REDES

Revista Eletrônica Direito e Sociedade

Canoas, v. 9, n. 1, 2021

Artigos

Recebido: 02.04.2020

Aprovado: 04.01.2021

Publicado: 29.03.2021

DOI http://dx.doi.org/10.18316/REDES.v9i1.6749

Considerações sobre anonimato, pseudoanonimato e criptomoedas

Jordan Vinícius Oliveira

Universidade do Estado do Rio de Janeiro, Rio de Janeiro, Brasil

http://orcid.org/0000-0002-6708-6086

Marília Carneiro da Cunha Lopes

Universidade do Estado do Rio de Janeiro, Rio de Janeiro, Brasil

https://orcid.org/0000-0002-8278-7243

Resumo: O presente artigo avalia a temática do anonimato e do pseudoanonimato para as criptomoedas. A pergunta de pesquisa avalia se existe, no ordenamento jurídico nacional, algum elemento restritivo para a transação de criptomoedas com o intuito de anonimato. Sob o prisma jurídico, a Lei Geral de Proteção de Dados Pessoais e as normativas do Banco Central e da Receita Federal integram o quadro de avaliação. Sob o prisma tecnológico, o modo de funcionamento e a relação com anonimato ou pseudoanonimato do Bitcoin, do Monero, do Zcash e do Dash compõem a análise. A conclusão é a de que, até o momento, a transação de criptomoedas verdadeiramente anônimas não encontra vedações expressas na legislação nacional, embora a obrigação de declará-las para a Receita Federal possa gerar repercussões concretas e converter a expectativa de anonimato em mero sigilo.

Palavras-chave: Anonimato; Bitcoin; Monero; Sigilo.

Reflections on anonymity, pseudonymity and criptocurrencies

Abstract: This paper evaluates the subject of anonymity and pseudonimity for cryptocurrencies. The research question investigates whether there is, within the Brazilian legislative framework, any prohibitive element regarding to cryptocurrencies designed to offer anonymity. In the legal view, the Brazilian General Data Protection Law and the norms edited by the Central Bank and the Department of Federal Revenue are analyzed. In the technological view, the operational elements and the anonymous or pseudonymous properties of cryptocurrencies such as Bitcoin, Monero, Zcash and Dash are investigated. The main conclusion is that, under the current Brazilian legislative context, anonymous cryptocurrencies are not undermined or forbidden, however the duty to file taxes, including these cryptocurrencies, is able to convert the expectancy of anonymity in a mere concrete state of secrecy.

Keywords: Anonymity; Bitcoin; Monero; Secrecy.

Introdução

Um sujeito nas sombras em frente à luz de um monitor de computador. Uma figura obscura com chapéu e terno, evitando ser identificada. Um indivíduo vestido com uma sorridente máscara eternizada pelo filme *Anonymous*. Seja qual a forma escolhida, são criativas e constantes as remissões ao anonimato na cultura, na mídia e no imaginário moderno. A visão misteriosa e sombria do anonimato foi aguçada, ainda mais, a partir do surgimento e da popularização de criptomoedas como o Bitcoin. E o caso do mercado paralelo operante em *darknet*, conhecido como *Silk Road*, constituiu um importante marco para essa associação. Fundado em 2011 e fechado em 2013 pelo FBI, o *Silk Road* povoou os noticiários policiais e chamou as atenções de autoridades públicas devido à comercialização de inúmeros itens ilegais na Internet, acessíveis pelo navegador *Tor* e transacionáveis em unidades de *bitcoins*[1].

Dessa maneira, o presente artigo tem por intuito averiguar a relação entre criptomoedas, anonimato e pseudoanonimato, desenvolvendo uma análise de elementos jurídicos e tecnológicos contidos na operacionalização de moedas digitais como o *Bitcoin*, o *Monero*, o *Zcash* e o *Dash*. A pergunta de pesquisa avalia se, no ordenamento jurídico nacional, existem elementos jurídicos que validem ou impeçam a comercialização de criptomoedas com verdadeiras propriedades de anonimato.

O presente estudo é pautado no método de análise qualitativa de conteúdo latente (*unobtrusive research*), segundo Earl Babbie[2]. Esta análise se desenvolve pelo levantamento de uma hipótese inicial de explicação para um fenômeno, a validação de situações fáticas capazes de contradizê-la e a revisão final da hipótese, seja pela sua reformulação completa ou por ajustes pontuais. Assim, nas próximas seções avaliar-se-á aspectos ligados às criptomoedas em sua complexidade tecnológica e fática, incluindo-se seus eventuais atributos de anonimato e pseudoanonimato, contrapondo-os à realidade do marco legislativo brasileiro. Para desenvolver essa análise, a seção 2 avalia os conceitos jurídicos de anonimato e pseudoanonimato diante da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), bem como estabelece uma análise acerca das criptomoedas Bitcoin, Monero, Zcash e Dash diante de seu eventual atributo de anonimato. Na seção 3 é desenvolvida uma análise do modelo regulatório das criptomoedas no Brasil, sobretudo acerca da eventual possibilidade de transações de moedas com atributos de anonimato e a obrigação de declaração das moedas junto ao imposto de renda. Na seção 4, por fim, são apresentadas as considerações finais.

Lei Geral de Dados Pessoais: o Direito entre o Anonimato e o Pseudoanonimato

A aprovação da lei nº 13.709/2018, Lei Geral de Dados Pessoais (LGPD) trouxe inúmeros avanços para a utilização de informações atinentes a pessoas naturais em tempos tecnológicos[3]. Entre temas

[1] WOOLF, Nicky. Silk Road sentencing: why governments can't win the war on darknet drugs. **The Guardian**, Londres, 31 mar. 2015. Disponível em <https://www.theguardian.com/technology/2015/may/31/silk-road-sentencing-darknet-drugs>. Acesso em 25 fev. 2020.

[2] BABBIE, Earl. **The practice of social research**. 11 ed. Belmont: Thomson Wadsworth, 2007. p. 328-329.

[3] Cabe destacar que embora publicada em agosto de 2018, a LGPD estava prevista para entrar em vigor 18 meses após sua publicação. Com a edição da Medida Provisória nº 869/2018, posteriormente convertida na Lei nº 13.583/2019, sua vigência foi adiada para agosto de 2020.

importantes, como o uso de dados sensíveis ou o tratamento de dados de crianças e adolescentes, a LGPD trouxe destaque ao chamado dado anonimizado. A bem da verdade, como bem destaca Danilo Doneda, a despeito de só restarem positivados agora, "a possibilidade ampla de utilização de dados submetidos a processos de anonimização ou a facilidade em usar dados pseudonimizados e seu impacto à privacidade são discutidas desde, ao menos, a primeira metade do século XX"[4].

Sendo o dado pessoal o atributo identificado ou identificável em relação a uma pessoa natural (também chamada de titular, artigo 5º, inciso I)[5], o dado anonimizado é, no sentido diverso, aquele do qual não se extrai essa titularidade por conta da utilização de técnicas razoáveis de anonimização (inciso III do mesmo artigo).

Os conceitos de anonimato e anonimização, embora próximos, não possuem o mesmo significado[6]. No anonimato, esforços concretos para que a identidade de um sujeito não seja revelada são tomados de antemão. Ao navegar no *Tor*[7] ou ao transacionar uma criptomoeda como o *Monero*, por exemplo, o próprio usuário, deliberadamente, deseja proteger a sua identidade de terceiros. Há, portanto, um esforço prévio e por parte do próprio titular da informação. Se bem arquitetada, a reversão desse expediente para a identificação do envolvido é muito difícil[8].

Na anonimização de dados, porém, os procedimentos técnicos razoáveis para retirar o vínculo do dado a um titular são tomados *a posteriori* e por parte de um terceiro, controlador ou operador dos dados. A identidade do titular é conhecida e o que se deseja fazer é tratar esse dado de maneira que inferências ou assunções sobre essa titularidade não possam ser realizadas. Há, portanto, um esforço posterior de romper o vínculo entre o dado e seu respectivo titular[9], por parte de um terceiro, o agente de tratamento, ainda que, após a anonimização ele perca a capacidade de identificação razoável do titular. Mesmo se bem arquitetada, a reversão desse expediente para a reidentificação do envolvido ainda é possível[10].

Exemplo notório é o caso *Netflix Prize* e consoante o qual, lançado concurso pela Netflix para

---

[4] DONEDA, Danilo. A proteção de dados em tempos de coronavírus. **JOTA**, São Paulo, 25 mar. 2020. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020>. Acesso em 27 abr. 2020.

[5] MENDES, Laura Schertel. Privacidade e dados pessoais. **Panorama setorial da Internet**, [s.l.], n. 2, a. 11, p 1-7, jun. 2019. p. 2. Discorre a autora que "por a LGPD se basear em um conceito amplo de dado pessoal, a princípio todo tratamento de dados – realizado tanto pelo setor público quanto pelo privado – está submetido a ela".

[6] MUNCHBACK, Cory. Data anonymization vs anonymous data. **Blueconic**. Disponível em <https://www.blueconic.com/blog/data-anonymization/>. Acesso em 25 fev. 2020.

[7] CHEIN FERES, Marcos; OLIVEIRA, Jordan. Dos Códigos Legais aos Códigos do Ciberespaço: Reflexões sobre Direito e Deep Web. **Revista de Propriedade Intelectual - Direito Constitucional e Contemporâneo**, Aracaju, v. 11, n. 2, p. 234-253, jun. 2017. O *Tor Browser* é um navegador de internet distinto dos comumente utilizados, como o *Google Chrome* ou o *Mozilla Firefox*. Enquanto nestes os atributos individuais que possibilitam a identificação do internauta costumam estar visíveis (como o histórico, os *cookies* de navegador, o número de IP, a resolução de tela ou o nome do usuário), naquele navegador as informações passam por um processo de proteção graças a recursos como a criptografia e o uso de *plugins* contra o rastreamento *online*.

[8] Id.

[9] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018. p. 104.

[10] LUBARSKY, Boris. Re-Identification of "Anonymized Data". **Georgetown Law Technology Review**, Washington, v. 1, n. 1, p. 202-213, 2017.

aprimorar seu algoritmo de sugestões de filmes, a plataforma de *streaming* disponibilizou sua base de dados com as avaliações dos filmes catalogados entre 1998 a 2005, suprimindo os nomes dos usuários e mantendo apenas a data e a nota da avaliação. Rodando o algoritmo por eles desenvolvido e cruzando as informações disponibilizadas pela Netflix com aquelas disponíveis na *Internet Movies Databases* (IMDB) – *website* que conta com avaliações de filmes por usuários, que incluem os nomes dos avaliadores –, os pesquisadores Arvind Narayan e Vitaly Shmatikov[11] correlacionaram as datas das avaliações, os filmes e as respectivas notas e desvendaram os nomes dos usuários suprimidos da plataforma Netflix[12]. Por isso o inciso III do artigo 5º da LGPD alude a "meios técnicos razoáveis e disponíveis na ocasião".

Mas e o que seriam os procedimentos técnicos razoáveis? Em estudo conduzido pelo Grupo de Trabalho de Proteção de Dados do Artigo 29[13], a questão fica melhor delimitada. São apontadas duas grandes famílias de técnicas para a anonimização de dados: a randomização e a generalização.

Nas técnicas de randomização, busca-se alterar a veracidade de um dado pessoal de modo que se dificulte a sua associação a um indivíduo. A adição de ruído é um exemplo: por essa técnica, os atributos de um dado são modificados para fazê-lo menos precisos, como arredondar a altura de uma pessoa para a casa de centímetros mais próxima. Nas técnicas de generalização, busca-se modificar as escalas ou magnitudes de um dado pessoal. Aqui, a técnica de *k-anonimato* é um exemplo: por essa técnica, os dados de um indivíduo são agrupados junto a um número pré-definido de outros indivíduos, ou *k-indivíduos,* como revelar dados de endereço por CEP de macrorregiões em vez de dados que identifiquem determinada rua[14].

O referido Grupo de Trabalho deixa, ainda, clara a distinção entre anonimização e pseudoanonimização, a qual será de especial proveito para este artigo. Na pseudoanonimização um atributo de identidade é substituído por um outro elemento inicialmente a ela desconectado, como um código ou uma função. Como um dado pseudoanonimizado pode ser cruzado junto a outras informações, como um número de CPF com as informações de data de nascimento, de endereço ou de filiação para descobrir quem é o titular desse número, o estudo do Conselho Europeu aponta que o recurso da pseudoanonimização é mera técnica adicional de segurança da informação e não se equipara à anonimização[15].

Feitos esses esclarecimentos, o momento é pertinente para elucidar qual o conceito de anonimato nos ambientes digitais, a ser utilizado para este estudo. Deve-se, de início, ter em mente que duas nuances interferem fortemente no uso dessa expressão: o estado da arte de soluções tecnológicas e a compreensão social desses fenômenos.

O anonimato deve ser compreendido de maneira fluida e transicional nas interações *online* entre

[11] NARAYAN, Arvind; SHMATIKOV, Vitaly. **Robust de-anonymization of large sparse datasets**. Disponível em <https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>. Acesso em 27 abr 2020.

[12] O exemplo é citado por BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018. p. 107-108.

[13] UNIÃO EUROPEIA. **Parecer 05/2014 sobre técnicas de anonimização**. p. 11-12. Grupo de Trabalho de Proteção de Dados do Artigo 29. Adotado em 10 de abril de 2014. Disponível em <https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf>. Acesso em 03 set. 2019.

[14] Id. p. 16-7.

[15] Id. p. 20-3.

indivíduos e não de forma absoluta ou estática. Trata-se de um mecanismo apercebido ao mesmo tempo por expedientes técnicos, como aplicações de criptografia ou o navegador *Tor*, e por expedientes sociais, como a cobertura da mídia ou a opinião de políticos sobre o tema[16]. Dessa maneira, fala-se em múltiplos anonimatos e, não raro, o uso da expressão é equivocada: vê-se anonimato em situações nas quais ele inexiste[17]. Assim, o conceito de anonimato utilizado para este estudo está contido em Wu[18], ao afirmar que o anonimato é viabilizado em concreto quando duas circunstâncias são atingidas: o pseudoanonimato e a desassociação ou *unlinkability*.

O pseudoanonimato significa que a real identidade do emitente de uma mensagem ou de uma transação não está revelada. Para o caso das criptomoedas, esse fenômeno indica que o endereço das chaves públicas[19] não revela, de início, a identidade da parte envolvida na transação. A desassociação, por sua vez, denota que não somente essa identidade não foi revelada em um primeiro momento, mas a sua descoberta concreta é difícil ou improvável. Assim, o nome das partes e mesmo as quantias transacionadas deveriam ser protegidas para que o anonimato seja proporcionado de forma concreta.

A grande maioria das criptomoedas possui apenas o atributo do pseudoanonimato por não associar, de imediato, a identidade dos sujeitos participantes de uma transação. O requisito da desassociação, contudo, é poucas vezes atendido em concreto, como se verá no próximo tópico desta seção.

As criptomoedas entre o anonimato e o pseudoanonimato

Embora ancorada em uma série de conceitos técnicos desenvolvidos anteriormente, a veiculação de uma ideia completa e executável de uma criptomoeda é creditada à publicação de um artigo[20], assinado por Satoshi Nakamoto, em 2008. Nele, Nakamoto apresenta os elementos necessários para o funcionamento

[16] SARDÁ, Thais et al. Understanding online anonymity. **Media, Culture & Society**, London , v. 41, n. 4, p. 557-564, 2019.

[17] O aplicativo *Secret*, por exemplo, foi compreendido socialmente e pela mídia como viabilizador de mensagens anônimas pelo mero fato de que um nome não era associado às mensagens difundidas em seu âmbito. *V.* CARPANEZ, Juliana. Aplicativo Secret cria polêmica ao permitir postagem anônima de 'segredos'. **Tilt**: o canal de tecnologia do UOL, São Paulo, 13 ago. 2014. Disponível em <https://www.uol.com.br/tilt/noticias/redacao/2014/08/13/secret-cria-polemica-ao-prometer-anonimato-acao-visa-proibir-o-aplicativo.htm>. Acesso em 15 fev. 2020. Ocorre que os elementos subjacentes como IP, porta lógica, dispositivo informático e registro, que tornam a identificação do emitente da mensagem possível, não passavam, nem de perto, por qualquer procedimento para assegurar esse anonimato. *V.* POULSEN, Kevin. Your Anonymous Posts to Secret Aren't Anonymous After All. **Wired**, [s.l.], 22 ago. 2014. Disponível em <https://www.wired.com/2014/08/secret/>. Acesso em 15 fev. 2020.

[18] WU, Wai. **Limitations of privacy guarantees in cryptocurrencies**. Thesis (EAS 499 Senior Capstone Thesis) – School of Engineering and Applied Science, University of Pennsylvania. Pennsylvania, 25 abr. 2018. p. 5. Disponível em <https://www.cis.upenn.edu/~fbrett/theses/wai_wu.pdf>. Acesso em 22 fev. 2020.

[19] O esquema criptográfico de endereçamento de registros no Blockchain é organizado pelo que se chama de criptografia assimétrica. Na criptografia simétria, seu oposto, uma mesma chave (ou senha) é utilizada para codificar e descodificar uma mensagem ou uma transação. Na criptografia assimétrica, em contrário, a chave pública serve para a identificação e o endereçamento do destinatário, enquanto a chave privada é mantida em segredo para validar as transações. *V.* PAL, Om et al. Key management for blockchain technology. **ICT Express**. [s.l.], 21 ago. 2019. Disponível em < https://www.sciencedirect.com/science/article/pii/S2405959519301894>. Acesso em 20 fev. 2020. Uma analogia útil para compreender a criptografia assimétrica se dá pela visualização da chave pública como endereço de uma residência, enquanto a chave privada contém o segredo para abrir a caixa de correio. Assim, embora a chave pública possa ser revelada de maneira segura, a validação da operação permanece na chave privada.

[20] NAKAMOTO, Satoshi. **Bitcoin: a peer-to-peer eletronic cash system**. Bitcoin.org, 2008.

de uma moeda virtual na qual a confiança em uma autoridade central para gerir e certificar transações é substituída por um sistema de registros transparente e descentralizado. A esse sistema de registros subjacente, ou livro-razão digital, deu-se o nome de *Blockchain*, enquanto a moeda virtual por ele viabilizada foi apresentada como *Bitcoin*. Transcorrida mais de uma década, a identidade de Nakamoto segue desconhecida[21] e mais de 2 (duas) mil criptomoedas com diferentes arquiteturas foram lançadas[22].

Nesse contexto, muito tem se discutido acerca da natureza jurídica das criptomoedas. Com efeito, questiona-se se, sob o espectro do ordenamento jurídico nacional, seria possível enquadrar criptomoedas, como o Bitcoin, no conceito de moedas. Para se responder a essa pergunta é necessário pontuar que o Código Civil brasileiro confere, em seus artigos 315 e 318, dois atributos essenciais às moedas para que possam ser juridicamente assim caracterizadas: curso legal forçado e poder liberatório. Por curso legal forçado, entende-se a imposição, pelo Estado, de utilização de uma moeda como meio de pagamento nas obrigações submetidas às suas leis. Por poder liberatório, entende-se a garantia, pela lei, de que qualquer obrigação estabelecida em moeda estatal poderá ser extinta mediante entrega da respectiva quantidade em dinheiro. Além disso, por força de norma constitucional, são emitidas e controladas única e exclusivamente pelo Banco Central[23].

Nesse cenário, as restrições legais contidas no ordenamento jurídico brasileiro inviabilizam a sua definição como moeda na acepção jurídica, haja vista não possuírem curso legal forçado, não contarem com uma autoridade central, mas com uma estrutura descentralizada, além da ausência de previsão legal expressa nesse sentido. Ademais, as criptomoedas ainda não contam com ampla utilização e aceitação.

Sendo assim, parece que a concepção mais adequada é a de que as criptomoedas consistem em bens móveis incorpóreos cuja finalidade é servir como meio de troca, por meio de uma rede descentralizada que garante maior segurança e redução de custos nas transações financeiras[24]. Diante disso, as obrigações decorrentes das relações jurídicas que envolvem a troca de criptomoedas podem ser classificadas como obrigações de dar bens móveis cuja fungibilidade é discutível, como se verá mais à frente neste artigo.

Feito este breve panorama, cabe destacar que do desenvolvimento do *Bitcoin* acompanhou-se uma verdadeira montanha russa em termos de ânimos e desilusões com as criptomoedas. Da ascensão à desesperança, ou melhor, da *hype* ao *flop*[25] no jargão moderno, muito se tem discutido sobre as possíveis aplicações da tecnologia de registros distribuídos *Blockchain*.

---

[21] Mais detalhes sobre a possível identidade de Nakamoto podem ser acompanhados pela sua entrada, devidamente atualizada e referenciada colaborativamente na Wikipedia. *V*. WIKIPEDIA. Satoshi Nakamoto. **Wikipedia, the free encyclopedia**. Disponível em <https://en.wikipedia.org/wiki/Satoshi_Nakamoto>. Acesso em 03 fev. 2020.

[22] COINMARKETCAP. **All cryptocurrencies**. Disponível em <https://coinmarketcap.com/all/views/all/>. Acesso em 20 fev. 2020.

[23] **BRASIL**. Constituição da República Federativa do Brasil de 1988. Brasília, Diário Oficial da União: 05 de out. 1988. Art. 164. A competência da União para emitir moeda será exercida exclusivamente pelo Banco Central.

[24] No mesmo sentido NAKAMURA, Pâmela Naomi. **Desmistificando o bitcoin**: análise da sua natureza jurídica, uso e impactos. Monografia (LLM) – Programa de Pós Graduação em Direito do INSPER. São Paulo, 2017. p. 23.

[25] Como bem pontua Ronaldo Lemos, as fortes emoções envolvendo as redes descentralizadas levaram alguns a apontá-las como solução para quase todos os problemas e, tempos após, a questionar a sua aplicabilidade prática. *v*. LEMOS, Ronaldo. Reconhecimento facial é o novo normal. Seção reader. **Folha de São Paulo**, São Paulo, 19 de agosto de 2019. Disponível em <https://www1.folha.uol.com.br/colunas/ronaldolemos/2019/08/reconhecimento-facial-e-o-novo-normal.shtml>. Acesso em 25 fev. 2020.

No presente tópico, o aspecto central a ser discutido decorre do *status* de anonimato conferido por algumas criptomoedas. Antes, contudo, é necessário compreender que a relação entre dinheiro e o anonimato não é um fenômeno novo. Antes das moedas digitais, as próprias moedas impressas por bancos centrais também foram observadas sob o prisma do anonimato.

Imagine que você possua, neste momento, uma nota de 100 (cem) reais em sua mão, já gasta pelo tempo. Para além da felicidade momentânea desse pequeno exercício mental, é muito improvável que você se questione acerca da identidade dessa nota, ou seja, sobre o seu passado, a quem ela pertenceu ou em quais tipos de transação foi envolvida. Pelo seu caráter fluido e facilmente transacionável, essa nota de 100 reais é dotada de fungibilidade – facilidade de troca de unidades de valor equivalentes – em relação às partes que a utilizaram ou às mercadorias negociadas no passado. Dessa facilidade de troca não restrita a uma identidade específica, observa-se a propriedade do anonimato da moeda.

Ocorre que, como explica Berg, a relação entre identidade, fungibilidade e anonimato é fluida e possui especificidades para o caso de moedas virtuais[26]. Ao contrário do que comumente é difundido[27], a maioria das criptomoedas atualmente em uso, como o *Bitcoin*, não são dotadas de anonimato, mas apenas de um pseudoanonimato.

De modo geral, as transações ocorridas e registradas na *Blockchain* revelam três componentes: os endereços de quem envia, de quem recebe e a quantia transacionada[28]. A destinação de uma criptomoeda depende, portanto, do esquema de direcionamento provido a partir das chaves públicas pertencentes aos sujeitos participantes de uma transação. E embora essas chaves não necessariamente possuam um nome associado, é possível cruzar uma série de informações, como os *cookies* de computador[29], os endereços de IP[30], as informações de *login* e o histórico das transações para se revelar as identidades dos sujeitos envolvidos nas transações de criptomoedas. Caso a identidade da moeda possa ser rastreada, poderá haver um efeito imediato de prejuízo em sua credibilidade, o que, por sua vez, levará à queda do anonimato e à impossibilidade de sua troca[31].

---

[26] BERG, Alastair. The identity, fungibility and anonymity of money. Economic papers, forthcoming. **Social Science Research Network**, [s.l.], v. 39, n. 02, p. 104-117, nov. 2019.

[27] SIMEÃO, Álvaro; VARELLA, Marcelo Dias. A impossibilidade de regulação jurídica nacional do blockchain: rumo à um direito criptográfico? **Revista de Direitos Culturais**, Santo Ângelo, v. 13, n. 31, p. 43-70, 2018.

[28] FAUZI, Muhammad Reza Rizky; NASUTION, Surya Michrandi; PARYASTO, Marisa W. Implementation and analysis of the use of the blockchain transactions on the workings of the bitcoin. **6th International Conference on Mechatronics** – ICOM'17 IOP Publishing, 2017. Disponível em <doi:10.1088/1757-899X/260/1/012003>. Acesso em 03 fev. 2020.

[29] OLIVEIRA, Jordan Vinícius de; SILVA, Lorena Abbas da. Cookies de navegador e história da internet: desafios à lei brasileira de proteção de dados pessoais. **Revista de Estudos Jurídicos**, Franca, a. 22, n. 36, p. 307-338, jul./dez. 2018. *Cookies* de navegador são arquivos depositados por um servidor (página de acesso) no computador de um cliente (usuário internauta) para facilitar e "recordar" de alguns atributos da interação entre ambos.

[30] LESSIG, Lawrence. **Code (version 2.0)**. New York: Basic Books, 2006. Disponível em <http://codev2.cc/download+remix/>. Acesso em 20 fev. 2020. *Internet Protocol* é um elemento componente da camada de endereçamento da web (*internet layer*), responsável por atribuir uma espécie de número de identificação aos dispositivos conectados em rede. De forma análoga, o protocolo de rede funciona como uma espécie de endereço, permitindo o encaminhamento de pacotes de dados na transmissão de informações pela rede.

[31] BERG, Alastair. The identity, fungibility and anonymity of money. Economic papers, forthcoming. **Social Science Research Network**, [s.l.], v. 39, n. 02, p. 104-117, nov. 2019. Berg cita justamente o caso do Bitcoin para demonstrar a interdependência

Essa característica específica do *Bitcoin* e de tantas outras criptomoedas afeta diretamente a percepção dos usuários acerca da propriedade de anonimato ou, no caso, do pseudoanonimato da moeda. No estudo relatado por Fabian e Ermakova[32], as preocupações de um grupo de usuários de *Bitcoin* com o seu anonimato – entendido como a habilidade de identificar certa parte em uma transação – atingiram níveis considerados medianos a altos em 70% dos casos[33].

Ao mesmo passo em que preocupações sobre anonimato e a moeda *Bitcoin* começam a surgir, Gaihre, Luo e Liu constataram que, faticamente, os usuários dessa criptomoeda dificilmente se preocupam com alguns indicadores objetivos[34] capazes de resguardar ou proteger a sua identidade quando da sua utilização. No estudo, os autores relatam que, além de não ser uma moeda anônima (mas pseudoanônima), o *Bitcoin* é subutilizado quanto aos seus recursos de proteção da identidade.

Diante dessa demanda por anonimato, algumas moedas virtuais foram inseridas no mercado com o intuito de proteger a identidade das partes envolvidas em uma transação. Para o escopo desse estudo, três criptomoedas foram escolhidas[35] para análise, levando-se em consideração a sua estrutura em torno do anonimato, bem como o fato de poderem ser negociadas diretamente no Brasil por intermédio de uma *Exchange*[36] brasileira[37]. Tais moedas são o *Zcash*, o *Dash* e o *Monero*.

Começando pelo *Zcash*, essa moeda foi lançada em 2016 e tem como maior atributo técnico o emprego do método criptográfico de Prova de Conhecimento-Nulo – *Zero-Knowledge Proof* – conhecido

entre esses elementos de identidade, fungibilidade e anonimato. No caso do mercado digital e paralelo de negociação de substâncias ilícitas conhecido como *Silk Road*, por exemplo, a identidade de cerca de 700 (setecentas) mil unidades de Bitcoin foram rastreadas pelo FBI, o que prejudicou diretamente na sua fungibilidade e aceitabilidade.

[32] FABIAN, Benjamin; ERMAKOVA, Tatiana; SANDER, Ulrike. Anonymity in bitcoin? – the users' perspective. **Thirty Seventh International Conference on Information Systems**, Dublin, 2016. Disponível em <Thirty Seventh International Conference on Information Systems, Dublin 2016>. Acesso em 10 fev. 2020.

[33] Id. O estudo não possuía intenções probabilísticas e foi realizado com 125 (cento e vinte e cinco) usuários ativos de Bitcoin, cujos perfis eram variados.

[34] GAIHRE, Anil; LUO, Yan; LIU, Hang. Do bitcoin users really care about anonymity? An analysis of the bitcoin transaction graph. **2018 IEEE International Conference on Big Data (Big Data)**, nov. 2018. Disponível em <10.1109/BigData.2018.8622442>. Acesso em 03 fev. 2020. O estudo foi desenvolvido por meio de análise objetiva de mais de 321 (trezentos e vinte e um) milhões de transações registradas na Blockchain, avaliando indicadores como a troca constante das chaves públicas, a transferência constante de recursos para uma conta-mestra (zero balance account) e a deixa de elementos indicadores da propriedade da carteira virtual.

[35] O critério utilizado para a escolha das três moedas foi a sua capitalização de mercado superior à casa de 1 (um) bilhão de dólares, a partir do ranking do CoinMarketCap à data de 25 de fevereiro de 2020. *V.* COINMARKETCAP. **Top 100 cryptocurrencies by market capitalization**. Disponível em <https://coinmarketcap.com/>. Acesso em 25 fev. 2020.

[36] CUNHA FILHO, Marcelo de Castro. Bitcoin: uma tentativa de construção da confiança por meio da tecnologia. **Revista de Informação Legislativa**, Brasília, v. 56, n. 221, p. 37-60, jan./mar. 2019. p. 53. *Exchanges* ou casas de câmbio são instituições que se inserem na cadeia de movimentação de criptomoedas facilitando o gerenciamento dessas moedas e a relação entre vendedores e compradores, bem como a sua troca por unidades de moeda nacionais com curso forçado, como o real ou o dólar.

[37] BRAZILIEX. Como comprar altcoin com real?. **Frequently asked questions**, 25 fev. 2020. Disponível em <https://braziliex.com/faq/como-comprar-altcoin-com-real-eth-ltc-usdt-xrp-entre-outras/327>. Acesso em 25 fev. 2020. Nota: outras exchanges nacionais foram consultadas, mas não apresentavam concomitantemente em sua cartela de produtos as três moedas. Os autores não receberam qualquer incentivo ou patrocínio para mencionar a *Exchange* em questão, não havendo qualquer conflito de interesse no estudo.

como *zk-SNARKs*. Esse método assegura que a veracidade de uma informação possa ser atestada sem que maiores detalhes precisem ser revelados e, para a criptomoeda em questão, serve para proteger o sigilo das informações envolvidas nas transações, assegurando apenas a sua autenticidade. Como essa prova de conhecimento é um atributo que pode ou não ser utilizado, os usuários podem realizar operações de quatro tipos básicos: privadas, públicas, blindadas e desblindadas. Uma transação privada decorre de dois endereços que desejam se proteger (transferência entre dois *endereços-z*), enquanto uma transação pública decorre de dois endereços públicos transparentes (transferência entre dois *endereços-t*). As transações blindadas, por sua vez, envolvem um endereço público e um endereço privado (transferência de um *endereço-t* para um *endereço-z*), enquanto as transações desblindadas fazem o movimento inverso (transferência de um *endereço-z* para um *endereço-t*)[38].

Em seu estudo empírico das operações realizadas no âmbito do *Zcash*, Kappos explica que, não obstante a disponibilização do recurso de proteção à identidade de seus usuários, mais de 73,5% (setenta e três vírgula cinco por cento) das transações ocorridas na plataforma são transparentes, enquanto apenas 0,3% (zero vírgula três por cento) das transações são efetivamente privadas. As constatações do autor são de que, portanto, pouquíssimos dos participantes dessa rede se beneficiam dos atributos de anonimato por ela propiciados[39].

Por sua vez, a moeda *Dash*, lançada em 2014, possui um recurso conhecido como Envio Privado, pelo qual a parte interessada pode mixar a denominação da unidade da moeda a ser transacionada junto a outros possíveis participantes da rede. A operação funciona da seguinte maneira: todas as carteiras (repositórios virtuais individuais de gerenciamento de criptoativos) possuem uma denominação, geralmente atrelada à chave pública do usuário e que não guarda necessária dependência com os fundos depositados na carteira, ou seja: uma alteração na denominação não implica em perda dos fundos do usuário. No caso do *Dash*, ocorre uma mixagem das denominações de carteiras individuais agrupadas (nas operações de mixagem elas são agrupadas por tipos como 0.01 *Dash*, 0.1 *Dash*, 1 *Dash*, 10 *Dash*), dificultando a descoberta da origem de uma transação. Dessa maneira, o usuário interessado em realizar uma transação privada faz a requisição de mixagem da denominação originária de seus fundos a um ponto de gestão descentralizado da rede (chamado de *Masternode* ou Nó-Mestre) o qual, por sua vez, "abre uma chamada" em busca de no mínimo mais dois usuários com o mesmo desejo e agrupamento. Uma vez reunidos os *inputs* de usuários, há uma operação de mixagem de suas denominações e uma instrução individualizada às carteiras para utilizarem aquele novo tipo de denominação criada. A operação é repetida por mais algumas vezes até tornar difícil a descoberta da origem dos fundos por um terceiro observador[40].

Como expressam Biryukov e Tikhomirov, tal como na moeda *Zcash*, o *Dash* implementa operações de proteção à identidade de maneira opcional. Dessa forma, caso o usuário não opte por usar o recurso de Envio Privado, será fácil rastrear a origem de uma transação com essa moeda[41]. Ademais, ainda que

[38] ZCASH. **How it works**. Disponível em <https://z.cash/pt/technology/>. Acesso em 25 fev. 2020.

[39] KAPPOS, George. et al. An empirical analysis of anonymity in zcash. **27th USENIX Security Symposium**, dez. 2017. Disponível em <https://www.researchgate.net/publication/327529465_An_Empirical_Analysis_of_Anonymity_in_Zcash>. Acesso em 14 fev. 2020.

[40] DASH. **Frequently asked questions**. Disponível em <https://www.dash.org/faq/>. Acesso em 25 fev. 2020.

[41] BIRYUKOV, Alex; TIKHOMIROV, Sergei. Deanonymization and Linkability of Cryptocurrency Transactions Based on

o usuário opte por este recurso, o destinatário da sua transação estará sempre visível, já que o foco da tecnologia está na obscurização da parte responsável pela sua origem[42].

Por fim, com relação ao *Monero*, essa criptomoeda criada em 2014 recebeu implementações de privacidade obrigatórias em 2017 e reúne três elementos em busca do anonimato: assinaturas em anel (*Ring Signatures*), endereços sigilosos (*Stealth Addresses*) e transações confidenciais em anel (*Ring Confidential Transactions*, ou *Ring CTs*). As assinaturas em anel asseguram que a identidade do usuário emitente de uma transação seja mantida em sigilo por meio de uma combinação da sua assinatura com as assinaturas de outros possíveis emitentes. Assim, a tecnologia valida a transação, mas inviabiliza que um terceiro compreenda qual a origem do fluxo da moeda, uma vez que a assinatura é feita em bloco. Por sua vez, os endereços sigilosos cuidam da proteção dos destinatários, removendo as associações ou links de saída das operações. Já as transações confidenciais em anel cuidam do sigilo da quantia envolvida na operação, tornando possível a um terceiro apenas atestar a validade da operação, sem distinguir o quanto foi efetivamente enviado e recebido. Em conjunto, essas três propriedades asseguram a constante fungibilidade do *Monero*, fazendo com que os dados de uma transação fiquem restritos apenas às partes interessadas e não a terceiros[43].

Como explicam Biryukov e Tikhomirov[44], o ponto forte do *Monero* é a utilização de mecanismos de proteção das transações como padrão (*privacy by default*), sem que o usuário precise optar por esses atributos. Ademais, dado o alto padrão de anonimato da tecnologia, propõe-se uma nova versão da moeda, o *Traceable Monero* (Monero Rastreável), diante da preocupação de sua utilização para os fins de operações ilícitas, de modo a equilibrar a privacidade do *Monero* com uma Autoridade Rastreadora (*Traceable Authority*), capaz de revogar o anonimato em situações que envolvam comportamentos ilegais[45].

Apresentadas as propriedades dessas três criptomoedas com pretensões de anonimato, faz-se pertinente avaliar, por fim, as possíveis desvantagens e vantagens em seu uso. Começando pelos pontos negativos, Houben e Snyers elencam três importantes argumentos em desfavor do anonimato em criptomoedas: lavagem de dinheiro, terrorismo e evasão fiscal[46]. Para os autores, uma vez que uma operação financeira ou as suas partes estejam cobertos pelo manto do anonimato, a dificuldade de monitorar essas transações e combater a lavagem de dinheiro e o financiamento de ações terroristas se torna maior. Com relação à evasão fiscal, o anonimato pode inviabilizar a detecção de operações financeiras tributáveis e a

Network Analysis. **2019 IEEE European Symposium on Security and Privacy (EuroS&P)**. May 2019. Disponível em <DOI: 10.1109/EuroSP.2019.00022>. Acesso em 13 fev. 2020.

[42] DASH. **PrivateSend**. Dash Documentation. Disponível em <https://docs.dash.org/en/stable/introduction/features.html#privatesend>. Acesso em 24 fev. 2020.

[43] MONERO. **Frequently asked questions**. Disponível em <https://web.getmonero.org/get-started/faq/>. Acesso em 23 fev. 2020.

[44] BIRYUKOV, Alex; TIKHOMIROV, Sergei. Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis. **2019 IEEE European Symposium on Security and Privacy (EuroS&P)**. May 2019. Disponível em <DOI: 10.1109/EuroSP.2019.00022>. Acesso em 13 fev. 2020.

[45] LI et. al. Traceable Monero: anonymous cryptocurrency with enhanced accountability. **Future Generation Computer Systems**, [s.l.], v. 101, p. 29-38, 2019. Disponível em <https://doi.org/10.1016/j.future.2019.05.081>. Acesso em 14 fev. 2020.

[46] HOUBEN, Robby; SNYERS, Alexander. Cryptocurrencies and blockchain legal context and implications for financial crime, money laundering and tax evasion. **European Parliament TAX3 Committee Study**. Disponível em <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%>. Acesso em 13 fev. 2020.

respectiva sanção para o não pagamento destes tributos[47].

Wu, em contrapartida, enfatiza a necessidade de se balancear estes aspectos negativos com alguns dos benefícios trazidos pelo anonimato para as esferas do usuário, do consumidor e para as perspectivas filosófica e constitucional. Na perspectiva do usuário, já há uma certa expectativa de anonimato e privacidade em relação às criptomoedas, de modo que a mera entrega do pseudoanonimato pode se revelar prejudicial ou insatisfatória sob o ponto de vista da proteção de transações na internet. Na ótica do consumidor, ele argumenta que a disponibilização de um histórico de transações virtuais ao público pode afetar o titular da conta, dada a sua exposição a ataques de inferência sobre sua renda, seus gostos de consumo, a discriminação de preços ou até a superexposição a anúncios. Em um prospecto mais amplo, sob o panorama filosófico é possível apontar que as criptomoedas visam justamente a assegurar que o poder monetário não fique concentrado nas mãos de poucas empresas gigantes da tecnologia, assegurando assim uma infraestrutura descentralizada e segura para transações privadas. Pelo olhar constitucional, aqueles autores pontuam que o direito fundamental à privacidade deve ser assegurado em face de governos cada vez mais paternalistas e suas intromissões na liberdade econômica individual[48].

Como visto, a noção de anonimato não pode ser absoluta e precisa levar em conta todas as possíveis nuances concretas[49]. Para o caso das criptomoedas, o fato técnico é que *Monero*, *Zcash* e *Dash* oferecem ferramentas concretas com diferentes graus de proteção de maneira acessível a qualquer interessado. Nesse sentido, a próxima seção pretende avaliar qual o cenário regulatório que essas moedas enfrentam diante das normativas nacionais sobre criptomoedas.

A regulação de criptomoedas entre e o anonimato e o pseudoanonimato

É inegável que o fenômeno das criptomoedas tem demandado, ao redor do mundo, certo esforço regulatório na tentativa de lidar com os impactos do uso de tais tecnologias nos mais diversos setores, especialmente no mercado monetário, de capitais, de câmbio e no âmbito fiscal[50].

Quando do aumento de sua popularidade, uma das maiores preocupações dos bancos centrais mundiais, inclusive do Banco Central do Brasil (Bacen), foi a de emitir comunicados oficiais alertando sobre os riscos das operações com criptomoedas.

Nessa linha, em 19 de fevereiro de 2014, o Bacen emitiu o Comunicado nº 25.306, por meio do qual, dentre outras questões, advertiu que as chamadas "moedas virtuais" não eram garantidas por autoridade monetária, tampouco possuíam "garantia de conversão para a moeda oficial", de modo que "todo o risco de sua aceitação" estaria "na mão dos usuários". Alertou, ainda, para a alta volatilidade dos preços de tais

[47] Id.

[48] WU, Wai. **Limitations of privacy guarantees in cryptocurrencies**. Thesis (EAS 499 Senior Capstone Thesis) – School of Engineering and Applied Science, University of Pennsylvania. Pennsylvannia, 25 abr. 2018. p. 24-25. Disponível em <https://www.cis.upenn.edu/~fbrett/theses/wai_wu.pdf>. Acesso em 22 fev. 2020.

[49] SARDÁ, Thais et al. Understanding online anonymity. **Media, Culture & Society**, London, v. 41, n. 4, p. 557-564, 2019.

[50] A esse respeito, vide pesquisa desenvolvida pelo Law Library of Congress, Global Research Center disponível em <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf >. Acesso em 05.02.2020.

ativos – o que poderia acarretar relevantes perdas patrimoniais para seus detentores. O teor do alerta demonstra que a autoridade monetária apresentou certa reserva quanto à utilização das criptomoedas, na medida em que – muito provavelmente por conta de questões relacionadas aos atributos de anonimato e pseudoanonimato de algumas delas – advertiu, de forma expressa, sobre a possibilidade de seu emprego em atividades ilícitas.

Pouco mais de três anos depois – em razão do crescente interesse dos agentes econômicos pelo mercado de criptoativos e do surgimento de diversas novas espécies de criptomoedas, tais como o *Monero* e o *Zcash* –, o Banco Central emitiu, em 16 de novembro de 2017, novo comunicado reiterando as considerações trazidas no alerta anterior sobre os riscos relacionados a tais operações[51]. Na ocasião, aproveitou-se para esclarecer, ademais, que as operações com criptoativos que acarretassem "transferências internacionais referenciadas em moedas estrangeiras" deveriam necessariamente observar as normas cambiais, notadamente a obrigatoriedade de realizar tais transações por meio de instituições autorizadas pelo Bacen a operar no mercado de câmbio.

Mais recentemente, em 3 de maio de 2019, a Secretaria Especial da Receita Federal inaugurou, no Brasil, a primeira regulamentação sobre o tema. A Instrução Normativa RFB nº 1.888, editada pelo órgão, passou a instituir a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos. Em vigor desde 1º de agosto de 2019, a regulamentação exige que as transações com criptoativos – incluindo-se aí operações de compra e venda, permuta, doação, empréstimo, dação em pagamento e outras que impliquem transferência de criptoativos –, realizadas pela via de *exchanges* de criptoativos[52] domiciliadas no Brasil, sejam informadas à Receita Federal, por meio de formulário próprio, até o último dia do mês subsequente às transações realizadas[53].

Quando as operações forem realizadas pela via de *exchanges* domiciliadas no exterior ou fora do ambiente de bolsa, como pela via P2P[54], a obrigação de informar recai sobre as pessoas físicas ou jurídicas domiciliadas no Brasil que efetuarem tais transações. Nessa hipótese, impõe-se que o dever de informação se torna exigível sempre que o valor mensal das operações, de forma isolada ou conjunta, ultrapassar R$ 30.000,00[55]. A Instrução Normativa RFB nº 1.888 impõe que sejam prestadas informações extremamente detalhadas acerca das operações com criptomoedas. Com efeito, devem constar (i) a data da operação;

[51] **BACEN.** Comunicado Bacen nº 31.379. Disponível em <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=31379>. Acesso em 15.02.2020.

[52] Assim definidas pela regulamentação como "a pessoa jurídica, ainda que não financeira, que oferece serviços referentes a operações realizadas com criptoativos, inclusive intermediação, negociação ou custódia, e que pode aceitar quaisquer meios de pagamento, inclusive outros criptoativos.".

[53] **BRASIL**. Instrução Normativa RFB nº 1888. Receita Federal do Brasil, 03 de maio de 2019. "Art. 6º Fica obrigada à prestação das informações a que se refere o art. 1º: I - a exchange de criptoativos domiciliada para fins tributários no Brasil; II - a pessoa física ou jurídica residente ou domiciliada no Brasil quando: a) as operações forem realizadas em exchange domiciliada no exterior; ou b) as operações não forem realizadas em Exchange".

[54] P2P ou *peer to peer* (pessoa a pessoa) é a transação que ocorre diretamente entre o emitente e o destinatário de criptomoedas, sem intermediários diretos e por meio dos endereços públicos das carteiras digitais, ou *wallets*.

[55] **BRASIL**. Instrução Normativa RFB n. 1888. Receita Federal do Brasil, 03 de maio de 2019

(ii) o tipo de operação; (iii) os criptoativos utilizados na operação; (iv) os titulares[56]; (v) a quantidade de criptoativos negociados, em unidades; e (vi) o valor da operação, em reais, excluídas as taxas de serviço cobradas, quando for o caso.

Com efeito, caso a operação seja efetuada no ambiente de bolsa, domiciliada no Brasil, ou privadamente, fora de ambiente de bolsa, a *exchange* de criptoativos ou a pessoa que realizar a transação, conforme o caso, deverá informar à Receita Federal os dados pessoais relativos aos titulares da operação. Nesse caso, deverão ser fornecidos o nome da pessoa física ou jurídica, seu endereço e domicílio fiscal, CPF e CNPJ, ou o número de identificação fiscal, em caso de residentes ou domiciliados no exterior.

A Instrução exige também que as *exchanges* de criptoativos domiciliadas no Brasil, quando da divulgação mensal das informações, forneçam, relativamente a cada usuário de seus serviços, as seguintes informações referentes a 31 de dezembro de cada ano: (i) o saldo de moedas fiduciárias, em reais; (ii) o saldo de cada espécie de criptoativos, em unidades dos respectivos criptoativos; e (iii) o custo, em reais, de obtenção de cada espécie de criptoativo, declarado pelo usuário de seus serviços, se houver.

Cumpre destacar que até a alteração promovida pela Instrução Normativa RFB nº 1.899, em 10 de julho de 2019, o normativo exigia, ainda, a indicação do endereço da *wallet* de remessa e de recebimento da transação. Nessa circunstância, a Receita Federal teria em seu poder os três componentes das operações envolvendo criptomoedas: os endereços de quem envia, de quem recebe e o valor da transação.

Em julho de 2019, contudo, o item 'h' dos incisos I e II do artigo 7º da Instrução Normativa RFB nº 1.888, que instituía tal requisito, foi revogado. Atualmente, o § 4º do mesmo dispositivo determina que a entrega das informações relativas ao endereço da *wallet* de remessa e de recebimento, se houver, será obrigatória apenas na hipótese de recebimento de intimação efetuada no curso do procedimento fiscal. Ou seja, a Receita Federal estabeleceu como padrão não informar o destinatário da transação, sendo a informação devida apenas em caso de requisição expressa por parte do órgão, provavelmente, por conta de abertura de procedimento de investigação por suspeita de irregularidade.

No entanto, dada a obrigação de usuários pessoas físicas e jurídicas residentes e domiciliadas no Brasil que transacionaram privadamente, pela via P2P, acima da faixa mínima obrigatória e das *exchanges* de criptoativos domiciliadas no Brasil declararem detalhes das operações à Receita Federal, inclusive dados de seus titulares, quantidade de criptoativos e data da operação, é possível que ao cruzar os dados fornecidos o anonimato da contraparte reste comprometido[57].

---

[56] Id. "Art. 7º Deverão ser informados para cada operação: (...) II - no caso previsto na alínea "a" do inciso II do art. 6º: a) a identificação da exchange; b) a data da operação; c) o tipo de operação, conforme o § 2º do art. 6º; d) os criptoativos usados na operação; e) a quantidade de criptoativos negociados, em unidades, até a décima casa decimal; f) o valor da operação, em reais, excluídas as taxas de serviço cobradas para a execução da operação, quando houver; g) o valor das taxas de serviços cobradas para a execução da operação, em reais, quando houver".

[57] NOVADAX. **Dúvidas sobre a declaração de criptomoedas no imposto de renda**. Disponível em https://blog.novadax.com/2020/02/11/duvidas-sobre-declaracao-de-criptomoedas-no-imposto-de-renda-2020/>. Acesso em 29 abr. 2020. Como explica a Exchange NovaDAX: "Porém, se você negocia em uma exchange internacional ou Peer to Peer (P2P) você deve declarar mensalmente caso o total negociado ultrapasse R$ 30 mil dentro do mês. Neste caso, a declaração deve ocorrer no mês seguinte as operações, na qual também deve conter a discriminação de todos os itens solicitados na Instrução Normativa RFB n. 1888".

Cumpre ressaltar que o não cumprimento das regras informacionais sujeita os infratores ao pagamento de multa, sem prejuízo da comunicação ao Ministério Público Federal caso haja indícios da ocorrência dos crimes de lavagem de dinheiro.

Interessante notar que nos dois primeiros meses de vigência do referido normativo – agosto e setembro de 2019 – as operações com criptoativos informados somaram o valor total de quase R$ 14 bilhões, evidenciando o notável interesse dos usuários nesse tipo de transação[58].

Dado o panorama regulatório das criptomoedas no Brasil, cabe indagar se a normativa vigente veda, expressamente, o atributo do anonimato ou do pseudoanonimato, conforme o caso, das transações com criptomoedas.

A resposta aqui defendida é a de que a utilização de criptomoedas com propriedades de anonimato, como o Monero, não é vedada pela ordem jurídica nacional. Com efeito, cumpre esclarecer que a vedação constitucional ao anonimato constante do artigo 5º, IV limita-se tão somente à expressão do pensamento[59] e, mesmo nesse contexto, existem importantes ressalvas que advêm de uma interpretação sistemática do texto constitucional, haja vista que, além de assegurar a liberdade de expressão, o próprio artigo 5º garante a proteção da vida privada, no inciso X, do que se depreende o direito constitucional à privacidade e protege o direito à informação e ao sigilo de fontes para o exercício profissional, em seu inciso XIV.

A despeito disso, a obrigação de declarar imposto de renda é capaz de prejudicar concretamente a expectativa de anonimato, uma vez que dados da operação, do emitente ou do destinatário da transação poderão ser compartilhados com a Receita Federal ... Nesse contexto, cabe distinguir anonimato de sigilo.

Muito embora seja possível apontar os robustos esforços de anonimato do Monero, tem-se que juridicamente as pessoas físicas e jurídicas e as exchanges legalmente vinculadas ao Erário Federal poderão revelar dados que venham a quebrar o atributo do anonimato das operações realizadas. Imagine, por exemplo, um usuário A que transacionou um valor declarável de unidades de Monero pela via de uma exchange brasileira ou pela via P2P com outro usuário brasileiro. Pela Instrução Normativa RFB nº 1.888, os dados poderão ser cruzados e a Receita Federal terá acesso aos dados da transação por um mecanismo jurídico. Esse fato revela a complexidade da relação entre direito, sociedade, mercado e tecnologia. Nesse ponto, revela-se uma nítida preocupação do regulador com a prática dos crimes de evasão fiscal, lavagem de dinheiro, entre outros mediante a realização de transações com criptomoedas, que acaba por se sobrepor aos avanços da tecnologia que viabilizam o anonimato.

Assim, diz-se que esta operação estará protegida sob a perspectiva de anonimato quanto a outros usuários da plataforma, já que a tecnologia do Monero possui uma série de atributos para manter a identidade das partes e os dados da operação seguros. No entanto, em razão das obrigações impostas pela regulamentação, a Receita poderá vir a ter acesso aos dados da transação, descortinando-se o anonimato perante o órgão, que, por outro lado, estará submetido ao sigilo constitucional e legal, com fundamento nos artigos 5º, XII da Constituição Federal e 198 do Código Tributário Nacional.

---

[58] AMATO, Fábio. Operações com criptomoedas informadas à Receita somam R$ 14 bilhões em dois meses.**G1**, Rio de Janeiro. Disponível em: <https:/g1.glo.com/economia/noticia2019/12/01/operacoes-com-criptomoedas.ghtml>. Acesso em 18.02.2020.

[59] V. OLIVEIRA, Jordan Vinícius. **O anonimato no mundo cibernético**: três mitos. 2020. No prelo.

O sigilo consiste em um compromisso de não divulgar uma informação já conhecida e, como explica Cunha e Melo, ele pode ser avaliado por dois prismas: o conteúdo da comunicação e os dados gerados para que esta comunicação se efetue[60]. Aplicada a explicação para o caso das criptomoedas, tem-se que a Receita Federal poderá vir a receber dados de transações originalmente anônimas, reveladas pelas próprias partes ou intermediários. Dessa forma, a Receita Federal passa a ser depositária dessa informação e deverá guardar o seu sigilo. Esses dados, contudo, não são mais anônimos, pois a ligação das informações a uma identidade já foi estabelecida, rompendo-se o principal atributo do anonimato.

Considerações finais

O presente artigo pretendeu analisar – sem a ousada pretensão de esgotar o tema – os atributos do anonimato e do pseudoanonimato propiciados pela tecnologia utilizada por algumas criptomoedas existentes no mercado, notadamente o *Bitcoin,* o *Monero*, o *Zcash* e o *Dash* e os eventuais desafios enfrentados diante do panorama regulatório brasileiro vigente. Embora alguns estudos empíricos[61] indiquem que, no cenário atual, poucos usuários de criptomoedas, de fato, usufruem de seus atributos de anonimato, fato é que essa característica parece ser um dos principais atrativos para a realização de transações com criptoativos, dada a proteção que visa conferir em relação a eventuais ataques de inferência sobre renda e preferências de consumo, entre outras informações pessoais.

Viu-se que, tal como no caso do dinheiro físico, o anonimato é um atributo importante interligado à identidade e, sobretudo, à fungibilidade da moeda, implicando diretamente na sua aceitação e utilização fluida na sociedade de mercado. Das quatro criptomoedas analisadas, observou-se ainda que o *Bitcoin* é dotado apenas de pseudoanonimato enquanto o *Dash*, o *Zcash* e, principalmente, o *Monero* possuem recursos técnicos de anonimato com diferentes escalas de eficiência.

Tendo sido feita, no presente artigo, a análise dos normativos vigentes no país, conclui-se não haver qualquer vedação expressa à utilização de criptomoedas que garantam o anonimato das transações de seus usuários, mas as obrigações regulamentares que impõem a comunicação mensal de informações relacionadas às transações com criptoativos à Receita Federal podem descaracterizar o atributo do anonimato conferido a algumas das criptomoedas, tais como o Monero.

A desnaturação do anonimato decorrente da possível identificação, pelo órgão, das partes e contrapartes da operação, dos valores envolvidos e do tipo de criptoativo utilizado não torna, contudo, públicas tais informações, que devem ser tratadas com sigilo pela Receita Federal, por força de normas constitucional e legal.

---

[60] CUNHA E MELO, Mariana. **Anonimato, proteção de dados e devido processo legal**: porque e como conter uma das maiores ameaças ao direito à privacidade no Brasil. ITS Rio, Rio de Janeiro, mar. 2017 Disponível em <https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf>. Acesso em 29 abr. 2020.

[61] V. KAPPOS, George et al. An empirical analysis of anonymity in zcash. **27th USENIX Security Symposium**, dez. 2017. Disponível em <https://www.researchgate.net/publication/327529465_An_Empirical_Analysis_of_Anonymity_in_Zcash>. Acesso em 14 fev. 2020.

Referências

AMATO, Fábio. Operações com criptomoedas informadas à Receita somam R$ 14 bilhões em dois meses. **G1**, Rio de Janeiro. Disponível em <https://g1.globo.com/economia/noticia/2019/12/01/operacoes-com-criptomoedas-informadas-a-receita-somam-r-14-bilhoes-em-dois-meses.ghtml>. Acesso em 18.02.2020.

BACEN. Comunicado Bacen nº 31.379. Disponível em <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=31379>. Acesso em 15.02.2020.

BERG, Alastair. The identity, fungibility and anonymity of money. Economic papers, forthcoming. **Social Science Research Network**, [s.l.], v. 39, n. 02, p. 104-117, nov. 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BIRYUKOV, Alex; TIKHOMIROV, Sergei. Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis. **2019 IEEE European Symposium on Security and Privacy (EuroS&P)**. May 2019. Disponível em <DOI: 10.1109/EuroSP.2019.00022>. Acesso em 13 fev. 2020.

BRAZILIEX. Como comprar altcoin com real?. **Frequently asked questions**, 25 fev. 2020. Disponível em <https://braziliex.com/faq/como-comprar-altcoin-com-real-eth-ltc-usdt-xrp-entre-outras/327>. Acesso em 25 fev. 2020.

CARPANEZ, Juliana. Aplicativo Secret cria polêmica ao permitir postagem anônima de 'segredos'. **Tilt**: o canal de tecnologia do UOL, São Paulo, 13 ago. 2014. Disponível em <https://www.uol.com.br/tilt/noticias/redacao/2014/08/13/secret-cria-polemica-ao-prometer-anonimato-acao-visa-proibir-o-aplicativo.htm>. Acesso em 15 fev. 2020.

CHEIN FERES, Marcos; OLIVEIRA, Jordan. Dos Códigos Legais aos Códigos do Ciberespaço: Reflexões sobre Direito e Deep Web. **Revista de Propriedade Intelectual - Direito Constitucional e Contemporâneo**, Aracaju, v. 11, n. 2, p. 234-253, jun. 2017.

COINMARKETCAP. **All cryptocurrencies**. Disponível em <https://coinmarketcap.com/all/views/all/>. Acesso em 20 fev. 2020.

COINMARKETCAP. **Top 100 cryptocurrencies by market capitalization**. Disponível em <https://coinmarketcap.com/>. Acesso em 25 fev. 2020.

CUNHA E MELO, Mariana. **Anonimato, proteção de dados e devido processo legal:** porque e como conter uma das maiores ameaças ao direito à privacidade no Brasil. ITS Rio, Rio de Janeiro. Disponível em <https://itsrio.org/wp-content/uploads/2017/03/Mariana-Cunha-e-Melo-V-Revisado.pdf>. Acesso em 29 abr. 2020.

CUNHA FILHO, Marcelo de Castro. Bitcoin: uma tentativa de construção da confiança por meio da tecnologia. **Revista de Informação Legislativa**, Brasília, v. 56, n. 221, p. 37-60, jan./mar. 2019.

DASH. **Frequently asked questions**. Disponível em <https://www.dash.org/faq/>. Acesso em 25 fev. 2020.

DASH. **PrivateSend**. Dash Documentation. Disponível em <https://docs.dash.org/en/stable/introduction/features.html#privatesend>. Acesso em 24 fev. 2020.

DONEDA, Danilo. A proteção de dados em tempos de coronavírus. **JOTA**, São Paulo, 25 mar. 2020. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020>. Acesso em 27 abr. 2020.

FABIAN, Benjamin; ERMAKOVA, Tatiana; SANDER, Ulrike. Anonymity in bitcoin? – the users' perspective. **Thirty Seventh International Conference on Information Systems**, Dublin, 2016. Disponível em <Thirty Seventh International Conference on Information Systems, Dublin 2016>. Acesso em 10 fev. 2020.

FAUZI, Muhammad Reza Rizky; NASUTION, Surya Michrandi; PARYASTO, Marisa W. Implementation and analysis of the use of the blockchain transactions on the workings of the bitcoin. **6th International Conference on Mechatronics** – ICOM'17 IOP Publishing, 2017. Disponível em <doi:10.1088/1757-899X/260/1/012003>. Acesso em 03 fev. 2020.

GAIHRE, Anil; LUO, Yan; LIU, Hang. Do bitcoin users really care about anonymity? An analysis of the bitcoin transaction graph. **2018 IEEE International Conference on Big Data (Big Data)**, nov. 2018. Disponível em <10.1109/BigData.2018.8622442>. Acesso em 03 fev. 2020.

HOUBEN, Robby; SNYERS, Alexander. Cryptocurrencies and blockchain legal context and implications for financial crime, money laundering and tax evasion. **European Parliament TAX3 Committee Study**. Disponível em <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%>. Acesso em 13 fev. 2020.

KAPPOS, George. et al. An empirical analysis of anonymity in zcash. **27th USENIX Security Symposium**, dez. 2017. Disponível em <https://www.researchgate.net/publication/327529465_An_Empirical_Analysis_of_Anonymity_in_Zcash>. Acesso em 14 fev. 2020.

KAPPOS, George. et al. An empirical analysis of anonymity in zcash. **27th USENIX Security Symposium**, dez. 2017. Disponível em <https://www.researchgate.net/publication/327529465_An_Empirical_Analysis_of_Anonymity_in_Zcash>. Acesso em 14 fev. 2020.

LEMOS, Ronaldo. Reconhecimento facial é o novo normal. Seção reader. **Folha de São Paulo**, São Paulo, 19 de agosto de 2019. Disponível em <https://www1.folha.uol.com.br/colunas/ronaldolemos/2019/08/reconhecimento-facial-e-o-novo-normal.shtml>. Acesso em 25 fev. 2020.

LESSIG, Lawrence. **Code (version 2.0)**. New York: Basic Books, 2006.

LI et. al. Traceable Monero: anonymous cryptocurrency with enhanced accountability. **Future Generation Computer Systems**, [s.l.], v. 101, p. 29-38, 2019. Disponível em <https://doi.org/10.1016/j.future.2019.05.081>. Acesso em 14 fev. 2020.

LUBARSKY, Boris. Re-Identification of "Anonymized Data". **Georgetown Law Technology Review**, Washington, DC, v. 1, n. 01, p. 202-213, 2017.

MENDES, Laura Schertel. Privacidade e dados pessoais. **Panorama setorial da Internet**, [s.l.], n. 2, a. 11, p 1-7, junho 2019.

MONERO. **Frequently asked questions**. Disponível em <https://web.getmonero.org/get-started/faq/>. Acesso em 23 fev. 2020.

MUNCHBACK, Cory. Data anonymization vs anonymous data. **Blueconic**. Disponível em <https://www.blueconic.com/blog/data-anonymization/>. Acesso em 25 fev. 2020.

NAKAMOTO, Satoshi. **Bitcoin: a peer-to-peer eletronic cash system**. Bitcoin.org, 2008.

NAKAMURA, Pâmela Naomi. **Desmistificando o bitcoin**: análise da sua natureza jurídica, uso e impactos. Monografia (LLM) – Programa de Pós Graduação em Direito do INSPER. São Paulo, 2017.

NARAYAN, Arvind; SHMATIKOV, Vitaly. **Robust de-anonymization of large sparse datasets**. Disponível em <https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>. Acesso em 27 abr. 2020.

NOVADAX. **Dúvidas sobre a declaração de criptomoedas no imposto de renda**. Disponível em https://blog.novadax.com/2020/02/11/duvidas-sobre-declaracao-de-criptomoedas-no-imposto-de-renda-2020/>. Acesso em 29 abr. 2020.

OLIVEIRA, Jordan Vinícius de; SILVA, Lorena Abbas da. Cookies de navegador e história da internet: desafios à lei brasileira de proteção de dados pessoais. **Revista de Estudos Jurídicos**, Franca, a. 22, n. 36, p. 307-338, jul./dez. 2018.

OLIVEIRA, Jordan Vinícius. **O anonimato no mundo cibernético**: três mitos.

PAL, Om et al. Key management for blockchain technology. **ICT Express**. [s.l.], 21 ago. 2019. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2405959519301894>. Acesso em 20 fev. 2020.

POULSEN, Kevin. Your Anonymous Posts to Secret Aren't Anonymous After All. **Wired**, [s.l.], 22 ago. 2014. Disponível em <https://www.wired.com/2014/08/secret/>. Acesso em 15 fev. 2020.

SARDÁ, Thais et al. Understanding online anonymity. **Media, Culture & Society**, London, v. 41, n. 4, p. 557-564, 2019.

SIMEÃO, Álvaro; VARELLA, Marcelo Dias. A impossibilidade de regulação jurídica nacional do blockchain: rumo à um direito criptográfico? **Revista de Direitos Culturais**, Santo Ângelo, v. 13, n. 31, p. 43-70, 2018.

UNIÃO EUROPEIA. **Parecer 05/2014 sobre técnicas de anonimização**. p. 11-12. Grupo de Trabalho de Proteção de Dados do Artigo 29. Adotado em 10 de abril de 2014. Disponível em <https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf>. Acesso em 03 set. 2019.

WIKIPEDIA. Satoshi Nakamoto. **Wikipedia, the free encyclopedia**. Disponível em <https://en.wikipedia.org/wiki/Satoshi_Nakamoto>. Acesso em 03 fev. 2020.

WOOLF, Nicky. Silk Road sentencing: why governments can't win the war on darknet drugs. **The Guardian**, Londres, 31 mar. 2015. Disponível em <https://www.theguardian.com/technology/2015/may/31/silk-road-sentencing-darknet-drugs>. Acesso em 25 fev. 2020.

WU, Wai. **Limitations of privacy guarantees in cryptocurrencies**. Thesis (EAS 499 Senior Capstone Thesis) – School of Engineering and Applied Science, University of Pennsylvania. Pennsylvania, 25 abr. 2018. p. 24-25. Disponível em <https://www.cis.upenn.edu/~fbrett/theses/wai_wu.pdf>. Acesso em 22 fev. 2020.

ZCASH. **How it works**. Disponível em <https://z.cash/pt/technology/>. Acesso em 25 fev. 2020.