Tarcisio Teixeira
Carlos Alexandre Rodrigues

Blockchain e Criptomoedas

aspectos jurídicos

4ª edição
revista e
atualizada

2023

EDITORA JusPODIVM
www.editorajuspodivm.com.br

9. *Big data* e *blockchain*

Em relação à proteção de dados, há um movimento global recente no sentido de normatizar o acesso a estas informações por empresas e governos, o que culminou em diversas legislações: no Brasil, embora a preocupação com essa questão já se anunciasse no Marco Civil da Internet (Lei 12.965/2014), em agosto de 2018 foi editada a Lei Geral de Proteção de Dados (Lei 13.709/2018), que versa especificamente sobre a proteção de dados pessoais em âmbito nacional[1].

Na definição adotada pelo artigo 5º, inciso I, da Lei 13.709/2018, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, "*dados pessoais*" são "*dados relacionados à pessoa natural identificada ou identificável",* enquanto, segundo o inciso IV do mesmo artigo, "bancos de

1. Tal legislação junta-se, dentre outras, ao Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, mais conhecido como GDPR (*General Data Protection Regulation*), o qual estabelece diretrizes para uniformização do tratamento de proteção de dados pessoais pelos Estados-membros da União Europeia e que serviu de clara inspiração ao modelo brasileiro, e ao Ato de Proteção de Informações Pessoais do Japão, em vigor desde 1º de abril de 2005. Alguns países, como os Estados Unidos, não possuem legislação específica a respeito até o momento.

dados" *"são conjuntos estruturados de dados pessoais, estabelecidos em um ou vários locais, em suporte eletrônico ou físico"*; semelhante definição é encontrável na "General Data Protection Regulation"[2], regulamento geral de proteção de dados em vigor na Comunidade Europeia desde maio de 2008:

> "*Para efeitos do presente regulamento, entende-se por: 1) 'Dados pessoais', informação relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular;"*

Para além da definição jurídica, o fato é que dados pessoais são informações produzidas, a todo o tempo, por todo aquele que se conecta à internet, não importando o dispositivo, site ou horário. Assim, enquanto navegamos em qualquer website, procuramos uma expressão num serviço de busca, baixamos qualquer tipo de música ou filme, enviamos ou recebemos um e-mail, utilizamos um serviço de mapas, postamos uma fotografia em redes sociais, fazemos uma ligação, enviamos ou mesmo simplesmente lemos qualquer coisa em nossos celulares, "dados" são produzidos e armazenados em servidores dos provedores de acesso e conteúdo.

Devidamente organizados, estes dados irão compor informações sobre nossas preferências, endereços, localizações,

2. PARLAMENTO EUROPEU. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho,** de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 27 jun. 2019.

gostos, compras e uma infinidade de atos do cotidiano que, de modo até inconsciente, diariamente praticamos – isto sem falar que, no estágio da internet das coisas em que nos encontramos, muitos dados são gerados sem que precisemos sequer operar, por nós mesmos, os dispositivos eletrônicos[3].

Esta organização de dados em informações, formam o que convencionou-se chamar de "*big data*", que nada mais é que um conjunto enorme de informações sobre todos nós, muitas em tempo real, coletadas por uma gama de corporações e ajustadas para usos comerciais e, portanto, privados destas. E, embora o Marco Civil da Internet (Lei 12.965/2014) trouxesse a previsão em seu artigo 7º da necessidade de consentimento expresso do usuário de internet para coleta de tais dados, não o exigiu que isso fosse feito previamente. Nesse sentido:

> *"Sem dúvida, a norma teria feito melhor se, em vez de prever apenas consentimento expresso, tivesse disposto consentimento prévio e expresso. Com isso, alguns agentes econômicos poderão se utilizar de ferramentas para obter o consentimento posteriormente, de forma a dificultar a opção do usuário, que muitas vezes já estará envolvido com a ferramenta tecnológica que lhe foi oferecida e já está sendo utilizada*"[4].

Na Lei 13.709/2018, o consentimento para tratamento de dados é tido como necessário (art. 7º, inciso I), a não ser quando os dados tenham sido tornados manifestamente públicos pelo titular (art. 7º, § 4º), e deverá sempre especificar

3. TECNOLOGIA IG. **Geladeira que manda fotos do seu interior prova que a Internet das Coisas chegou.** Disponível em: https://tecnologia.ig.com.br/2016-01-07/geladeira-que-manda-fotos-do-seu-interior-prova-que-a-internet-das-coisas-chegou.html. Acesso em: 27 jun. 2019.

4. TEIXEIRA, Tarcisio. **Curso de Direito e Processo Eletrônico: doutrina, jurisprudência e prática**. 4. ed. São Paulo: Saraiva, 2018, p. 113.

as finalidades do tratamento, sob pena de nulidade (art. 8º, § 4º). Igualmente, quem tenha autorização para tratamento de dados precisará de uma nova, se pretender repassá-los a terceiros (art. 7º, § 5º). Ainda mais rigorosa é a situação do tratamento dos dados pessoais sensíveis, estes definidos no artigo 5º, II, da lei nacional de proteção de dados, e que abrangem, por exemplo, dados sobre origem racial ou étnica, convicção religiosa, opinião política, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos de pessoas naturais.

Ninguém ignora que tais dados são valiosos para as empresas, na medida em que, após tal "tratamento" (*big data analytics*) – que nada mais é, afinal, uma operação realizada com os dados coletados, para os fins comerciais de interesse de cada empresa – podem ser utilizados para descoberta de padrões de consumo, ou mesmo situações mais sensíveis, como toda a sorte de preferências, sejam profissionais, esportivas, políticas, sexuais... É lícito dizer que a coleta e tratamento destes dados expõem a intimidade do ser humano, mais do que ele mesmo pode imaginar, e, muitas vezes, reconhecendo padrões que nem ele próprio teria se atentado[5].

O fato é que há uma lista interminável de sites, programas, jogos ou serviços disponibilizados de forma aparentemente gratuita e que na verdade, são "pagos" pela coleta de dados dos usuários, numa situação em que a mercadoria é o próprio consumidor[6].

---

5. ACADEMIA IN. **Afinal, como o Big Data ajuda a entender o comportamento do consumidor?** Disponível em: http://blog.academiain1.com.br/afinal-como-o-big-data-ajuda-a-entender-o-comportamento-do-consumidor. Acesso em: 30 jun. 2019.
6. PASI, Renata Capriolli Zocatelli Queiroz; TEIXEIRA, Tarcisio. **Privacidade na internet: a formação de banco de dados e a transformação das pessoas em mercadorias**. Revista dos Tribunais nº 990, abril 2018, p. 114.

Uma vez que a interpretação da legislação permite concluir também que tais dados podem ser cedidos a terceiros de forma onerosa, um ponto relevante é questionar se o titular dos dados (*rectius:* cada um de nós) não deveria possuir um controle maior sobre tais informações, evitando vazamentos e mau uso por terceiros, e até mesmo se não deveria ser ele o remunerado pelo acesso a estas. Este panorama, aparentemente inviável, nos parece ser possível, mediante a aplicação da tecnologia *blockchain* ao chamado "big data".

Como se viu, no núcleo da tecnologia *blockchain* está a capacidade de criar um banco de dados global que é imutável, transparente e confiável – mesmo quando as partes que participam da troca de dados não são confiáveis uma pela outra.

Neste sentido, a grande revolução em relação ao cenário atual, decorreria então do fato da tecnologia ser criptografada e descentralizada sem perda da segurança, vez que os dados dos usuários não necessitariam mais ser armazenados por uma única pessoa ou entidade, mas, ao contrário, residiriam no *blockchain*. Isso é o oposto do tradicional modelo atual, no qual as corporações armazenam a grande quantidade de dados sobre todos os consumidores, com as implicações de privacidade e segurança.

Com a utilização da tecnologia *blockchain* para esta finalidade, não haveriam bancos de dados "privados", sob o controle de uma empresa que acumula dados confidenciais sobre pessoas e instituições para usos comerciais. Diferentemente do modelo atual, em que as empresas coletam os dados dos consumidores, e os armazenam para usos privados – o que gera os riscos tanto da má administração quanto na falha na guarda destes dados, ocasionando vazamentos em proporções

gigantescas[7] – o modelo baseado no *blockchain* inverteria esta lógica: os dados seriam armazenados em um banco de dados público, com o usuário liberando apenas os dados necessários para cada operação, mediante uma chave privada.

Neste modelo, a aplicação da tecnologia *blockchain* permitiria, por exemplo, que embora os dados armazenados de cada consumidor num ambiente descentralizado possam ser sempre os mesmos, os dados liberados para cada utilização poderiam ser restritos conforme a sua natureza. Assim, os dados vistos numa compra on-line não seriam os mesmos que seriam disponibilizados para cadastro em uma clínica médica ou para acesso a financiamentos, por exemplo. Diferentemente, somente os aspectos relevantes para cada operação específica seriam disponibilizados pelo usuário/consumidor, não obstando, entretanto, que, dentro do modelo de recompensas natural à tecnologia *blockchain*, dados mais aprofundados fossem disponibilizados mediante recompensa financeira em moedas virtuais – mas isso seria uma opção do detentor dos dados, e seria feita caso a caso, e não como ocorre agora, uma situação sem nenhum controle deste.

Além disso, como o armazenamento de tais dados não ficaria a cargo de nenhuma instituição particular, a possibilidade de mau uso ou má guarda destes dados seria reduzida de forma considerável, modificando até mesmo a lógica das responsabilidades jurídicas neste campo, atualmente foco de grandes discussões.

---

7. OLHAR DIGITAL. **Dados de 10 milhões de cartões de crédito Visa e Mastercard são roubados nos EUA.** Disponível em: https://olhardigital.com.br/fique_seguro/noticia/10-milhoes-de-dados-de-cartoes-de-credito-visa-e-mastercard-roubados-nos-eua/25215. Acesso em: 27 jun. 2019.

Em artigo no qual avalia a compatibilidade entre a tecnologia *Blockchain* e a LGPD, Renata Baião apresenta solução bastante engenhosa para este controle de dados:

> "*Assim, blockchain apresenta um ambiente relativamente seguro para o armazenamento de informações pessoais e, mais, permite o gerenciamento do dado por meio de seu titular. Veja-se: o registro na rede jamais será modificado. Todavia, poderá tornar-se inacessível, inclusive por escolha do titular ao destruir a chave privada ou o arquivo original.*
>
> *Na prática, sob a perspectiva dos prestadores de serviço e desenvolvedores, caso uma aplicação pretenda trabalhar com dados sensíveis (registros médicos, por exemplo), a alternativa é a manutenção de tais dados off-chain (fora da blockchain) ou em uma sidechain (blockchain secundária). Assim, a blockchain dita principal exerceria mera função indexadora do dado ou da transação, mas sem revelá-lo(a), ainda que de forma criptografada, o que, ao menos em tese, permite o completo atendimento aos parâmetros estabelecidos pelo GDPR e pela Lei Geral de Proteção de Dados Pessoais*"[8].

Isto traz reflexos jurídicos evidentes, na medida em que o acesso aos dados seria seletivo, e, normalmente, liberado pelo próprio titular, além de rastreável. Com isso, as próprias figuras do "controlador" (pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, segundo o artigo 5º, VI, da Lei 13.709/2019) e do "operador" (conforme artigo 5º, VII, da Lei 13.709/2019, a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador) teriam de ser revistas, uma vez que

8. BAIÃO, Renata. Afinal, *blockchain* é incompatível com a LGPD? Disponível em https://www.serpro.gov.br/lgpd/noticias/2019/*blockchain*-lgpd-dados-pessoais-brasil. Acesso em: 5 set. 2020.

as decisões sobre tais tratamentos partiriam do próprio titular, como regra.

Ademais, tratando-se de banco de dados único, seria facilitada a sua correção pelo consumidor ou usuário nas hipóteses de dados inverídicos ou incompletos (situação igualmente prevista tanto na GPDR quanto na Lei Geral de Proteção de Dados, como direitos básicos do titular dos dados), além de que as informações disponibilizadas seriam sempre as mesmas para qualquer instituição da mesma natureza (os mesmos dados médicos de um usuário seriam acessados quando fosse necessário submeter-se a uma consulta, ainda que de especialidades diferentes, não dependendo do grau de informatização da clínica pública ou particular, por exemplo) e, principalmente, seria possível auditar quem viu cada informação, quando e para qual finalidade. O controle social destes dados armazenados seria amplamente possível[9].

Outro aspecto de relevância jurídica está na rastreabilidade, dado que seria possível identificar o responsável pelo tratamento, se houver, quando especialmente, em que situações os dados foram acessados, de forma transparente e imutável. Seria uma hipótese de liberação descentralizada, em que as informações e os dados são de propriedade do usuário, em vez do provedor de serviços.

---

9. Sendo que a proteção de dados já é tratado como direito fundamental do ser humano, conforme a Constituição Federal brasileira, art. 5º, inc. LXXIX (Incluído pela Emenda Constitucional n. 115, de 2022). Isto também consta expressamente no Considerando nº 1 do GPDR: *"A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8º, n. 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16º, nº 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito"*.

Dan Tapscott e Alex Tapscott escrevem a respeito, resumindo o modelo aqui estudado, tratando-o por *"little data"*:

> *"Com a tecnologia blockchain [...] você conseguiria proteger suas informações particulares dando apenas a informação necessária em qualquer trabalho de troca social ou econômica sob o seu comando, e se certificando que você receba uma compensação por qualquer um dos seus dados que tenham valor para outras partes. É uma mudança a partir do big data para os dados privados. Chame isso de little data."*[10]

No modelo atual, diferentes dados e informações são mantidos e tratados separadamente por diferentes "controladores", de sorte que o titular dos dados tem pouco ou nenhum controle sobre os dados colhidos, tratados e compartilhados. Com utilização do modelo baseado em *blockchain*, os elementos de informação pessoal poderiam ser mantidos em uma espécie de *carteira virtual* sob total administração do titular dos dados, que definiria qual ou quais desses elementos revelar em determinados contextos.

Isto é possível, como se viu, em virtude de a tecnologia *blockchain* basear-se em alguns conceitos que lhes são inerentes, especialmente ser descentralizada, de modo que nenhuma pessoa, governo, corporação ou empresa controlaria a entrada de dados ou sua integridade (a veracidade das informações é verificada continuamente por todos os computadores da rede); também sua imutabilidade merece ser destacada, pois a informação permanece no mesmo estado enquanto a rede existir, e é disponibilizada de forma pública, acessível por qualquer usuário da rede, não em um computador central, mas justamente em todos os computadores conectados da rede, sem controle

10. TAPSCOTT, Alex; TAPSCOTT, Dan. ***Blockchain* Revolution.** São Paulo: Senai-SP, 2016, p. 77.

privado de nenhum ente. Enfim, parece emergir como uma alternativa de grande valia para a solução ou mitigação dos problemas decorrentes da formação dos chamados "big data" que atualmente vislumbramos.

9.1. Uma camada de identidade para a internet

Ainda neste campo dos dados, podem ser destacados, dos conhecidos efeitos colaterais mais notáveis da confusão entre a vida real e a vida on-line[11], a precarização cada vez maior do direito à privacidade individual na internet[12], bem como a ausência de uma identidade digital que gere segurança e confiança aos partícipes destas relações digitais (e isto vale para qualquer categoria de relações, sejam o uso de e-mails, aplicativos bancários ou mesmo aplicativo de encontros, indistintamente).

Na verdade, há uma ligação entre os pontos: como no sistema atual de utilização e acesso aos meios digitais não existe um modo seguro de certificar-se que os internautas são

11. "*Enfim, o uso da Tecnologia da Informação em geral (internet, celular etc.) tem sido para muitos um fim em si mesmo, não um meio que facilite as atividades cotidianas e permita maior interação humana. Ao contrário, promove o afastamento, o egoísmo, impedindo o compartilhamento e o companheirismo. Assim, mais difícil para o ser o humano desenvolver-se e aprimorar-se como ser social que é.*" In: TEIXEIRA, Tarcisio. **Curso de Direito e Processo Eletrônico: doutrina, jurisprudência e prática**. 4. ed. São Paulo: Saraiva, 2018, p. 149.
12. O direito à intimidade consiste, afinal, *"na faculdade que cada pessoa tem de impedir a intromissão de estranhos na sua vida privada e familiar"* (TEIXEIRA, Tarcisio. **Curso de Direito e Processo Eletrônico: doutrina, jurisprudência e prática**. 4. ed. São Paulo: Saraiva, 2018, p. 82). Percebe-se, nestes tempos vida digital, como o exercício desta faculdade é cada vez mais difícil, pois por vezes sequer sabemos que os dados estão sendo colhidos.

quem dizem ser, abre-se espaço para que os fornecedores de aplicativos e softwares, sob o pretexto de garantir a segurança das operações, colham uma infinidade de dados dos usuários de seus serviços e assim, passem a ser eles (os fornecedores) os detentores destes dados, como visto acima.

Esta ausência de identidade digital confiável tem sido, enfim, um dos principais desafios enfrentados pela Internet desde a abertura para sua utilização comercial, pois nenhum dos meios tradicionais e off-line são capazes de verificar, com segurança, a identidade do usuário[13].

Isto permite, por exemplo, a proliferação de perfis falsos em redes sociais – eis que um endereço utilizado para acesso à internet, o TCP/IP, embora rastreável, não é considerado um ID público, pois não identifica um único usuário, a princípio –, os quais são utilizados para toda sorte de manifestações, das mais inofensivas (como comentários de baixa qualidade em notícias ou fóruns de internet), até ações coordenadas para a propagação de notícias falsas, as chamadas *fake news,* as quais são conceituadas pela Comissão Europeia[14] como *"informações verificáveis, falsas ou enganosas, que são criadas, apresentadas e divulgadas para ganho econômico ou para enganar intencionalmente o público, e podem causar danos públicos"*[15].

13. Um cartum da Revista The New Yorker, de 1993, já satirizava esta situação nos primórdios da internet, numa icônica tira que retratava dois cães utilizando um computador e um está dizendo para o outro "na internet, ninguém sabe que você é um cachorro."
14. COMISSÃO EUROPEIA. **Tackling online disinformation**. Disponível em: https://ec.europa.eu/digital-single-market/en/fake-news. Acesso em: 28 jun. 2019.
15. Tradução livre do original: "Disinformation – or fake news – consists of verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm".

Com efeito, a intenção da propagação das *fake news* pode variar, mas em geral o objetivo é econômico (notícias alarmistas geram cliques e acessos a sites, que, por sua vez, lucram com anúncio; estudo do MIT publicado na conceituada Revista Science constatou que a propensão dos internautas a propagar notícias falsas é 70% maior do que no caso de notícias verdadeiras[16]), ou, como tem se visto mais recentemente, político (com intenção de denegrir ou elevar a imagem de determinado candidato). A preocupação recente com o assunto é tamanha que o Facebook foi levado a editar novas diretrizes sobre o que pode ou não ser publicado, bem como implementar novas estratégias para combater a divulgação de notícias falsas[17], e o Tribunal Superior Eleitoral a criar um Conselho Consultivo para debater o assunto tendo em vista as eleições de 2018 no país, buscando soluções[18].

Neste sentido, merece ser então mencionada a Lei 13.444/2017, que dispõe sobre a Identificação Civil Nacional (ICN), com o objetivo de identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados. Ela pretende não apenas identificar toda a população brasileira com base na biometria, mas também

16. REVISTA SCIENCE. **The spread of true and false news online.** Disponível em: https://science.sciencemag.org/content/359/6380/1146.full. Acesso em: 21 jun. 2019.
17. FACEBOOK NEWSROOM. **Questões complexas: Qual é a estratégia do Facebook para combater notícias falsas?** Disponível em: https://br.newsroom.fb.com/news/2018/05/questoes-complexas-qual-e-a-estrategia-do-facebook-para-combater-noticias-falsas/. Acesso em: 28 jun. 2019.
18. TRIBUNAL SUPERIOR ELEITORAL. **TSE vai combater fake news com apoio da imprensa.** Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2018/Fevereiro/tse-vai-combater-fake-news-com-apoio-da-imprensa. Acesso em: 28 jun. 2019.

integrar as bases de dados já existentes para as mais diversas finalidades. Pretende-se, enfim, criar uma identidade que pode ser utilizada também como identidade digital[19].

Diante desse cenário, mais uma vez cumpre analisar em que aspectos a tecnologia *blockchain*, por conta de suas características, pode representar uma possibilidade de uma identidade digital verdadeira, controlada pelo usuário e resistente a violações e registros digitais.

Como já visto em outras passagens, a tecnologia *blockchain* desloca a ideia de confiança baseada em uma autoridade centralizadora (uma agência de notícias, por exemplo) para a confiança baseada na rede, de modo que nesta proposta descentralizadora, nenhuma entidade "central" opere como intermediária certificadora de forma individualizada de nenhuma operação ou informação, as quais são realizadas diretamente pelos próprios usuários.

Don Tapscott e Alex Tapscott abordam o assunto sob um prisma interessante, tratando como a ideia de um "avatar digital":

> *"E se "o você virtual" fosse de fato de sua propriedade – seu avatar pessoal – e "vivesse" na caixa-preta de sua identidade, de modo que você pudesse monetizar seu fluxo de dados e revelar apenas o necessário quando estivesse reivindicando um direito específico? Porque a sua carteira de habilitação contém mais informações que o fato de ter passado no teste de condução e possuir habilidade para dirigir? Imagine uma*

19. Esta é uma das aplicações possíveis na *blockchain* no serviço público, como trata interessante artigo do SERPRO, denominado "**Como utilizar a Tecnologia Blockchain no Governo?**" Disponível em https://www.serpro.gov.br/menu/noticias/noticias-2017/como-utilizar-a-tecnologia-*blockchain*-no-governo. Acesso em: 6 fev. 2021.

> *nova era da internet em que o seu avatar pessoal gerencia e protege o conteúdo de sua caixa-preta. Esse confiável software poderia liberar apenas os detalhes ou as quantidades necessários para cada situação, e, ao mesmo tempo, ir varrendo as migalhas de dados à medida que você navega pelo mundo digital"*[20].

Outrossim, os dados necessários a estas operações ou informações igualmente não são concentradas em nenhuma entidade central, permanecendo disponíveis a todos no livro-razão (*ledger*) com acesso irrestrito a qualquer internauta, em um site público. Assim, todas as operações são feitas diretamente "parte a parte" (*peer-to-peer*) e registradas em um livro público, disponível na internet, e certificadas pela própria rede. Também se viu que no caso do protocolo Bitcoin, os usuários da *blockchain* são também os seus certificadores, e recebem por este "trabalho" uma remuneração em moedas digitais (os bitcoins, no caso das operações financeiras originalmente criadas por Satoshi Nakamoto[21]).

A criação de uma identidade digital poderia ser combinada com uma *camada de identidade* com validade para acesso à internet[22], na forma de uma identidade digital segura e verificável no *blockchain*, exigindo a apresentação da chave privada para acessos, de sorte a reduzir (ou mesmo evitar) o

---

20. TAPSCOTT, Alex; TAPSCOTT, Don. ***Blockchain* revolution: como a tecnologia por trás do bitcoin está mudando o dinheiro, os negócios e o mundo**. São Paulo, SENAI-SP, 2016, p. 46.
21. NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Eletronic Cash System**, 2008. Disponível em: < https://bitcoin.org/bitcoin.pdf>. Acesso em: 12 jun. 2019.
22. O advogado Ronaldo Lemos, em palestra denominada "O impacto do *Blockchain* na sociedade", ministrada no evento *Blockchain* Festival (realizado em São Paulo, no dia 23 de maio de 2018), defendeu ideia parecida como contraponto à simples utilização de certificados digitais em alguns sites governamentais.

anonimato na rede – e que poderia ser utilizada em conjunto com certificações digitais, para acessos específicos.

Deste modo, em vez de conceder amplo consentimento a inúmeros aplicativos, serviços e portais, e assim ver seus dados de identidade espalhados por vários provedores, internautas teriam algo como um *"hub"* digital criptografado e seguro, onde poderiam armazenar seus dados de identidade e controlar a forma de liberação de acesso a eles conforme o acesso pretendido, diretamente, sem intervenção de terceiros. Ao mesmo tempo, o acesso à internet que implicasse em propagação de informações em maior ou menor grau (abrangendo, conforme o caso, o envio de e-mails, acesso a perfis ou replicação de notícias), seria feito por meio desta identidade digital, permitindo a identificação do autor originário da informação. Em hipóteses ainda mais específicas (como o acesso a dados oficiais ou de saúde), poderia ainda ser combinado com a utilização de uma certificação digital.

Como se nota, a criação desta camada de identidade digital, adotando a tecnologia *blockchain* como um *meta-sistema* (ou seja, um sistema necessário para acesso a outro), implicaria em uma maneira confiável de estabelecer quem está se conectando com o que, e em qualquer lugar na Internet. Tal utilização criaria meios para que pudessem conviver, sem conflitos aparentes, os princípios como da proteção da privacidade e de dados pessoais (art. 2º), com o direito de acesso à internet. Além disso, a possibilidade de utilização da tecnologia *blockchain* para a criação de uma camada de identidade em toda a internet, seria um marco revolucionário na forma como utilizamos a rede, representando talvez a maior utilidade da própria tecnologia.

10. Aspectos tributários[1]

Em relação aos aspectos tributários, a maior atenção é dirigida às obrigações impostas pela legislação tributária aos detentores de criptomoedas, especialmente a partir da Instrução Normativa RFB 1871/19, em virtude de, segundo dados da Receita, *"os clientes de exchanges superaram o número de usuários inscritos na bolsa de valores de São Paulo"*, tanto que, em 2017, foram negociados aproximadamente R$ 8.300.000.000,00 em Bitcoins.

Oficialmente, como se viu ao estudar a natureza jurídica das criptomoedas, a Receita Federal do Brasil – RFB manifestou-se no sentido de que *"as moedas virtuais (bitcoins, por exemplo), muito embora não sejam consideradas como moeda nos termos do marco regulatório atual, devem ser declaradas na Ficha Bens e Direitos como 'outros bens', uma vez que podem ser equiparadas a um ativo financeiro"*[2].

1. Capítulo escrito com apoio de João Victor Ribeiro Aldinucci, Conselheiro do CARF.
2. RECEITA FEDERAL DO BRASIL. **Perguntas e Respostas IRPF 2019.** Disponível em: http://receita.economia.gov.br/interface/cidadao/irpf/2019/perguntao/perguntas-e-respostas-irpf-2019.pdf#page=22&zoom=100,0,66. Acesso em: 11 maio 2019.