividades suspeitas sem expor dados pessoais.

A pseudonimização, por outro lado, trata-se de substituir os identificadores pessoais por códigos ou pseudónimos, de tal modo que, em vez de remover completamente os dados de identificação, há uma substituição por pseudónimos ou códigos, não sendo possível a reversão facilmente revertidos para os dados originais sem a pseudonimização. Tal técnica permite que as obrigações de relatórios e análises de AML/CFT sejam cumpridas pelas instituições, e também os titulares dos dados têm os seus dados protegidos. Isso ajuda a alcançar um equilíbrio entre proteção de dados e conformidade regulatória.

Importa salientar que a implementação eficaz dessas técnicas de anonimização e de pseudonimização requer tecnologia avançada, nomeadamente o uso de algoritmos de *hash*[61], técnicas de criptografia, e sistemas de gerenciamento de identidades para que os dados permaneçam seguros e anónimos ou pseudónimos. Também é igualmente importante desenvolver políticas rigorosas de segurança de dados e treinar equipas para garantir que a tecnologia seja usada corretamente.

2.4.2. Meio Regulatório (MiCA)

No âmbito da União Européia, a uniformização da legislação dos estados membros no tocante à AML/CFT, em matéria de *cryptoassets*, é essencial para que exista um real enfrentamento às atividade ilícitas. O MiCA ratifica esse ideal, uma vez que, em seu considerando 5[62], reconhece que "A ausência de um regime geral da União Europeia aplicável aos mercados de criptoativos pode levar a uma falta de confiança dos

[61] O mesmo utilizado na tecnologia *blockchain*. Ponto 2.1.2.
[62] Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo aos mercados de criptoativos e que altera a Diretiva (UE) 2019/1937, MiCA, Consultado em 13 de fevereiro de 2024. Disponível aqui: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0006.02/DOC_1&format=PDF

utilizadores nesses ativos, que poderia prejudicar consideravelmente o desenvolvimento do respetivo mercado, e a uma perda de oportunidades em termos de serviços digitais inovadores, de instrumentos de pagamento alternativos ou de novas fontes de financiamento para as empresas da União. Além disso, as empresas que utilizassem criptoativos não teriam qualquer segurança jurídica quanto ao tratamento que seria dado aos seus criptoativos nos diferentes Estados-Membros, o que minaria os seus esforços no sentido de uma utilização desse tipo de instrumentos no quadro da inovação digital. A inexistência de um regime geral da União aplicável aos mercados de criptoativos poderia ainda conduzir à fragmentação regulamentar, o que provocaria distorções da concorrência no mercado interno, dificultaria a expansão transfronteiras das atividades dos prestadores de serviços de criptoativos e resultaria em arbitragem regulamentar. Os mercados de criptoativos possuem, por enquanto, uma dimensão modesta, não representando, de momento, uma ameaça à estabilidade financeira. No entanto, é possível que tipos de criptoativos que procuram estabilizar o seu preço em relação a um determinado ativo ou cabaz de ativos, possam, no futuro, merecer a aceitação generalizada dos detentores não profissionais. Uma tal evolução poderia colocar novos desafios em termos da estabilidade financeira, do bom funcionamento dos sistemas de pagamento, da transmissão da política monetária ou da soberania monetária."

A proposta do MiCA (Regulamento dos Mercados de Criptoativos) no combate ao branqueamento de capitais e ao financiamento do terrorismo visa aumentar a transparência e a responsabilidade dos participantes do mercado de criptoativos, uma vez que possui diretrizes regulatórias e de supervisão que abrangem criptoativos, prestadores de serviços de criptoativos e emissões de criptoativos, com foco na proteção dos consumidores, na integridade do mercado, e na prevenção de riscos financeiros.

A transparência promovida pelo MiCA pretende criar um ambiente de mercado mais seguro e confiável, reduzindo a assimetria de informação e protegendo contra práticas fraudulentas e abusivas no mercado de criptoativos. É exigindo que os emissores de criptoativos e os prestadores de serviços de criptoativos divulguem informações claras e compreensíveis sobre os riscos, direitos e obrigações, dentre outras dinformações, associados aos seus produtos e serviços[63].

[63] Art.º 6.º, MiCA

As obrigações de diligência devida[64] também são impostas aos prestadores de serviços de criptoativos, na obrigação de realizar verificações de diligência devida sobre seus clientes para identificar e mitigar os riscos de branqueamento de capitais e financiamento do terrorismo.

O MiCA estabelece um sistema de licenciamento e supervisão para prestadores de serviços de criptoativos em toda a UE, promovendo a cooperação entre as autoridades nacionais competentes, que está descrito nos artigos 59.º e seguintes. Percebe-se que a transparência e a cooperação entre os Estados (membros e terceiros) são medidas imprescindíveis para um efetivo combate ao branqueamento de capitais e financiamento ao terrorismo.

[64] Art.º 76.º, MiCA

3. Proteção de Dados à luz do combate ao branqueamento de capitais e financiamento ao terrorismo

A proteção de dados tornou-se uma questão de importância fundamental à medida em que há um avanço tecnológico, culminando na adoção de leis específicas para garantir a segurança e a privacidade dos dados pessoais. A UE é um exemplo proeminente dessa tendência, com o RGPD representando um marco legal significativo.

O RGPD, em vigor desde maio de 2018, estabelece um conjunto uniforme de regras para a proteção de dados em todos os Estados-Membros da UE. Ele aplica-se às organizações baseadas na UE e àquelas fora da UE que processam dados de indivíduos residentes na UE[65]. Além do RGPD, existem outras leis e diretivas na UE, como a Diretiva sobre a Proteção de Dados na Aplicação da Lei, que regula o processamento de dados pessoais pelas autoridades de aplicação da lei.

Os princípios fundamentais relativos ao tratamento de dados pessoais orientam o processamento de dados no RGPD. Estes incluem a licitude, lealdade, transparência; limitação de finalidade; minimização de dados; exatidão; limitação da conservação; integridade e confidencialidade; e responsabilidade. Estes princípios garantem que os dados são processados de forma legal e justa, para propósitos específicos, e mantidos apenas pelo tempo necessário.

O RGPD fortalece os direitos dos indivíduos em relação aos seus dados pessoais. Estes direitos incluem o direito à autodeterminação informacional, direito de acesso, direito de retificação, direito ao apagamento, direito à limitação do tratamento, direito à portabilidade dos dados, direito de Oposição.

Esses direitos e princípios são vitais para garantir a proteção e o controlo dos dados pessoais em um mundo cada vez mais digital e interconectado.

[65] Art.º 3.º, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE), RGPD, Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679

3.1. Legislação na União Europeia

Em 1995 entrou em vigor a Diretiva de Proteção de dados (Diretiva 95/46/CE), que foi a primeira grande legislação de proteção de dados na UE. O objetivo da Diretiva era harmonizar a proteção de dados pessoais em todos os Estados-Membros da UE, incluindo princípios fundamentais de proteção de dados, como consentimento, finalidade limitada, e direitos dos titulares dos dados.

A Diretiva *e-Privacy* de 2002 (Diretiva 2002/58/CE) foi elaborada com o foco especificamente voltado para a privacidade nas comunicações eletrónicas. Regulamentou questões como cookies, comunicações comerciais por e-mail e confidencialidade das comunicações.

O RGPD foi proposto em 2012, após um longo período de discussões e negociações, foi aprovada em 2016, entrando em vigor em maio de 2018 e representa um marco fundamental na regulamentação global de proteção de dados. A regulamentação teve como objetivo principal garantir a uniformidade das leis de proteção de dados em toda a União Europeia, tendo aplicabilidade em todas as empresas que processam dados de residentes da UE, independentemente da localização em que a empresa está estabelecida. Os direitos dos titulares dos dados foram reforçados e ampliados (como o direito ao esquecimento e à portabilidade de dados), regras mais rígidas para o consentimento foram determinadas, bem como multas significativas para violações de dados foram instituídas.

Um dos aspectos mais notáveis do RGPD é o seu alcance global. Embora seja uma legislação europeia, como referido, ela se aplica a todas as organizações que processam dados pessoais de cidadãos da União Europeia, independentemente de onde a organização esteja localizada. Isso significa que empresas de todo o mundo que fazem negócios com residentes na UE devem cumprir as regulamentações do RGPD.

A Lei n.º 58/2019, aprovada em agosto de 2019, transpôs o RGPD para o direito português, estabelecendo regras detalhadas para o processamento de dados pessoais e reforçando os direitos dos titulares dos dados. Para além de expandir os direitos dos titulares dos dados, como o direito ao esquecimento e à portabilidade de dados, reforçou princípios como consentimento, transparência, limitação de finalidade e segurança dos dados.

Importa mencionar que o artigo 35.º[66] da Constituição da República Portuguesa trata do tema "Utilização da informática", ao abordar os dados pessoais, os direitos de acesso, retificação, atualização e finalidade a que se destinam, bem como o tratamento e o acesso às redes informáticas de uso público.

A proteção de dados não é um conceito novo, mas tem ganhado destaque nas últimas décadas devido à explosão da tecnologia digital e à coleta massiva de informações pessoais. Antes do RGPD, a legislação de proteção de dados na União Europeia estava fragmentada e variava consideravelmente entre os Estados-Membros. A necessidade de uma abordagem unificada e atualizada tornou-se evidente à medida que os desafios de proteção de dados se tornaram cada vez mais complexos.

Além do RGPD, a Diretiva (UE) 2016/680, conhecida como a Diretiva sobre a Proteção de Dados na Aplicação da Lei, também desempenha um papel importante. Esta diretiva, que entrou em vigor em 5 de maio de 2016, foca na proteção de dados pessoais processados para fins de prevenção, investigação, deteção ou repressão de infrações penais. Ela assegura a proteção dos dados pessoais das vítimas, testemunhas e suspeitos de crimes, facilitando a cooperação transnacional na luta contra a criminalidade e o terrorismo.

Para garantir a aplicação coerente das regras de proteção de dados em toda a União Europeia, foi criado o Comité Europeu para a Proteção de Dados (CEPD). Este órgão é composto por representantes das autoridades nacionais de proteção de dados dos países da UE e da Autoridade Europeia para a Proteção de Dados (AEPD), e tem a

[66] RGPD, Artigo 35.º: Utilização da informática
1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.
5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

função de emitir orientações sobre o RGPD e aconselhar a Comissão Europeia sobre questões relacionadas à proteção de dados pessoais.

O regulamento (UE) 2018/1725, por sua vez, estabelece regras para o tratamento de dados pessoais pelas instituições e órgãos da União Europeia, alinhando-se ao RGPD e à Diretiva sobre a Proteção de Dados na Aplicação da Lei.

3.2. Princípios fundamentais

O RGPD é baseado em uma série de princípios fundamentais que orientam o tratamento de dados pessoais. Estes princípios formam a base da regulamentação e são essenciais para a compreensão de como o RGPD funciona na prática, e, em um mundo cada vez mais digital, esses princípios se tornam igualmente relevantes no contexto dos *cryptoassets*.

Os dados pessoais na era digital são protegidos por um conjunto de princípios sólidos estabelecidos no RGPD. É de suma importância que as empresas que operam com *cryptoassets* compreendam e cumpram esses princípios. Dessa forma, a proteção dos direitos dos indivíduos está assegurada e a economia digital desenvolve-se de uma forma mais sustentável.

No contexto dos *cryptoassets*, a aplicação do RGPD é desafiadora, uma vez que eles operam em um ambiente descentralizado e muitas vezes anónimo. No entanto, os princípios da proteção de dados continuam sendo relevantes para nortear as relações.

3.2.1. Princípio da Licitude

Esse princípio deve ser compreendido de duas maneiras: em sentido estrito e em sentido amplo. A Barreto Menezes Cordeiro [67]faz essa distinção e explica que "na primeira aceção respeita ao tratamento dos dados e na segunda ao cumprimento da Lei". De acordo com o princípio da licitude, o tratamento dos dados em concreto deve estar enquadrado em uma das causas previstas no art.º 6.º do RGPD[68].

[67] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de dados à luz do RGPD e da Lei n.º 58/2019*, Reimpressão, Almedina, Coimbra, 2020, p. 152.
[68] RGPD, Art.º 6.º: 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

3.2.2. Princípio da lealdade

Trata-se de um conceito aberto, de modo que se torna possível ser invocado em casos de situações contrárias ao espírito do RGPD. Está fundamentado no art.º 5.º, a) do RGPD[69], sem prejuízo de considerar outros dispositivos[70] do RGPD que versem sobre "tratamento equitativo" para corroborar tal princípio.

Importa salientar que não se pode atribuir aos considerandos o valor de lei, todavia o texto contido tem o propósito de "clarificar o sentido de uma norma ou de explicitar as suas fundamentações, mas em caso algum poderão ser invocados para sustentar uma interpretação que nao encontre correspondência na letra da lei"[71].

3.2.3. Princípio da transparência

A transparência deve sempre estar presente em todo o processo de tratamento de dados, que tem início na recolha e conserva-se até mesmo após o termo da relação (conforme situação disposta no art.º 17, 2, RGPD[72]).

O direito de acesso do titular dos dados às informações relativas ao tratamento dos dados, art.º 15.º do RGPD[73], é uma manifestação do princípio da transparência em concreto.

---

a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

[69] RGPD, Art.º 5.º: 1. Os dados pessoais são:
a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»)

[70] RGPD, Considerandos 60 e 71; art.º 13.º, 2; art.º 14.º, 2; art.º 40, 2, a).

[71] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de dados à luz do RGPD e da Lei n.º 58/2019*, Reimpressão, Almedina, Coimbra, 2020, p. 264.

[72] "Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos."

Qualquer entidade que colete e processe dados pessoais em transações de *cryptoassets* deve fornecer informações claras e concisas aos indivíduos sobre o tratamento dos seus dados, sendo particularmente relevante em *exchanges* de criptomoedas que exigem verificação de identidade.

3.2.4. Limitação das Finalidades

As expressões utilizadas para adjetivar a finalidade da recolha dos dados no art.º 5.º, 1, b) do RGPD[74] são "determinadas, explícitas e legítimas", de tal modo que o tratamento dos dados também devem respeitar a esse princípio.

Relativamente à recolha e tratamento dos dados por parte de instituições financeiras no contexto das criptomoedas, deve-se observar se a finalidade está bem determinada, para além de ser explícita e legítima.

---

[73] 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:
a) As finalidades do tratamento dos dados;
b) As categorias dos dados pessoais em questão;
c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;
d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;
e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;
f) O direito de apresentar reclamação a uma autoridade de controlo;
g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;
h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.
2. Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 46.o relativo à transferência de dados.
3. O responsável pelo tratamento fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente.
4. O direito de obter uma cópia a que se refere o n.o 3 não prejudica os direitos e as liberdades de terceiros.

[74] 1. Os dados pessoais são:
b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («limitação das finalidades»);

Evitar e/ou combater os crimes de branqueamento e financiamento ao terrorismo trata-se de uma finalidade legítima e determinada para a recolha e o tratamento dos dados. Contudo, é necessário que essa finalidade seja explícita, ou seja, deve ser comunicada ao titular dos dados.

Há uma correlação deste princípio com o princípio da minimização dos dados (na sequência), uma vez que a limitação da finalidade acaba por limitar os dados pessoais que são passíveis de recolha e tratamento.

O artigo 41.º, 2 da 5AMLD está em consonância com este princípio consagrado no RGPD, uma vez que determina que "Os dados pessoais são tratados pelas entidades obrigadas com base na presente diretiva apenas para efeitos da prevenção do branqueamento de capitais e do financiamento do terrorismo conforme referido no artigo 1.º e não podem ser posteriormente tratados de forma incompatível com essas finalidades. É proibido o tratamento posterior de dados pessoais com base na presente diretiva para quaisquer outros fins como os fins comerciais."

3.2.5. Princípio da Minimização de Dados

O artigo 5.ª, 1, c) do RGPD determina que os dados pessoais são "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados". As organizações devem coletar apenas os dados pessoais necessários para a finalidade pretendida, de modo que o citado dispositivo do RGPD limita os dados e também a finalidade da recolha e do tratamento.

A coleta de informações excessivas e irrelevantes devem ser evitadas, o que ajuda a reduzir o risco de exposição indevida e a proteger a privacidade dos titulares dos dados.

O mesmo deve ser aplicado no contexto das criptomoedas, ou seja, apenas devem ser coletados e partilhados os dados necessários para realizar uma transação ou cumprir uma obrigação legal. Isso implica que não se deve coletar dados além do estritamente necessário.

3.2.6. Princípio da Exatidão

De acordo com o Prof. Dr. A. Barreto Menezes Cordeiro[75], há três dimensões abrangidas neste princípio, disposto na alínea d) do artigo 5.º/1: (i) proibição de recolher ou armazenar dados incorretos; (ii) o dever de atualização dos dados recolhidos e (iii) o dever de apagar ou corrigir os dados.

O comando de proibir a recolha e armazenamento dos dados incorretos tem a finalidade de zelar pela veracidade dos dados em causa. O dever de atualização dos dados recolhidos não deve ser encarado de forma absoluta, visto que, por vezes, faz-se necessário manter o histórico dos dados no contexto financeiro. Relativamente ao dever de apagar ou retificar os dados incorretos, observa-se que "apagar" ou "retificar" não devem estar circunscritos na esfera dos "dados incorretos", uma vez que o direito ao apagamento dos dados – direito a ser esquecido está garantido no artigo 17.º, RGPD[76], sob os motivos expostos no número 1.

Os direitos dos titulares de dados são objeto de estudo na sequência desta dissertação e será analisada a possibilidade ou relativização desses direitos no contexto das criptomoedas.

3.2.7. Princípio da Limitação da Conservação

Os dados pessoais devem ser retidos apenas pelo tempo necessário para cumprir a finalidade para a qual foram coletados, em conformidade com o artigo 5.º, 1, e), RGPD[77]. Após esse período, os dados devem ser apagados ou anonimizados. Esse

---

[75] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de dados à luz do RGPD e da Lei n.º 58/2019*, Reimpressão, Almedina, Coimbra, 2020, p. 159.

[76] Art.º 17.º: 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:
a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
c) O titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.o, n.o 2;
d) Os dados pessoais foram tratados ilicitamente;
e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.

[77] Art.º 5.º: 1. Os dados pessoais são:
e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser

princípio protege a privacidade dos indivíduos, evitando o armazenamento excessivo de informações pessoais.

Esse princípio foi amplamente discutido no âmbito do caso Google Spain, conhecido formalmente como Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González (Caso C-131/12), em conjunto com o direito ao apagamento, que será exposto na sequência desta dissertação.

Em se tratando de dados financeiros e o bem jurídico a ser protegido no combate ao branqueamento e ao financiamento ao terrorismo, é necessário ponderar a aplicação deste princípio.

3.2.8. Princípio da Integridade e Confidencialidade

Esse princípio pressupõe que as organizações são responsáveis por garantir a segurança dos dados pessoais que coletam e processam, com a implementação de medidas de segurança apropriadas para proteger os dados contra "o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas" (artigo 5.º, 1, f), RGPD).

Percebe-se que esse princípio tem alta relevância para a proteção dos dados pessoais no contexto das criptomoedas, uma vez que os dados em causa trazem informações passíveis de enquadrá-las em investigações de crimes de branqueamento e financiamento ao terrorismo.

3.2.9. Princípio da Responsabilidade

Há dois deveres distintos previstos neste princípio: (i) o responsável pelo tratamento dos dados tem o dever de atuar no estrito cumprimento dos princípios constantes no artigo 5.º/1; (ii) o cumprimento desses princípios deve ser comprovado pelo responsável pelo tratamento dos dados às autoridades de controlo e aos tribunais.

---

conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);

Este princípio coloca a responsabilidade diretamente nas organizações que coletam e processam dados pessoais, devendo demonstrar conformidade com o RGPD e ser capazes de prestar contas por suas ações.

O RGPD[78] traz possibilidades de como o responsável pelo tratamento dos dados pode comprovar a observância do princípio da responsabilidade nos artigos 40.º e 42.º, através de códigos de conduta e certificação.

[78] Artigo 40.º: Códigos de conduta
1. Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem a elaboração de códigos de conduta destinados a contribuir para a correta aplicação do presente regulamento, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas.
2. As associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes podem elaborar códigos de conduta, alterar ou aditar a esses códigos, a fim de especificar a aplicação do presente regulamento, como por exemplo:
a) O tratamento equitativo e transparente;
b) Os legítimos interesses dos responsáveis pelo tratamento em contextos específicos;
c) A recolha de dados pessoais;
d) A pseudonimização dos dados pessoais;
e) A informação prestada ao público e aos titulares dos dados;
f) O exercício dos direitos dos titulares dos dados;
g) As informações prestadas às crianças e a sua proteção, e o modo pelo qual o consentimento do titular das responsabilidades parentais da criança deve ser obtido;
h) As medidas e procedimentos a que se referem os artigos 24.o e 25.o e as medidas destinadas a garantir a segurança do tratamento referidas no artigo 30.o;
i) A notificação de violações de dados pessoais às autoridades de controlo e a comunicação dessas violações de dados pessoais aos titulares dos dados;
j) A transferência de dados pessoais para países terceiros ou organizações internacionais; ou
k) As ações extrajudiciais e outros procedimentos de resolução de litígios entre os responsáveis pelo tratamento e os titulares dos dados em relação ao tratamento, sem prejuízo dos direitos dos titulares dos dados nos termos dos artigos 77.o e 79.o.
3. Além dos responsáveis pelo tratamento ou dos subcontratantes sujeitos ao presente regulamento, também os responsáveis pelo tratamento ou subcontratantes que não estão sujeitos ao presente regulamento por força do artigo 3.o podem cumprir códigos de conduta aprovados em conformidade com o n.o 5 do presente artigo e de aplicabilidade geral por força do n.o 9 do presente artigo, de modo a fornecer garantias apropriadas no quadro das transferências dos dados pessoais para países terceiros ou organizações internacionais nos termos referidos no artigo 46.o, n.o 2, alínea e). Os responsáveis pelo tratamento ou os subcontratantes assumem compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias apropriadas, inclusivamente em relação aos direitos dos titulares dos dados.
4. Os códigos de conduta referidos no n.o 2 do presente artigo devem prever procedimentos que permitam ao organismo referido no artigo 41.o, n.o 1, efetuar a supervisão obrigatória do cumprimento das suas disposições por parte dos responsáveis pelo tratamento ou subcontratantes que se comprometam a aplicá-lo, sem prejuízo das funções e competências das autoridades de controlo competentes por força do artigo 55.o ou 56.o.
5. As associações e outros organismos a que se refere o n.o 2 do presente artigo que tencionem elaborar um código de conduta, ou alterar ou aditar a um código existente, apresentam o projeto de código, a alteração ou o aditamento à autoridade de controlo que é competente por força do artigo 55.o. A autoridade de controlo emite um parecer sobre a conformidade do projeto de código de conduta ou da alteração ou do aditamento com o presente regulamento e aprova este projeto, esta alteração ou este aditamento se determinar que são previstas garantias apropriadas suficientes.
6. Se o código de conduta, ou a alteração ou o aditamento for aprovado nos termos do n.o 5, e se o código de conduta em causa não estiver relacionado com atividades de tratamento realizadas em vários Estados-Membros, a autoridade de controlo regista e publica o código.

Os princípios do RGPD estabelecem um alicerce para a proteção de dados pessoais. Para além de promoverem a transparência, a responsabilidade e a privacidade, garantindo que os dados pessoais sejam coletados e processados de maneira justa e

---

7. Se o projeto do código de conduta estiver relacionado com atividades de tratamento realizadas em vários Estados-Membros, a autoridade de controlo competente nos termos do artigo 55.o, antes da aprovação, apresenta o projeto do código, a alteração ou o aditamento, pelo procedimento referido no artigo 63.o, ao Comité, que emite um parecer sobre a conformidade do projeto de código de conduta, ou da alteração ou do aditamento, com o presente regulamento, ou, na situação referida no n.o 3 do presente artigo, sobre a previsão de garantias adequadas.
8. Se o parecer a que se refere o n.o 7 confirmar que o projeto do código de conduta, ou a alteração ou o aditamento, está conforme com o presente regulamento ou, na situação referida no n.o 3, prevê garantias adequadas, o Comité apresenta o seu parecer à Comissão.
9. A Comissão pode, através de atos de execução, decidir que os códigos de conduta aprovados, bem como as alterações ou os aditamentos, que lhe sejam apresentados nos termos do n.o 8 do presente artigo, são de aplicabilidade geral na União. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.o, n.o 2.
10. A Comissão assegura a publicidade adequada dos códigos aprovados que declarou, mediante decisão, serem de aplicabilidade geral em conformidade com o n.o 9.
11. O Comité recolhe todos os códigos de conduta aprovados, respetivas alterações e respetivos aditamentos num registo e disponibiliza-os ao público pelos meios adequados.
Artigo 42.º: Certificação
1. Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem, em especial ao nível da União, a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento. Serão tidas em conta as necessidades específicas das micro, pequenas e médias empresas.
2. Além do cumprimento pelos responsáveis pelo tratamento ou pelos subcontratantes sujeitos ao presente regulamento, os procedimentos de certificação em matéria de proteção de dados, bem como selos ou marcas aprovados de acordo com o n.o 5 do presente artigo também podem ser estabelecidos para efeitos de comprovação da existência de garantias adequadas fornecidas por responsáveis pelo tratamento ou por subcontratantes que não estão sujeitos ao presente regulamento por força do artigo 3.o no quadro das transferências de dados pessoais para países terceiros ou organizações internacionais nos termos referidos no artigo 46.o, n.o 2, alínea f). Os responsáveis pelo tratamento ou os subcontratantes assumem compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias adequadas, inclusivamente em relação aos direitos dos titulares dos dados.
3. A certificação é voluntária e está disponível através de um processo transparente.
4. A certificação prevista no presente artigo não diminui a responsabilidade dos responsáveis pelo tratamento e subcontratantes pelo cumprimento do presente regulamento nem prejudica as funções e competências das autoridades de controlo competentes por força do artigo 55.o ou 56.o.
5. A certificação prevista no presente artigo é emitida pelos organismos de certificação referidos no artigo 43.o ou pela autoridade de controlo competente, com base nos critérios por esta aprovados por força do artigo 58.o, n.o 3, ou pelo Comité por força do artigo 63.o. Caso os critérios sejam aprovados pelo Comité, podem ter como resultado uma certificação comum, o Selo Europeu de Proteção de Dados.
6. Os responsáveis pelo tratamento ou subcontratantes que submetem o seu tratamento ao procedimento de certificação fornecem ao organismo de certificação a que se refere o artigo 43.o, ou, consoante o caso, à autoridade de controlo competente, todo o acesso às suas atividades de tratamento e toda a informação de que haja necessidade para efetuar o procedimento de certificação.
7. A certificação é emitida aos responsáveis pelo tratamento e subcontratantes por um período máximo de três anos e pode ser renovada nas mesmas condições, desde que os requisitos aplicáveis continuem a estar reunidos. A certificação é retirada, consoante o caso, pelos organismos de certificação referidos no artigo 43.o ou pela autoridade de controlo competente, se os requisitos para a certificação não estiverem ou tiverem deixados de estar reunidos.
8. O Comité recolhe todos os procedimentos de certificação e todos os selos e marcas de proteção de dados aprovados num registo e disponibiliza-os ao público por todos os meios adequados.

segura, atribuem deveres ao responsável pelo tratamento dos dados para assegurar o cumprimento dos princípios.

No mundo digital em constante evolução, esses princípios desempenham um papel vital na proteção da privacidade dos indivíduos e na promoção da confiança no tratamento de dados pessoais, visto que os direitos definidos no RGPD para os titulares dos dados encontram fundamento nos princípios analisados.

O RGPD teve um impacto significativo em todo o mundo. Muitos países fora da União Europeia revisaram suas próprias leis de proteção de dados para se alinhar com os princípios do RGPD, que funcionam como um norte nas relações que envolvem recolha e tratamento de dados pessoais. Assim, empresas de todos os setores que coletam dados pessoais de cidadãos europeus tiveram que se adaptar às regulamentações, implementando mudanças significativas em suas práticas de coleta, armazenamento e processamento de dados.

Para além de representar um modelo importante para outras jurisdições considerarem ao desenvolver suas próprias regulamentações de proteção de dados, o RGPD também é responsável por impactar positivamente a cultura organizacional. A importância da privacidade e da segurança de dados em todas as etapas do ciclo de vida dos dados, desde a coleta até a exclusão está reforçada e fundamentada nos princípios. No geral, as organizações estão cada vez mais conscientes de sua responsabilidade em relação aos dados pessoais e investem em treinamento e conscientização para seus funcionários, através de códigos de conduta e certificações, em consonância com os artigos 40.º e 42.º do RGPD. As organizações que operam com cryptoassets são responsáveis por cumprir o RGPD e também devem estar preparadas para demonstrar sua conformidade.

Os princípios estabelecidos pelo RGPD são claros e rigorosos, e afetam não apenas as empresas na UE, mas também aquelas em todo o mundo que lidam com dados de cidadãos da UE. O RGPD não apenas promove a proteção de dados, mas também encoraja a transparência, a responsabilidade e a ética no tratamento das informações pessoais, criando um padrão global para a privacidade e a segurança dos dados.

3.3. Direitos dos Titulares dos Dados

O titular dos dados, de acordo com o RGPD[79] em seu art.º 3.º, é todo indivíduo cujos dados são objeto de tratamento por um esdtabelecimento de um responsável ou subcontratante situado em território da União Europeia, bem como todos os residentes no território da União Europeia, cujos dados pessoais sejam objeto de tratamento.

Os direitos dos titulares de dados, conforme estabelecidos pelo Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, são fundamentais para a proteção da privacidade e a gestão de informações pessoais. Cada direito é respaldado por artigos específicos do RGPD, e estão em conformidade com os princípios estudados.

3.3.1. Direito à autodeterminação informacional

Para além da privacidade, esse direito traz uma conotação mais profunda de proteção, no sentido de garantir ao titular dos dados a capacidade de controlar a recolha, o uso e a disseminação de suas informações pessoais. O direito à autodeterminação informacional dá "a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em 'simples objeto de informação'"[80]

Os demais direitos concedidos aos titulares dos dados, bem como os deveres impostos aos responsáveis pelo tratamento dos dados, ambos positivados no RGPD, corroboram e reforçam a autodeterminação informativa (direito de acesso, direito de retificação, direito ao esquecimento, limitação do processamento, portabilidade de dados e oposição ao processamento). Pode-se dizer que o direito à autodeterminação informacional trata-se de um direito basilar para os demais.

Os titulares dos dados devem ser expressamente informados sobre o modo como os seus dados pessoais serão utilizados e, caso assim o entendam, devem consentir de

[79] Artigo 3.º: Âmbito de aplicação territorial
1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.
2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:
a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;
b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.
3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.

[80] CANOTILHO, Gomes, MOREIRA, Vital, *Constituição da República Portuguesa - Anotada - Volume I - Artigos 1º a 107º*, 4.ª Edição, Coimbra Editora, Coimbra, 2007, p. 150

forma explícita e livre. Trata-se do consentimento informado, amplamente expresso no RGPD. Importa mencionar que o artigo 6.º[81] condiciona a licitude do tratamento dos dados ao consentimento dado pelo titular dos dados.

[81] Artigo 6.º
Licitude do tratamento
1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.
O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.
2. Os Estados-Membros podem manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras do presente regulamento no que diz respeito ao tratamento de dados para o cumprimento do n.o 1, alíneas c) e e), determinando, de forma mais precisa, requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude e lealdade do tratamento, inclusive para outras situações específicas de tratamento em conformidade com o capítulo IX.
3. O fundamento jurídico para o tratamento referido no n.o 1, alíneas c) e e), é definido:
a) Pelo direito da União; ou
b) Pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito.
A finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no n.o 1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Esse fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido.
4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:
a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.o, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.o;
d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;
e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

Relativamente a dados pessoais no segmento financeiro, mais especificamente no contexto das criptomoedas e o combate aos crimes de branqueamento e ficanciamento ao terrorismo, o titular dos dados deve ser informado expressamente sobre a forma como os dados serão utilizados, e o consentimento para tal também deve ser expresso. Procedimentos de "Conheça o Seu Cliente" (do inglês: *Know Your Costumer* - KYC), a fim de monitorizar as transações financeiras, são passíveis de conflitos com o direito a autodeterminação informativa, uma vez que o titular dos dados abstem-se do controlo sobre a utilização dos dados recolhidos.

Tendo em conta a proteção do bem jurídico no combate aos crimes de branqueamento e ficanciamento ao terrorismo, pode-se afirmar que os dados coletados em sede de procedimento KYC mitigam o direito a autodeterminação informativa do titular dos dados.

Por outro lado, com a maior sofisticação da tecnologia de *blockchain*, algumas criptomoedas têm mais grau de privacidade sobre as informações das transações financeiras, o que limita a atuação AML/CFT, porém privilegia o direito à autodeterminação informativa. Exige um equilíbrio cuidadoso entre proteger a privacidade dos usuários e garantir a transparência necessária para prevenir atividades ilícitas.

3.3.2. Direito de Acesso

A base para assegurar o cumprimento dos demias direitos (retificação, apagamento, limitação do tratamento, portabilidade e oposição) é exatamente o direito ao acesso. É pelo acesso aos dados que são objeto de tratamento que o titular tem o condão de pleitear qualquer outro direito previsto no RGPD. O teor fundacional deste direito é também ratificado na Contituição da República Portuguesa, no artigo 35.º, 1.

O direito ao acesso, previsto no artigo 15.º do RGPD[82], confere duas etapas ao acesso do titular: a primeira passa pela confirmação do tratamento, ou seja, o titular dos

[82] Artigo 15.º
Direito de acesso do titular dos dados
1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:
a) As finalidades do tratamento dos dados;
b) As categorias dos dados pessoais em questão;

dados envia um pedido de informação ao responsável pelo tratamento dos dados a requerer a informação se os seus dados pessoais (e quais deles) estão a ser objeto de tratamento ou não. A segunda etapa inicia quando, em caso de resposta afirmativa, o titular dos dados solicita o acesso os seus dados pessoais, bem como às informações contidas nas alíneas do n.º 1 do artigo 15.º

A transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados é assegurada no artigo 12.º do RGPD[83]. Todavia, o

---

c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;
d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;
e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;
f) O direito de apresentar reclamação a uma autoridade de controlo;
g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;
h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.
2. Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 46.º relativo à transferência de dados.
3. O responsável pelo tratamento fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente.
4. O direito de obter uma cópia a que se refere o n.º 3 não prejudica os direitos e as liberdades de terceiros.

[83] Artigo 12.º
Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados
1. O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.
2. O responsável pelo tratamento facilita o exercício dos direitos do titular dos dados nos termos dos artigos 15.º a 22.º. Nos casos a que se refere o artigo 11.o, n.o 2, o responsável pelo tratamento não pode recusar-se a dar seguimento ao pedido do titular no sentido de exercer os seus direitos ao abrigo dos artigos 15.º a 22.º, exceto se demonstrar que não está em condições de identificar o titular dos dados.
3. O responsável pelo tratamento fornece ao titular as informações sobre as medidas tomadas, mediante pedido apresentado nos termos dos artigos 15. º a 20. º, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. O responsável pelo tratamento informa o titular dos dados de alguma prorrogação e dos motivos da demora no prazo de um mês a contar da data de receção do pedido. Se o titular dos dados apresentar o pedido por meios eletrónicos, a informação é, sempre que possível, fornecida por meios eletrónicos, salvo pedido em contrário do titular.

mesmo dispositivo admite recusas de esclarecimentos em casos de pedidos que forem manifestamente infundados ou excessivos. Nessas situações, o responsável pelo tratamento dos dados tem o ônus da prova de demonstrar o caráter manifestamente ou excessivo do pedido.

Na prática, há um certo ceticismo relativamente a esse direito, especialmente no que concerne ao universo das criptomoedas. O caráter anónimo vai ao encontro da transparência inerente ao direito de acesso do titular dos dados o que cria um conflito na aplicação do direito de acesso. Há também outra dificuldade em relação às criptomoedas que utilizam a tecnologia *blockchain* e a identificação do responsável pelo tratamento de dados, visto que as redes de *blockchain* são descentralizadas e não têm uma entidade central que possa ser facilmente responsabilizada, o que complica o exercício do direito de acesso. Considerando que uma entidade tenha sido identificada como responsável pelo tratamento dos dados, ainda assim pode haver dificuldades técnicas significativas para atender aos pedidos de acesso aos dados, especialmente se as informações estiverem distribuídas em uma *blockchain*.

3.3.3. Direito de Retificação

4. Se o responsável pelo tratamento não der seguimento ao pedido apresentado pelo titular dos dados, informa-o sem demora e, o mais tardar, no prazo de um mês a contar da data de receção do pedido, das razões que o levaram a não tomar medidas e da possibilidade de apresentar reclamação a uma autoridade de controlo e intentar ação judicial.
5. As informações fornecidas nos termos dos artigos 13. º e 14. º e quaisquer comunicações e medidas tomadas nos termos dos artigos 15. º a 22. º e 34. º são fornecidas a título gratuito. Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, o responsável pelo tratamento pode:
a) Exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas; ou
b) Recusar-se a dar seguimento ao pedido.
Cabe ao responsável pelo tratamento demonstrar o caráter manifestamente infundado ou excessivo do pedido.
6. Sem prejuízo do artigo 11. º, quando o responsável pelo tratamento tiver dúvidas razoáveis quanto à identidade da pessoa singular que apresenta o pedido a que se referem os artigos 15.º a 21. º, pode solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados.
7. As informações a fornecer pelos titulares dos dados nos termos dos artigos 13. º e 14. º podem ser dadas em combinação com ícones normalizados a fim de dar, de uma forma facilmente visível, inteligível e claramente legível, uma perspetiva geral significativa do tratamento previsto. Se forem apresentados por via eletrónica, os ícones devem ser de leitura automática.
8. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 92. º, a fim de determinar quais as informações a fornecer por meio dos ícones e os procedimentos aplicáveis ao fornecimento de ícones normalizados.

O direito à retificação está consagrado no artigo 16.º do RGPD[84] e divide-se em dois direitos: a correção dos dados inexatos e que sejam completados os dados incompletos. O exercício do direito de retificação faz emergir o dever do responsável pelo tratamentos dos dados de retificar os dados incorretos e/ou completar os dados incompletos, que está traduzido no princípio da exatidão (art.º 5.º, 1, d)), analisado nesta dissertação.

3.3.4. Direito ao Apagamento ou "Direito ao Esquecimento"

O artigo 17.º do RGPD[85] consagra o direito ao apagamento dos dados, e inclui no título do artigo a expressão "direito a ser esquecido". De antemão, infere-se que o

[84] Artigo 16.º
Direito de retificação
O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.

[85] Artigo 17.º
Direito ao apagamento dos dados («direito a ser esquecido»)
1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:
a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
c) O titular opõe-se ao tratamento nos termos do artigo 21. , n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2;
d) Os dados pessoais foram tratados ilicitamente;
e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.
2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.o 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.
3. Os n.ºs 1 e 2 não se aplicam na medida em que o tratamento se revele necessário:
a) Ao exercício da liberdade de expressão e de informação;
b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;
c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.º, n.º 2, alíneas h) e i), bem como do artigo 9.º, n.º 3;
d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou

apagamento dos dados não será suficiente; é preciso que seja assegurado ao titular dos dados o direito ao esquecimento.

O princípio da minimização dos dados[86] e o princípio da limitação da conservação[87] encontram concretude neste direito, em que o legislador atribui ao titular de dados o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais sem demora injustificada, e o dever que o responsável pelo tratamento dos dados tem de, também sem demora injustificada, apagar os dados pessoais do titular.

O acórdão Google Spain, conhecido formalmente como Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González (Caso C-131/12), é um marco significativo na jurisprudência da União Europeia sobre proteção de dados. M. Costeja González apresentou, em 2010, reclamação na Agencia Española de Protección de Datos (AEPD) contra La Vanguardia Ediciones (jornal de grande tiragem na Espanha), Google Spain e Google Inc.

O objecto da reclamação era o facto de que, quando um internauta inseria o nome do autor no motor de busca do grupo Google, obtinha duas ligações para o referido jornal nas quais figurava um anúncio de uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social, que mencionava o nome de M. Costeja González[88].

O autor pedia que ordenasse à La Vanguardia que suprimisse ou alterasse as referidas páginas, para que os seus dados pessoais[89] deixassem de aparecer, ou que utilizasse determinadas ferramentas disponibilizadas pelos motores de busca para proteger esses dados. À Google, o autor reclamava que suprimissem ou ocultassem os seus dados pessoais, para que deixassem de aparecer nos resultados de pesquisa e de figurar nas ligações da La Vanguardia. M. Costeja González alegava a falta de pertinência da informação.

---

e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

[86] Ponto 2.3.2.5.

[87] Ponto 2.3.2.7.

[88] *Acordão do Tribunal de Justiça Europeu,* de 13 de maio de 2014, *processo C – 131/12*, p. 7

[89] Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Art. 2º. a) 'Dados pessoais', qualquer informação relativa a uma pessoa singular identificada ou identificável; é considerado identificável todo aquele que pode ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social;

A primeira decisão ocorreu no mesmo ano, quando a AEPD indeferiu no que dizia respeito à La Vanguardia, sob o fundamento de que tal publicação estava legalmente justificada; ao passo que deferiu o pedido em relação à Google Spain e à Google Inc, considerando que os motores de busca realizam tratamento de dados[90] pelo qual são responsáveis[91], atuando como intermediários da sociedade de informação e, por isso, estão sujeitos à legislação sobre a matéria.

A decisão foi no sentido de que os direitos fundamentais de M. González prevalecem sobre o interesse econômico do operador do motor de busca e também sobre o interesse deste público em ter acesso a informação numa pesquisa sobre os dados pessoais desta pessoa. O Tribunal de Justiça Europeu, portanto, em 2014, proferiu a decisão e o autor do referido processo conquistou o direito de ter os seus dados pessoais retirados de circulação e o futuro acesso as informações impossibilitadas.

Salienta-se que, aquando da decisão do acórdão em causa, a legislação sobre a matéria em vigor era a Diretiva 95/46/CE. Atualmente o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD) e que revoga a Diretiva 95/46/CE regula a matéria e já dispõe de normas mais específicas quanto ao direito ao apagamento dos dados (direito a ser esquecido), em seu art.º 17[92].

---

[90] Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Art. 2º. b) 'Tratamento de dados pessoais', qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;

[91] Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Art. 2º. d) 'Responsável pelo tratamento', a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinados por disposições legislativas ou regulamentares nacionais ou comunitárias, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser indicados pelo direito nacional ou comunitário;

[92] RGPD, 17.º Direito ao apagamento dos dados («direito a ser esquecido») 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e

O acórdão em questão faz prova de que a Diretiva 95/46/CE, bem como a Convenção do Conselho da Europa para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, em seu art.º 8º. Alínea C já trazia os subsídios necessários apara que o julgador decidisse pelo apagamento dos dados. O RGPD traz a novidade no tocante ao direito ao esquecimento, conforme o Professor António Crodeiro[93] quando menciona em sua obra intitulada Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 59/2019 que "A grande novidade trazida pelo RGPD não foi, consequentemente, a positivação do direito ao apagamento, mas a consagração legal do direito ao esquecimento, recorrendo à terminologia adotada".

O direito ao apagamento é uma concretização do princípio da minimização dos dados, positivado no art.º 5º., 1, c, RGPD[94], que, conforme o Professor António Cordeiro[95], "a adequação impõe a circunscrição dos tratamentos aos dados pessoais que se enquadrem nas finalidades prosseguidas. Os dados não relacionados ou inapropriados encontram-se, *ab initio*, excluídos".

O art.º. 17.º, 1, RGPD, já mencionado, trata de um direito do titular dos dados (de obter o apagamento dos seus dados pessoais, sem demora injustificada), e de uma

---

não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1. 2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos. 3. Os n.os 1 e 2 não se aplicam na medida em que o tratamento se revele necessário: a) Ao exercício da liberdade de expressão e de informação; b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.º, n.º 2, alíneas h) e i), bem como do artigo 9.º, n.º 3; d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

[93] CORDEIRO, A. Barreto Menezes. *Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019*. Almedina, Coimbra, 2020. p. 277.

[94] RGPD: Artigo 5.º Princípios relativos ao tratamento de dados pessoais 1. Os dados pessoais são: c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (minimização dos dados);

[95] CORDEIRO, A. Barreto Menezes. *Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019*. Almedina, Coimbra, 2020. p. 159.

obrigação do responsável pelo tratamento desses dados (de apagar os dados pessoais, sem demora injustificada), quando aplicáveis as razões dispostas nas respetivas alíneas.

As exceções ao direito descito no art.º 17.º estão estabelecidas no n.º 3, estando a alínea a) a dispor sobre a limitação do direito ao apagamento (esquecimento) face ao exercício da liberdade de expressão e de informação. Trata-se da mais relevante exceção, por ser um conflito de princípios muito intrincados, de difícil aferimento no caso concreto sobre qual lado teria mais peso. No acórdão em análise, o TJUE optou por preservar o direito ao apagamento em detrimento do direito à liberdade de expressão e de informação. O autor do processo não era uma pessoa com vida pública, informação que o TJUE pontuou ao final da decisão[96] que, caso fosse, teria que se ter em causa outro parâmetro decisório: "Na medida em que esta pode, tendo em conta os seus direitos fundamentais nos termos dos artigos 7.° e 8.° da Carta, requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão nessa lista de resultados, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em aceder à informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão."

O crescimento exponencial dos dados disponíveis para análises e outras finalidades duvidosas pode atentar contra direitos de personalidade, direitos tidos como fundamentais, sejam estes direitos à intimidade, à imagem, à honra, ou à vida privada. Deste modo, o direito ao esquecimento tem sido matéria de discussão em várias cortes no mundo.

O dieito ao pagamento dos dados / direito ao esquecimento sob a perspetiva de uma situação hipótetica no contexto das criptomoedas, mostra-se uma análse diferente ao acórdão mencionado neste ponto. Ter-se-ia, por exemplo, o titular dos dados – adquirente de criptomoedas, recorrente ao direito ao apagamento dos seus dados pessoais passados 2 anos do dia em que adquiriu-as, sob a alegação da alínea a) do n.º 1

[96] *Acordão do Tribunal de Justiça Europeu,* de 13 de maio de 2014, *processo C – 131/12*, p. 23

do art.º 17.º, de que "os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento".

Efetivamente, pode-se afirmar que o motivo da recolha dos dados ou tratamento (aquisição de criptomoedas) já tivera a finalidade alcançada aquando do momento da aquisição, o que poderia servir de fundamento para o apagamento dos dados.

Há, contudo, fatores que contrapõem ao direito alegado pelo titular dos dados, tais como (i) a necessidade de manutenção do histórico das informações contidas nos dados pessoais em casos de informações financeiras, o que excepciona o princípio da exatidão[97]; (ii) a alínea b) do n.º 3 do artigo 17.º, em que retira a apliação do direito ao esquecimento / apagamento quando haja o "cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento".

O artigo 40.º[98] da 5AMLD traz a obrigação legal às instituições financeiras de conservarem os dados pessoais dos clientes (os documentos e as informações obtidos

[97] Ponto 2.3.2.6.

[98] Artigo 40.º

1. Os Estados-Membros exigem que as entidades obrigadas conservem os seguintes documentos e informações nos termos do direito nacional para efeitos de prevenção, deteção e investigação, por parte da UIF ou de outras autoridades competentes, de possíveis atos de branqueamento de capitais ou financiamento do terrorismo:

a) No caso de diligência quanto à clientela, uma cópia dos documentos e das informações que sejam necessários para cumprir os requisitos de diligência quanto à clientela previstos no capítulo II, incluindo, sempre que disponíveis, informações obtidas através de meios de identificação eletrónica, serviços de confiança relevantes em conformidade com o Regulamento (UE) n.o 910/2014 ou qualquer outro processo de identificação eletrónica ou à distância seguro, regulamentado, reconhecido, aprovado ou aceite pelas autoridades nacionais relevantes, durante um período de cinco anos após o termo da relação de negócio com o respetivo cliente ou após a data de uma transação ocasional;

b) Os documentos comprovativos e os registos das transações efetuadas que consistam em documentos originais ou cópias admissíveis nos processos judiciais nos termos do direito nacional aplicável e que sejam necessários para identificar aquelas transações, durante um período de cinco anos após o termo da relação de negócio com o respetivo cliente ou após a data da transação ocasional.

Findo o período de conservação a que se refere o primeiro parágrafo, os Estados-Membros devem assegurar que as entidades obrigadas apagam os dados pessoais, salvo disposição em contrário do direito nacional, que determina as circunstâncias em que as entidades obrigadas podem ou devem conservar esses dados por mais tempo. Os Estados-Membros podem autorizar ou exigir a conservação por período adicional após terem efetuado uma avaliação exaustiva da necessidade e proporcionalidade de tal conservação por período adicional e considerarem que ela se justifica como sendo necessária para a prevenção, deteção ou investigação do branqueamento de capitais ou do financiamento do terrorismo. Esse período de conservação adicional não pode exceder cinco anos adicionais.

O período de conservação referido no presente número, incluindo o período de conservação adicional que não pode ser superior a cinco anos, aplica-se igualmente no que diz respeito aos dados acessíveis através dos mecanismos centralizados referidos no artigo 32.º-A.

através das medidas de diligência devida ao cliente, bem como os registros das transações) por um período de 5 anos após o término da relação. A 5AMLD traz, inclusive, uma adição a esse dispositivo no que concerne ao período de conservação dos dados, podendo ser prorrogado por mais 5 (cinco) anos, por motivos relacionados à necessidade de prevenir, detetar ou investigar casos de lavagem de dinheiro ou financiamento do terrorismo.

É importante destacar que qualquer prorrogação do período de retenção de dados deve ser justificada e proporcional ao objetivo de combate ao branqueamento de capitais e ao financiamento do terrorismo. Além disso, deve estar em conformidade com as leis de proteção de dados, como o RGPD, que impõe limites e condições sobre como os dados pessoais podem ser processados e armazenados.

Verifica-se, portanto uma limitação, e não uma negação, ao direito ao apagamento quando está em causa a proteção a um bem jurídico hierarquicamente superior assegurada em casos de investigação contra o branqueamento de capitais e financiamento ao terrorismo.

3.3.5. Direito à Limitação do Processamento

A limitação do processamento está definida no artigo 4.º, 3 do RGPD, e significa "a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro". O direito à limitação do tratamento dos dados pode ser requerido pelo titular dos dados nas situações expressas no artigo 18.º, 1 do RGPD: a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; c) O responsável pelo tratamento já não

2. Se, em 25 de junho de 2015, estiverem pendentes num Estado-Membro processos judiciais e administrativos relativos à prevenção, deteção, investigação ou repressão de suspeita de branqueamento de capitais ou de financiamento do terrorismo, e uma entidade obrigada conservar informações ou documentos relativos a esses processos pendentes, essas informações ou documentos podem ser conservados pela entidade obrigada nos termos do direito nacional durante um período de cinco anos a contar da data de 25 de junho de 2015. Sem prejuízo do direito penal em matéria de meios de prova aplicável a investigações criminais e a processos judiciais e administrativos pendentes os Estados-Membros podem autorizar ou exigir a conservação dessas informações ou de tais documentos por um novo período de cinco anos se tiver sido determinada a necessidade e proporcionalidade de tal conservação adicional para a prevenção, deteção, investigação ou repressão de suspeita de branqueamento de capitais ou de financiamento do terrorismo.

precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; d) Se tiver oposto ao tratamento nos termos do artigo 21.º, n.º 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

Regra geral, quando houver a limitação do tratamento dos dados, o único tratamento possível a ser dado aos dados será a conservação dos mesmos. Há exceções[99] para o tratamento dos dados quando houver a limitação, ou seja, é possível que, mesmo com a limitação, ainda haja tratamento dos dados nas situações taxativas de (i) com o consentimento do titular, ou (ii) para efeitos de declaração, exercício ou defesa de um direito num processo judicial, (iii) de defesa dos direitos de outra pessoa singular ou coletiva, ou (iv) por motivos ponderosos de interesse público da União ou de um Estado-Membro.

O direito à limitação do tratamento dos dados ao titular dos dados precisa ser assegurado por um dever ao responsável pelo tratamento dos dados, que está imposto no artigo 12.º do RGPD, de responder ao pedido do titular, sem demora injustificada, no prazo de 1 mês e de expor as suas razões quando indeferir o pedido.

No âmbito das criptomoedas, não há restrição para o titular dos dados requerer a limitação ao tratamento dos seus dados. Todavia, para fins de uma eventual investigação AML/CFT, a limitação dos dados não ocorrerá, tendo em vista que, de acordo com o artigo 43.º da 5AMLD, "O tratamento de dados pessoais com base na presente diretiva para efeitos da prevenção do branqueamento de capitais e do financiamento do terrorismo conforme referido no artigo 1.o é considerado uma questão de interesse público ao abrigo do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho." Logo, está assegurada como uma das exceções mencionadas, ou seja, pode haver uma limitação ao tratamento dos dados no tocante à publicidade, por exemplo, mas não ocorrerá para efeitos de prevenção do branqueamento de capitais e do financiamento do terrorismo.

3.3.6. Direito à Portabilidade dos Dados

[99] Artigo 18.º, 2, RGPD.

O direito de portabilidade dos dados pode ser exercido de duas formas: (i) o titular dos dados solicita ao responsável pelo tratamento que transfira os seus dados a um novo responsável de sua indicação – transferência direta (art.º 20.º, 1, RGPD[100]); (ii) o titular dos dados atua como um intermediário, promovendo a transferência dos dados – transferência indireta (art.º 20.º, 2, RGPD[101]).

O princípio da autodeterminação informacional manifesta-se no direito de portabilidade, uma vez que o titular dos dados, no exercício desse direito, vê-se na posição de autodeterminar o destino dos seus dados pessoais. Trata-se de um direito coerente à intenção do legislador de conceder ao titular dos dados o poder de definir o que deseja fazer com os seus dados. Também é possível perceber uma relevância social que surge como consequência do direito de portabilidade, que fomenta a livre concorrência, visto que facilita a contratação de outras prestadoras de serviços.

Há, todavia, críticas a esse direito, uma vez que surge a situação de empresas serem obrigadas a fazer a portablidade dos dados a uma empresa concorrente. Conforme explicita A. Barreto Menezes Cordeiro[102], "a situação assume especial relevância se estivermos a lidar com segredos de negócio ou com direitos de propriedade intelectual".

Se verificarmos a viabilidade do exercício do direito à portabilidade em relação aos dados dos adquirentes de criptomoedas, percebe-se uma dificuldade na origem: as transações de criptomoedas são geralmente pseudônimas e não necessariamente vinculadas a dados pessoais identificáveis. Portanto, o conceito de portabilidade de dados pode não ser diretamente aplicável ou relevante para os dados da própria transação de criptomoeda. Contudo, aplica-se o direito de portabilidade aos dados pessoais coletados pelas exchanges de criptomoedas e os provedores de carteiras digitais, sendo possível que os utilizadores solicitem a portabilidade de seus dados pessoais para uma outra plataforma, indicada pelo titular dos dados.

---

[100] Artigo 20.º: Direito de portabilidade dos dados
1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:
a) O tratamento se basear no consentimento dado nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a), ou num contrato referido no artigo 6.º, n.º 1, alínea b); e
b) O tratamento for realizado por meios automatizados.

[101] Artigo 20.º: Direito de portabilidade dos dados
2 Ao exercer o seu direito de portabilidade dos dados nos termos do n.º 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.

[102] CORDEIRO, A. Barreto Menezes, *Direito da Proteção de dados à luz do RGPD e da Lei n.º 58/2019*, Reimpressão, Almedina, Coimbra, 2020, p. 291.

3.3.7. Direito de Oposição

O direito de oposição encontra fundamento direto no princípio da autodeterminação informacional, visto que cabe ao titular dos dados determinar acerca da utilização dos próprios dados. É nesse sentido que o titular dos dados pode opor-se a qualquer momento, por motivos relacionados com a sua situação particular, conforme preleciona o artigo 21.º do RGPD[103].

O direito à oposição assume três situações distintas:

Direito geral de oposição: o titular dos dados deve demonstrar que a sua situação particular justifica a oposição ao tratamento dos seus dados pessoais. Importa mencionar que não está em causa a (i)licitude do tratamento dos dados, pois, caso assim o fosse, incidiria o artigo 17.º, RGPD – direito ao apagamento – ao caso, e não o artigo 21.º, RGPD – direito de oposição. A arguição desse direito com base no fundamento da situação particular do titular dos dados, leva o responsável pelo tratamento dos dados a cessar o tratamento, a menos que (i) apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou (ii) esse tratamento seja necessário para efeitos de declaração, exercício ou defesa de um direito num processo judicial, conforme número 1 do art.º 21.º do RGPD.

[103] Artigo 21.º: Direito de oposição
1. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.º, n.o 1, alínea e) ou f), ou no artigo 6.º, n.º 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
2. Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.
3. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim.
4. O mais tardar no momento da primeira comunicação ao titular dos dados, o direito a que se referem os n.os 1 e 2 é explicitamente levado à atenção do titular dos dados e é apresentado de modo claro e distinto de quaisquer outras informações.
5. No contexto da utilização dos serviços da sociedade da informação, e sem prejuízo da Diretiva 2002/58/CE, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas.
6. Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público.

O dispositivo não traz a exceção de “interesse público”, que estaria enquadrada em caso de dados relacionados a criptomoedas (art.º 43.º, 5AML), no entanto pode-se interpretar de forma extensiva, de forma que seja o argumento utilizado para negar o direito à oposição nesses casos e não cessar o tratamento dos dados em causa.

Direito de oposição relativo à comercialização direta: trata-se de um direito potestativo clássico, ou seja, os titulares dos dados podem opor-se ao tratamento dos seus dados que estejam sendo utilizados para comercialização direta, de forma unilateral e sem a necessidade de o responsável analisar se o pedido de oposição será ou não concedido.

Direito de oposição relativo ao tratamento para fins de investigação científica:

Para pleitear esse direito, o titular dos dados terá de demonstrar a particularidade da sua situação, enquanto o responsável pelo tratamento dos dados contrapõe invocando a necessidade do tratamento para a prossecução de interesse público.

4. O Desafio da Proteção de Dados na Era dos *Cryptoassets*

A proteção de dados na era dos *cryptoassets* na União Europeia (UE) representa um desafio multifacetado e de crescente importância. Os *cryptoassets*, que não são emitidos nem garantidos por bancos centrais ou autoridades públicas, apresentam riscos para a proteção do consumidor e a estabilidade financeira e estão atualmente fora do escopo da legislação da UE

As chaves privadas que controlam os *cryptoassets* são dados sensíveis que necessitam de importante proteção, no que toca à proteção de dados. Conforme exposto no ponto 3.2 deste trabalho, a UE está continuamente a desenvolver um quadro regulatório que inclui supervisão, proteção do consumidor e sustentabilidade dos *cryptoassets*, exigindo transparência, divulgação e autorização de transações.

Além disso, a supervisão dos *cryptoassets* é encarada como essencial para a proteção de dados, sendo a Autoridade Europeia dos Valores Mobiliários e dos Mercados - *European Securities and Markets Authority* (ESMA) a entidade que supervisionará a emissão de *tokens* referenciados a ativos, enquanto a Autoridade Bancária Europeia - *European Banking Authority* (EBA) será responsável pela supervisão de *tokens* de dinheiro eletrónico.[104]

As iniciativas legislativas, como o relatório MiCA adotado pelo Parlamento Europeu, visam estabelecer uma regulamentação de *cryptoassets* amigável à inovação, proteção do consumidor, segurança jurídica e a criação de estruturas de supervisão confiáveis. Iniciativas como estas refletem a complexidade de equilibrar a inovação tecnológica com a necessidade de proteger dados e oferecer segurança aos utilizadores na UE.

4.1. A Necessidade de Proteger os Dados Pessoais dos utilizadores

[104] European Parliament, *Cryptocurrencies in the EU: new rules to boost benefits and curb threats* Bruxelas, 2022, Consultado em 26 de Janeiro de 2024. Disponível aqui: <https://www.europarl.europa.eu/news/en/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats

A necessidade de proteger os dados pessoais dos utilizadores no contexto dos ativos criptográficos é um assunto de grande relevância e complexidade. A crescente popularidade das criptomoedas (e outras formas de ativos digitais) traz desafios importantes para a proteção de dados, principalmente devido à sua natureza.

A regulamentação dos *cryptoassets* e a proteção dos dados pessoais dos seus titulares, na UE, são de suma importância para o desenvolvimento seguro desta nova classe de ativos digitais. A ascensão rápida dos *cryptoassets* trouxe consigo um conjunto de desafios inéditos em termos de privacidade e proteção de dados, o que exige uma atenção regulatória especializada e focada. A natureza descentralizada e anónima/pseudónima das transações de *cryptoassets* pode, por um lado, salvaguardar a privacidade dos usuários, mas, por outro, pode ser explorada para fins ilícitos, tornando imperativa a criação de um quadro regulatório robusto que proteja os dados pessoais sem inibir a inovação.

As transações em criptomoedas são frequentemente alvos de *hackers* devido ao valor elevado dos ativos digitais. Isso coloca em risco não apenas os ativos financeiros dos usuários, mas também seus dados pessoais. Vazamentos de dados podem ocorrer através de ataques a *exchanges* de criptomoedas ou carteiras digitais.

A atualização das diretivas de AML/CFT pela UE, que agora incluem provedores de serviços de *cryptoassets*, evidencia o reconhecimento da necessidade de uma governança mais rigorosa. Com a 5AMLD, os provedores de serviços são obrigados a identificar e verificar seus clientes, o que implica no tratamento de dados pessoais, colocando a proteção de dados no centro das operações com *cryptoassets*

Os membros do Parlamento Europeu propuseram regulamentações que visam endereçar especificamente os riscos associados aos *cryptoassets*, mencionados neste trabalho, incluindo medidas para um rastreamento eficaz das transferências, o que ajudaria a prevenir atividades ilícitas como lavagem de dinheiro e financiamento ao terrorismo. Esta regulamentação também visa a proteção dos dados pessoais dos titulares de *cryptoassets*, alinhando-se às normas estabelecidas pelo RGPD.

A proposta da criação de um registo público[105] de entidades de alto risco envolvidas com *cryptoassets* pela EBA é um exemplo de como a UE está trabalhando para atender à dupla exigência de transparência e proteção de dados. Este registo aumentaria a visibilidade sobre as operações de *cryptoassets*, ao mesmo tempo que garantiria a proteção dos dados dos usuários ao limitar o acesso a informações sensíveis

O equilíbrio entre inovação e proteção de dados é delicado. Por um lado, a UE procura apoiar a inovação tecnológica e o crescimento económico proporcionados pelos *cryptoassets*. Por outro, acaba por ter de fazer o oposto ao reconhecer a necessidade de proteger os cidadãos europeus de riscos associados ao mau uso de dados pessoais. Essa tensão destaca a importância de uma abordagem regulatória que seja flexível, mas que também seja suficientemente forte para se adaptar à evolução do mercado de *cryptoassets*.

Para proteger os dados pessoais dos utilizadores, as plataformas de criptomoedas devem implementar medidas de segurança de dados, tais como o uso de criptografia forte, autenticação de dois fatores e protocolos seguros de comunicação. Para além disso, as políticas de privacidade devem ser claras e acessíveis, garantindo que os utilizadores estejam cientes[106] de como seus dados são usados.

A educação e conscientização dos utilizadores sobre a legislação de privacidade de dados e as práticas de segurança de dados também são essenciais. Isso inclui instruí-los sobre a legislação em vigor, além de proteger as chaves privadas, escolher carteiras seguras e identificar possíveis golpes ou fraudes. À medida que o mercado de criptomoedas continua a crescer, também aumenta a necessidade de proteger os dados pessoais. Isso requer uma abordagem multidisciplinar que envolve tanto avanços tecnológicos quanto uma estrutura regulatória.

A proteção dos dados pessoais dos titulares de *cryptoassets* na UE é um elemento crítico que deve ser endereçado com políticas claras e consistentes. O compromisso da UE com a proteção de dados e a privacidade se reflete nas suas iniciativas regulatórias, buscando assegurar que o crescimento dos *cryptoassets* ocorra

[105] European Parliament, *Crypto assets: new rules to stop illicit flows in the EU*, Bruxelas, 2022, Consultado em 26 de janeiro de 2024. Disponível aqui: https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

[106] Princípio da transparência, ponto 3.2.3.

dentro de um ambiente seguro e confiável, que proteja os cidadãos e o sistema financeiro como um todo.

4.2. Os Riscos de Proteção de Dados Associados à Regulamentação AML/CFT

A regulamentação AML/CFT desempenha um papel crucial na prevenção de atividades ilícitas no setor financeiro. No entanto, essa regulamentação não está isenta de desafios significativos relacionados à proteção de dados pessoais. A coleta e o tratamento massivos de informações sensíveis são necessários para cumprir as obrigações da AML/CFT, e isso pode aumentar os riscos de violações de privacidade e uso indevido de dados.

Encontrar o equilíbrio adequado entre a eficácia das medidas de AML/CFT e a proteção de dados pessoais é um dos principais desafios do legislador. A exposição de informações financeiras e pessoais dos titulares dos dados a terceiros não autorizados é um risco indesejável da recolha excessiva de informações que as investigações AML/CFT por vezes necessitam. Para além disso, é preciso ter atenção ao armazenamento prolongado de dados, pois pode aumentar a probabilidade de violações de dados, especialmente em um ambiente de ameaças cibernéticas em constante evolução.

As criptomoedas são frequentemente valorizadas por seu anonimato/pseudonimato e descentralização e, em contrapartida, as regulamentações AML/CFT exigem a identificação e a verificação de clientes (CDD e KYC) para prevenir atividades ilícitas. Isso pode entrar em conflito com a natureza anónima das transações em criptomoedas e levantar preocupações sobre a proteção de dados pessoais.

Os procedimentos KYC coletam informações sensíveis relativamente ao cliente e, se não forem adequadamente protegidas, podem estar vulneráveis a vazamentos e ataques cibernéticos. As plataformas que lidam com *cryptoassets* devem implementar fortes medidas de segurança de dados para proteger esses dados.

A União Europeia, por exemplo, enfrenta esses desafios ao tentar harmonizar a regulamentação AML/CFT com o RGPD. Embora ambas as regulamentações busquem objetivos legítimos, sua implementação conjunta requer um cuidadoso ajuste para proteger a privacidade dos cidadãos sem comprometer a segurança financeira. É essencial encontrar abordagens inovadoras, como o uso de tecnologias de anonimização e pseudonimização, para alcançar esse equilíbrio.

4.2.1. **O Interesse Público no contexto de AML/CFT e a Mitigação da Proteção de Dados**

O Artigo 43.º da 5AMLD da UE e a necessidade de proteção de dados no contexto das criptomoedas representam um interessante ponto de equilíbrio entre a segurança pública e a privacidade individual. A questão do interesse público como fundamento para mitigar a proteção de dados surge como um aspecto chave quando se trata de regulamentar e monitorar atividades financeiras, incluindo aquelas que envolvem criptomoedas.

O Artigo 43.º reconhece que, para efeitos da prevenção do branqueamento de capitais e do financiamento do terrorismo, o interesse público pode justificar limitações nos direitos de proteção de dados. O legislador reconhece a necessidade de violação à porteção de dados, e utiliza a exceção do "interesse público" para fundamentá-la. Significa que as autoridades podem ter acesso a dados pessoais, bem como proceder com o tratamento desses dados, com a finalidade de investigar e prevenir atividades ilícitas, como branqueamento de capitais e financiamento do terrorismo. Este acesso é necessário para rastrear transações suspeitas, identificar atividades ilegais e garantir a integridade do sistema financeiro.

A necessidade de equilibrar a segurança pública com o direito à privacidade gera uma tensão entre o Artigo 43.º da 5AML e a proteção de dados no contexto das criptomoedas. Por um lado, as autoridades precisam de ferramentas (dados pessoais) para combater o branqueamento de capitais e o financiamento do terrorismo efetivamente; enquanto por outro lado, é fundamental garantir que a privacidade dos

indivíduos seja protegida e que os dados pessoais não sejam indevidamente expostos ou utilizados.

Na prática, a aplicação do Artigo 43.º no contexto das criptomoedas requer um equilíbrio sensível. Os dados pessoais dos utilizadores precisam ser protegidos, enquanto as autoridades reguladoras e as empresas que operam com criptomoedas devem garantir a conformidade com as regulamentações AML/CFT, o que parece desafiador. Isso pode envolver o desenvolvimento de sistemas avançados que permitam o rastreamento de transações suspeitas, sem comprometer desnecessariamente a privacidade dos utilizadores.

O Artigo 43.º da 5AMLD e a necessidade de proteção de dados no contexto das criptomoedas destacam a complexidade de regular um setor financeiro inovador e em rápida evolução. É preciso que as autoridades busquem prevenir atividades financeiras ilícitas, e garantam a proteção da privacidade dos utilizadores de criptomoedas. Encontrar um equilíbrio entre esses dois objetivos é essencial para o desenvolvimento saudável e seguro do mercado de criptomoedas.

4.3. Equilibrando Regulamentação AML/CFT e Proteção de Dados

A necessidade de se achar um equilíbrio entre a legislação AML/CFT e a proteção de dados é tão importante quanto desafiador. Importa salientar que, em havendo um conflito entre normas de proteção de dados e normas AML/CFT, estas devem prevalecer, tendo em vista o bem jurídico tutelado e o interesse público[107] prevalecente. Não se pode, contudo, negligenciar a proteção dos dados sempre sob a justificativa do interesse público. É preciso ter cautela e prudência na conciliação das normas para assegurar a salvaguarda do tanto quanto possível da proteção dos dados. Assim, ao balancear a proteção de dados com a regulamentação AML/CFT, há áreas na proteção dos dados que precisam ser mitigadas para garantir a conformidade com ambas as regulamentações:

Relativamente à recolha dos dados pesoais, a regulamentação AML/CFT exige que seja coletados dados pessoais no detalhe para sejam atendidos os critérios dos

[107] Ponto 4.2.1

processos de CDD, noemadamente KYC. Isso pode entrar em conflito com os princípios do RGPD, como a minimização de dados, que exige a recolha de dados que sejam estritamente necessários. Para que sejam atendidos tanto a regulamentação AML-CFT, quanto o RGPD, seria necessário limitar a coleta de dados ao que seja estritamente necessário para cumprir com as obrigações de AML/CFT.

Na prática, as informações coletadas para atender aos requisitos de AML/CFT estão descritas na al. a), número 1 do artigo 13.º da 5AML, que são "A identificação do cliente e a verificação da respetiva identidade, com base em documentos, dados ou informações obtidos junto de uma fonte independente e credível, incluindo, se disponíveis, os meios de identificação eletrónica"

Relativamente ao MiCA, houve uma preocupação do legislador em estabelecer um alinhamento com a legislação em proteção de dados, nomeadamente o RGPD, ou seja, os princípios fundamentais e os direitos dos titulares dos dados são preservados, devendo as autoriadades competentes exercer as suas funções em conformidade com o RGPD.

Por definição (artigo 4.º, 2, RGPD), a recolha dos dados faz parte do tratamento dos dados, o que pode-se dizer que seria o primeiro ato do tratamento por parte do responsável pelo tratamento dos dados. O artigo 6.º do RGPD trata das situações que descrevem a licitude do tratamento e, em sua al. e), assegura a licitude do tratamento em casos de necessidade para o exercício de funções de interesse público. Conforme já analisado neste trabalho, o interessse público (art.º 43.º, 5AML) é o fundamento chave para justificar uma mitigação à proteção de dados no contexto de investigação AML/CFT. Não se pode, contudo, extrapolar as exigências AML/CFT em detrimento da proteção de dados sob a eterna justificativa do interesse público. Para que as legislações funcionem na sociedade em harmonia, é preciso parcimônia por parte do legislador nesse aspeto. A coleta excessiva de dados pode levar a preocupações com a privacidade, aumentar o risco de vazamentos de dados e potencialmente violar as leis de proteção de dados.

Embora não seja um caso específico de excesso de recolha de dados no contexto de *cryptoassets* e AML/CFT, o TJUE frequentemente lida com casos envolvendo o equilíbrio entre a privacidade dos dados e a segurança, especialmente em contextos onde a vigilância governamental e a coleta de dados são questionadas. Os casos

Schrems I (Caso C-362/14[108]) e Schrems II (Caso C-311/18[109]) são bons exemplos para ilustrar essa situação: em Shrems I, Maximillian Schrems, um ativista austríaco de privacidade, questionou a transferência de seus dados pessoais do Facebook da Irlanda para os EUA, argumentando que os EUA não ofereciam proteção adequada de dados. O TJUE invalidou o acordo *Safe Harbor*[110], afirmando que os EUA não garantiam um nível adequado de proteção de dados, principalmente devido à vigilância governamental. Após o Schrems I, a UE e os EUA estabeleceram o *Privacy Shield*[111], e Schrems continuou a desafiar a adequação da proteção de dados sob este novo acordo. O TJUE invalidou o *Privacy Shield*, concluindo que ele não fornecia proteção suficiente contra o acesso do governo dos EUA aos dados dos cidadãos da UE. O tribunal também esclareceu que as cláusulas contratuais padrão (SCCs) são válidas, mas destacou a necessidade de avaliar caso a caso a adequação da proteção de dados no país receptor. Ambas as decisões enfatizam a importância da proteção de dados e a necessidade de mecanismos de transferência que respeitem os direitos de privacidade dos cidadãos da UE, destacando preocupações com o excesso de coleta e acesso a dados pessoais por autoridades governamentais, nomeadamente nos EUA.

O artigo 35.º do RGPD[112] trata da avaliação de impacto sobre a proteção de dados - *Data Protection Impact Assessments* (DPIA), que ajudam a identificar e analisar

[108] Acordão do Tribunal de Justiça Europeu, de 6 de outubro de 2015, processo C – 362/14. Consultado em 27 de janeiro de 2024. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0362&qid=1706376152672

[109] Acordão do Tribunal de Justiça Europeu, de 16 de julho de 2020, processo C – 311/18. Consultado em 27 de janeiro de 2024. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62018CJ0311&qid=1706376152672

[110] Mecanismo que permitia a transferência de dados da UE para os EUA.

[111] Novo mecanismo de transferência de dados.

[112] Artigo 35.º: Avaliação de impacto sobre a proteção de dados

1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.
2. Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado.
3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.o 1 é obrigatória nomeadamente em caso de:
a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o; ou
c) Controlo sistemático de zonas acessíveis ao público em grande escala.

como os dados pessoais são processados e os riscos potenciais para a privacidade dos titulares dos dados. Após a identificação dos riscos, as DPIAs são usadas para achar maneiras de minimizá-los, a fim de garantir que o processamento de dados esteja em conformidade com o RGPD. As DPIAs são cabíveis para processamento de dados que possa resultar em um alto risco para os direitos e liberdades dos indivíduos. Isso inclui, mas não se limita a, monitoramento em larga escala, processamento de categorias especiais de dados (como dados sensíveis) e uso de novas tecnologias (nomeadamente, *cryptoassets*). É através da DPIA que será avaliada a necessidade do tratamento dos dados em causa e se é proporcional aos objetivos pretendidos, identificação dos riscos para os direitos e liberdades dos indivíduos, bem como serão propostas medidas para reduzir ou eliminar os riscos identificados, o que auxilia as organizações a evitar multas e outras penalidades.Como consequência, aumentam a transparência do tratamento de

---

4. A autoridade de controlo elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados por força do n.o 1. A autoridade de controlo comunica essas listas ao Comité referido no artigo 68.o.
5. A autoridade de controlo pode também elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados. A autoridade de controlo comunica essas listas ao Comité.
6. Antes de adotar as listas a que se referem os n.os 4 e 5, a autoridade de controlo competente aplica o procedimento de controlo da coerência referido no artigo 63.o sempre que essas listas enunciem atividades de tratamento relacionadas com a oferta de bens ou serviços a titulares de dados ou com o controlo do seu comportamento em diversos Estados-Membros, ou possam afetar substancialmente a livre circulação de dados pessoais na União.
7. A avaliação inclui, pelo menos:
a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;
b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;
c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.o 1; e
d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.
8. Ao avaliar o impacto das operações de tratamento efetuadas pelos responsáveis pelo tratamento ou pelos subcontratantes, em especial para efeitos de uma avaliação de impacto sobre a proteção de dados, é tido na devida conta o cumprimento dos códigos de conduta aprovados a que se refere o artigo 40.o por parte desses responsáveis ou subcontratantes.
9. Se for adequado, o responsável pelo tratamento solicita a opinião dos titulares de dados ou dos seus representantes sobre o tratamento previsto, sem prejuízo da defesa dos interesses comerciais ou públicos ou da segurança das operações de tratamento.
10. Se o tratamento efetuado por força do artigo 6.o, n.o 1, alínea c) ou e), tiver por fundamento jurídico o direito da União ou do Estado-Membro a que o responsável pelo tratamento está sujeito, e esse direito regular a operação ou as operações de tratamento específicas em questão, e se já tiver sido realizada uma avaliação de impacto sobre a proteção de dados no âmbito de uma avaliação de impacto geral no contexto da adoção desse fundamento jurídico, não são aplicáveis os n.os 1 a 7, salvo se os Estados-Membros considerarem necessário proceder a essa avaliação antes das atividades de tratamento.
11. Se necessário, o responsável pelo tratamento procede a um controlo para avaliar se o tratamento é realizado em conformidade com a avaliação de impacto sobre a proteção de dados, pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam.

dados e podem melhorar a confiança dos utilizadores e clientes. Por esses motivos, é salutar que as organizações que operam com *cryptoassets* realizem DPIAs.

Em consonância com o artigo 40.º da 5AMLD, já mencionado nesta dissertação, e o artigo 32.º do RGPD[113], importa salientar que os dados recolhidos devem ser armazenados com segurança para evitar acessos não autorizados ou vazamentos. As entidades devem implementar e manter medidas de segurança robustas, como criptografia, controle de acesso e monitoramento regular de sistemas. Para assegurar uma maior proteção dos dados, é importante que sejam tomadas algumas medidas, como a utilização de criptografia forte para proteger dados pessoais durante a transmissão e enquanto estão armazenados; restrição do acesso aos dados a pessoal autorizado e implementação de autenticação de múltiplos fatores para aceder sistemas sensíveis; implementação de sistemas de monitoramento para detetar e alertar sobre atividades suspeitas ou tentativas de violação de dados; manutenção de *backups* regulares dos dados e obtenção de um plano de recuperação de desastres com vistas a restaurar dados em caso de perda ou corrupção; realização de auditorias periódicas de segurança e avaliações de vulnerabilidade para identificação e correção de possíveis falhas de segurança; desenvolvimento e implementação de políticas de segurança de dados abrangentes e garantia de que os funcionários recebam treinamento regular sobre práticas de segurança de dados.

---

[113] Artigo 32.º: Segurança do tratamento
1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:
a) A pseudonimização e a cifragem dos dados pessoais;
b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.
2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.
3. O cumprimento de um código de conduta aprovado conforme referido no artigo 40.o ou de um procedimento de certificação aprovado conforme referido no artigo 42.o pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas no n.o 1 do presente artigo.
4. O responsável pelo tratamento e o subcontratante tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União ou de um Estado-Membro.

Relativamente à matéria em causa, houve um caso em que foi aplicada uma multa à British Airways[114] pela ICO (*Information Commissioner's Office*) no valor de 20 milhões de libras por processar dados pessoais dos seus clientes sem a devida adoção de medidas de segurança. No mesmo mês, a ICO multou a Marriott International [115]devido a uma violação de segurança de dados que expôs informações pessoais de milhões de hóspedes, após um ataque cibernético.

Esses casos sublinham a importância de ter medidas rigorosas de segurança de dados em vigor e a necessidade de conformidade com o RGPD. Para as entidades que lidam com *cryptoassets*, o cumprimento das melhores práticas de segurança de dados não é apenas uma questão de conformidade regulatória, mas também uma necessidade crítica para manter a confiança dos utilizadores e proteger contra riscos financeiros e legais.

As entidades devem informar os usuários sobre como seus dados são recolhidos, usados e partilhados. Para além disso, embora o consentimento nem sempre seja viável ou necessário, no âmbito da legislação AML/CFT, é importante considerar os direitos dos titulares de dados sob o RGPD, incluindo o direito de ser informado e o direito de acesso. Estes direitos garantem que os titulares dos dados estejam plenamente informados sobre o tratamento dos seus dados, e que tenham um papel ativo na gestão desses dados[116].

A transparência e o consentimento são essenciais para garantir a confiança e a segurança dos usuários no ecossistema dos *cryptoassets*. As entidades que operam neste espaço devem se esforçar para manter práticas claras e éticas de tratamento de dados, assegurando que o consentimento seja obtido de forma justa e que os usuários estejam plenamente informados sobre o uso de seus dados. Essas práticas atendem às exigências legais, e ajudam a construir uma relação de confiança com os utilizadores.

Os dados devem ser mantidos apenas pelo tempo necessário para cumprir com os requisitos de AML/CFT e, depois disso, devem ser excluídas ou anonimizadas, a menos que existam outras bases legais para a retenção. As empresas de *cryptoassets*

---

[114] Information Commissioner's Office, *Information Commissioner's Annual Report and Financial Statements 2020-21*, 2021, p. 31. Consultado em 27 de janeiro de 2024. Disponível aqui: https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf

[115] Information Commissioner's Office, *Information Commissioner's Annual Report and Financial Statements 2020-21*, 2021, p. 31. Consultado em 27 de janeiro de 2024. Disponível aqui: https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf

[116] Direito à Autodeterminação Informacional, ponto 2.3.3.1.

estabelecem políticas que definem quanto tempo os dados pessoais serão retidos. Estas políticas geralmente baseiam-se na necessidade de cumprir com as obrigações legais, contratuais e regulatórias.

A 5AMLD determina que as empresas mantenham registos dos clientes e transações por um período mínimo de 5 anos após o término da relação de negócios ou da transação, prorrogável por mais 5 anos, e, após o período de retenção, as empresas devem revisar os dados armazenados a fim de eliminar ou anonimizar os dados que não são mais necessários. Durante o período de retenção, as empresas devem garantir a segurança dos dados para protegê-los contra acessos não autorizados ou vazamentos. A violação desse dever por parte do responsável pelo tratamento dos dados ceifa o direito ao esquecimento do titular dos dados.

Embora casos específicos no contexto de *cryptoassets* possam ainda não ter sido discutidos em tribunais, as práticas de retenção de dados na indústria devem alinhar-se às diretrizes estabelecidas pelo RGPD e pelas regulamentações AML/CFT, incluindo definir claramente os períodos de retenção, assegurar a proteção dos dados durante esse período e garantir a eliminação ou anonimização dos dados quando eles não forem mais necessários. Essas práticas são essenciais para proteger a privacidade dos usuários e manter a conformidade com as leis de proteção de dados.

Os funcionários de empresas de *cryptoassets* devem ser treinados sobre as obrigações de proteção de dados e AML/CFT, a fim de que possam garantir que compreendam e apliquem adequadamente as políticas e procedimentos. O objetivo é oferecer programas de treinamento para educar a equipa sobre o RGPD, e sobre as práticas específicas de AML/CFT. Dar formação para certificação[117] e ter um código de conduta[118] são formas de os responsáveis pelo tratamento dos dados provarem que estão em cumprimento com os deveres estabelecidos no RGPD (isso pode incluir sessões de treinamento regulares, *workshops* e *e-learning*).

As referidas formações geralmente abrangem melhores práticas de segurança cibernética, como a gestão segura de chaves de criptografia, identificação de tentativas de *phishing* e outras ameaças à segurança de dados, para além dos aspectos legais. É salutar que as formações sejam atualizadas regularmente para refletir as últimas tendências, ameaças e mudanças na legislação, tendo em vista a natureza em rápida evolução do setor de criptomoedas.

[117] Art.º 42.º, RGPD.
[118] Art.º 40.º, RGPD.

Importa destacar que diferentes departamentos podem necessitar de formação específica com base em suas funções, como desenvolvedores de *blockchain*, equipa de *compliance* ou pessoal de atendimento ao cliente. Essas práticas ajudam a prevenir violações de dados e fortalecem a cultura de proteção de dados na organização.

Pode haver casos em que seja necessário equilibrar os direitos à privacidade e proteção de dados com o interesse público na prevenção de atividades criminosas. As entidades devem ter a devida diligência para avaliar tais situações a fim de tomar decisões justificadas e proporcionais. As empresas de *cryptoassets* devem seguir as regulamentações de AML/CFT, que exigem a recolha e o armazenamento de dados detalhados dos clientes para prevenir atividades ilícitas, o que pode entrar em conflito com o direito à privacidade dos usuários. No contexto da UE, as empresas devem aderir aos princípios do RGPD, como minimização de dados, consentimento e direito de acesso, que visam proteger os dados pessoais dos usuários. O balanceamento de direitos no contexto de *cryptoassets* é um desafio contínuo que requer uma abordagem cuidadosa e ponderada. As empresas devem estar cientes das obrigações legais sob as regulamentações de AML/CFT e GDPR, e devem buscar maneiras de cumprir ambas de maneira que respeite os direitos de privacidade dos usuários.

Em caso de violações de dados, as entidades devem ter processos claros para notificação rápida às autoridades e, se necessário, aos indivíduos afetados. As empresas de *cryptoassets* devem ter sistemas em vigor para detetar violações de segurança de dados rapidamente. Isso inclui monitoramento constante e sistemas de alerta precoce. Conforme o RGPD[119], em caso de uma violação de dados pessoais que possa resultar

[119] Artigo 33.º: Notificação de uma violação de dados pessoais à autoridade de controlo
1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.o, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.
2. O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais.
3. A notificação referida no n.o 1 deve, pelo menos:
a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;
b) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;
c) Descrever as consequências prováveis da violação de dados pessoais;
d) Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;
4. Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada.

em um risco para os direitos e liberdades dos indivíduos, a empresa deve notificar a autoridade de proteção de dados competente, geralmente em até 72 horas após tomar conhecimento da violação. As empresas devem devem comunicar a violação aos indivíduos afetados, especialmente se a violação puder resultar em um alto risco para seus direitos e liberdades, bem como notificar as autoridades, que deve ser clara e conter informações sobre a natureza da violação, os contatos onde podem obter mais informações, e as medidas recomendadas para mitigar seus riscos pessoais. Todas as violações de dados devem ser documentadas, incluindo os efeitos da violação e as medidas tomadas em resposta. O setor de *cryptoassets* não está imune a violações de dados, e várias plataformas de câmbio de criptomoedas já sofreram violações de segurança significativas. Embora estes incidentes não tenham necessariamente levado a ações judiciais focadas na notificação de violação sob o RGPD, eles ressaltam a importância de ter processos adequados de notificação de violação em vigor.

Verifica-se, portanto, que o equilíbrio necessário entre a regulamentação AML/CFT e a proteção de dados, no contexto de cryptoassets não é um tema de fácil resolução. Para uma regulamentação equilibrada nesse aspeto, faz-se importante analisar casos em concreto para que seja possível pontuar medidas que construam as arestas necessárias para a obtenção de uma maior segurança (de dados, financeira) a ser usufruída pela sociedade.

5. O responsável pelo tratamento documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo.

CONCLUSÃO

Esta dissertação apresentou uma exploração detalhada dos *cryptoassets*, destacando sua natureza emergente e impacto transformador no sistema financeiro global, com enfoque nas criptomoedas. A análise da tecnologia *blockchain* revelou sua importância fundamental, não apenas para os *cryptoassets*, mas como uma ferramenta para a inovação em diversas áreas. A discussão sobre regulamentações AML/CFT e a proteção de dados pessoais destacou a complexidade e a necessidade de abordagens regulatórias adaptativas.

Os *cryptoassets* estão redefinindo os paradigmas do sistema financeiro, desafiando as instituições tradicionais com novas oportunidades e riscos adjacentes. Demonstrou-se como esses ativos digitais estão a quebrar padrões estabelecidos de práticas de investimento e transações comerciais, forçando uma reavaliação dos métodos regulatórios e operacionais. As implicações para os mercados financeiros são profundas, apresentando tanto desafios quanto oportunidades para inovação e crescimento.

A tecnologia *blockchain*, com sua capacidade de proporcionar segurança, transparência e eficiência, é reconhecida nesta dissertação como um elemento disruptivo com potencial para transformar não apenas o setor financeiro, mas muitos outros. Sua aplicação vai além dos *cryptoassets*, oferecendo soluções inovadoras para questões de confiança e verificação em diversos campos, desde cadeias de suprimentos até governança corporativa.

A regulação dos *cryptoassets* apresenta desafios únicos, especialmente em termos de proteção de dados e de AML/CFT. A dissertação enfatizou os desafios regulatórios apresentados na atualidade para que seja possível a devida adaptação à natureza dinâmica e descentralizada dos *cryptoassets*.

Destacou-se a relevância de equilibrar a regulamentação dos *cryptoassets* com a promoção da inovação, a fim de que se obtenha um resultado eficaz no combate ao branqueamento de capitais e financiamento ao terrorismo. Discutiu-se como a regulação excessiva pode inibir o progresso da tecnologia, enquanto a ausência de regulação pode

acarretar em riscos para o sistema financeiro e os utilizadores. Foi proposta uma abordagem regulatória que reconhece a singularidade dos *cryptoassets* e estimula a inovação responsável.

A observância da proteção de dados na utilização de *cryptoassets* é desafiadora. A dissertação destacou as questões com a privacidade e segurança dos dados nas transações de criptomoedas, com destaque para a importância de regulamentações estratégicas e medidas eficazes de proteção de dados. Discutiu-se a importância de garantir a confiança dos utilizadores e a integridade dos sistemas em um ambiente onde a privacidade é um desafio constante.

Os *cryptoassets* e a tecnologia *blockchain* têm um potencial significativo para moldar a economia digital. Esta dissertação explorou as tendências emergentes e as possíveis direções para o desenvolvimento dessas tecnologias e as necessárias regulações, discutindo sobre seu papel na economia global e nas inovações futuras. Com base nas descobertas, esta dissertação sugere uma abordagem dinâmica e informada para a regulamentação dos *cryptoassets*, destacando que acompanhe a evolução tecnológica e atenda às necessidades de segurança, estabilidade e inovação.

Em suma, faz-se necessário que seja adoptada uma abordagem equilibrada e inovadora na regulamentação destes ativos, para que seja viável a promoção da inovação, a garantia da estabilidade financeira e a proteção dos dados pessoais. Este trabalho reforça a relevância dos *cryptoassets* como um fenómeno económico e tecnológico significativo, cujo impacto continuará a evoluir e a moldar o futuro da economia digital.

BIBLIOGRAFIA

Ac. do TJUE, de 13 de maio de 2014, processo C – 131/12. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CA0131&qid=1706532547622

Ac. do TJUE, de 6 de outubro de 2015, processo C – 362/14. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0362&qid=1706376152672

Ac. do TJUE, de 16 de julho de 2020, processo C – 311/18. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62018CJ0311&qid=1706376152672

AKED, Symon, BOLAN, Christopher, BRAND, Murray. *Determining What Characteristics Constitute a Darknet*, 2013. Disponível aqui: https://doi.org/10.4225/75/57b561bfcd8e0

Bank for International Settlements – *BIS, AML and CFT in banking – Executive Summary*. Disponível aqui: https://www.bis.org/fsi/fsisummaries/aml_cft_banking.pdf

Bank for International Settlements - *BIS, History – overview*, Disponível aqui: https://www.bis.org/about/history.htm?m=11

BOWLER, Ryan, GOODELL, Geoffrey, REVANS, Joe, BIZAMA Gabriel, SPEED Chris. *A Non-Custodial Wallet for CBDC: Design Challenges and Opportunities*. 2023. Disponível aqui: https://doi.org/10.48550/arXiv.2307.05167

BRADBURY, Danny, *The problem with Bitcoin. Computer Fraud & Security*, 2013. Disponível aqui: https://doi.org/10.1016/s1361-3723(13)70101-5

BRAGUÊS, José Luis. *O Processo de Branqueamento de Capitais, Edições Húmus & OBEGEF*, 2009, Disponível aqui: https://obegef.pt/wordpress/wp-content/uploads/2009/02/wp0021.pdf

BUTERIN, Vitalik. *Privacy in the Blockchain*. The Ethereum Blog. Disponível aqui: https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

CACHIN, Christian. *Blockchain-From the Anarchy of Cryptocurrencies to the Enterprise (Keynote Abstract)*, 2017. Disponível aqui: https://doi.org/10.4230/LIPIcs.OPODIS.2016.2

CANELLIS, David. *Here's how criminals use Bitcoin to launder dirty money*, 2018. Disponível aqui: https://thenextweb.com/news/bitcoin-money-laundering-2

CANOTILHO, Gomes, MOREIRA, Vital, *Constituição da República Portuguesa - Anotada - Volume I - Artigos 1º a 107º*, 4.ª Edição, Coimbra Editora, Coimbra, 2020

Carta dos Direitos Fundamentais da União Europeia. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12016P/TXT

CARVALHO, Adão, *O aumento da criminalidade associada às moedas virtuais*, 2021. Consultado em 07 de fevereiro de 2024. Disponível aqui: https://smmp.pt/smmp-na-imprensa/prova-digital-e-correio-eletronico-2/

CHATAIN, Pierre-Laurent, MCDOWELL, John, MOUSSET, Cedric, SCHOTT Paul Allan, VAN DER DOES DE WILLEBOIS, Emile. *Preventing Money Laundering and Terrorist Financing – A Practical Guide for Bank Supervisors*. The World Bank, Washington, DC. 2009.

CHOO, Kim-Kwang Raymond. *New payment methods: A review of 2010–2012 FATF mutual evaluation reports*, Computers & Security, Volume 36, 2013, Disponível aqui: https://doi.org/10.1016/j.cose.2013.01.009.

Comissão Europeia. *Comissão intensifica a luta contra o branqueamento de capitais e o financiamento do terrorismo*. Bruxelas, 2020. Disponível aqui: https://ec.europa.eu/commission/presscorner/detail/pt/ip_20_800

Conselho da União Europeia. *Combate ao branqueamento de capitais: Conselho e Parlamento Europeu chegam a acordo sobre regras mais estritas*. 2024. Disponível aqui: https://www.consilium.europa.eu/pt/press/press-releases/2024/01/18/anti-money-laundering-council-and-parliament-strike-deal-on-stricter-rules/

CORDEIRO, A. Barreto Menezes, *Direito da Proteção de dados à luz do RGPD e da Lei n.º 58/2019*, Reimpressão, Almedina, Coimbra, 2020

DE FILIPPI, Primavera, *Bitcoin: A Regulatory Nightmare to a Libertarian Dream*. Internet Policy Review, 3(2).. 2018. Disponível aqui: https://ssrn.com/abstract=2468695

DE FILIPPI, Primavera, *The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies*, Journal of Peer Production, 2016. Disponível aqui: https://ssrn.com/abstract=2852689

DE FILIPPI, Primavera, HASSAN, Samer. *Blockchain technology as a regulatory technology: From code is law to law is code*. First Monday, 2016. Disponível aqui: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097430

Directiva 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. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31991L0308

Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046

Directiva 2001/97/CE do Parlamento Europeu e do Conselho, de 4 de Dezembro de 2001, que altera a Directiva 91/308/CEE do Conselho relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais - Declaração da Comissão. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32001L0097

Directiva 2005/60/CE do Parlamento Europeu e do Conselho, de 26 de Outubro de 2005, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais e de financiamento do terrorismo (Texto relevante para efeitos do EEE) Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005L0060

Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, 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, que altera o Regulamento (UE) n.° 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão (Texto relevante para efeitos do EEE), 4AML/CFT. Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015L0849

Diretiva (UE) 2018/843 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera as Diretivas 2009/138/CE e 2013/36/UE (Texto relevante para efeitos do EEE), 5AML/CFT, Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32018L0843

DUARTE, Jorge Manuel Vaz Monteiro Dias. *Branqueamento de Capitais - O Regime do D.L 15/93, de 22 de Janeiro, e a Normativa Internacional*. Coimbra Editora, 2002.

European Parliament, *Crypto assets: new rules to stop illicit flows in the EU*, Bruxelas, 2022, Disponível aqui: https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

European Parliament, *Cryptocurrencies in the EU: new rules to boost benefits and curb threats*, Bruxelas, 2022, Disponível aqui: https://www.europarl.europa.eu/news/en/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats

European Parliament. *How blockchain technology could change our lives*, 2017. Disponível aqui: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

Europol Spotlight. Cryptocurrencies: *Tracing the Evolution of Criminal Finances*. Disponível aqui: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Europol. *European Union Terrorism Situation and Trend Report 2023*. Disponível aqui: https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf

FATF, *Country Members*, Disponível aqui: https://www.fatf-gafi.org/en/countries/fatf.html

FATF, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation*, The FATF Recommendations, 2023. Disponível aqui: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

Information Commissioner's Office, *Information Commissioner's Annual Report and Financial Statements 2020-21*, 2021. Disponível aqui: https://ico.org.uk/media/about-the-ico/documents/2620166/hc-354-information-commissioners-ara-2020-21.pdf

Innovative Technology Arrangements And Services Act. *Chapter 592*. Disponível aqui: https://legislation.mt/eli/cap/592/eng/pdf

KIVIATT, Trevor I. *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*. 2015. Disponível aqui: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3827&context=dlj

Lei n.º 89/2017, de 21 de Agosto, *Regime Jurídico do Registo Central do Beneficiário Efetivo*, Disponível aqui: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2755&tabela=leis&so_miolo=

Malta Digital Innovation Authority Act, *Chapter 591*. Disponível aqui: https://legislation.mt/eli/cap/591/eng

MAXIMILIAN JOHANNES TEICHMANN, Fabian and FALKER, Marie-Christin. *Money laundering via cryptocurrencies – potential solutions from Liechtenstein*. Disponível aqui https://doi/10.1108/JMLC-05-2020-0060

MOUGAYAR, William. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, 1.ª Edição, Wiley, New Jersey, 2016.

NAKAMOTO, Satoshi, Bitcoin: *A Peer-to-Peer Electronic Cash System*. Disponível aqui: https://bitcoin.org/bitcoin.pdf

NARAYANAN, Arvind, SHMATIKOV, Vitaly. *Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)*. The University of Texas at Austin, 2008. Disponível aqui: http://arxiv.org/pdf/cs/0610105v2.pdf

PINHEIRO, Alexandre Sousa; COELHO, Cristina Pimenta; DUARTE, Tatiana; GONÇALVES, Carlos José; GONÇALVES, Catarina Pina. *Comentário ao Regulamento Geral de Proteção de Dados.* Almedina, Coimbra, 2018

Proposta de DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO relativa aos mecanismos a criar pelos Estados-Membros para prevenir a utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que revoga a Diretiva (UE) 2015/849, 6AML/CFT, Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0423

Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo aos mercados de criptoativos e que altera a Diretiva (UE) 2019/1937, MiCA, Disponível aqui: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0006.02/DOC_1&format=PDF

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE), RGPD, Disponível aqui: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679

ROMETTY, Ginni, *From Yelp reviews to mango shipments: IBM's CEO on how blockchain will change the world*. Business Insider, 2017. Disponível aqui: http://www.businessinsider.com/ibm-ceo-ginni-rometty-blockchain-transactions-internet-communications-2017-6

SCHWAB, Klaus, *A quarta revolução industrial*, Edipro, São Paulo: Edipro, 2016.

TAPSCOTT, Don, & TAPSCOTT, Alex, Blockchain Revolution: *How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* 1.ª Edição, Senai-SP, São Paulo-SP, 2017.

Tribunal de Contas Europeu. *Os esforços da UE para combater o branqueamento de capitais no setor bancário são fragmentados e a aplicação é insuficiente*. 2021. Disponível aqui: https://www.eca.europa.eu/Lists/ECADocuments/SR21_13/SR_AML_PT.pdf

Virtual Financial Assets Act, *Chapter 590*. Disponível aqui: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=NIM:202103962

WRIGHT, Aaron; DE FILIPPI, Primavera, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Disponível aqui: https://ssrn.com/abstract=2580664

ZETZSCHE, Dirk, BUCKLEY, Ross P., ARNER, Douglas W., & FÖHR, Linus, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, UNSW Sydney Australia, 2018. Disponível aqui: https://dx.doi.org/10.2139/ssrn.3072298