SEMINÁRIO NACIONAL DE FORMAÇÃO DE PESQUISADORES E INICIAÇÃO CIENTÍFICA EM DIREITO DA FEPODI

S472
Seminário Nacional de Formação de Pesquisadores e Iniciação Científica em Direito da FEPODI [Recurso eletrônico on-line] organização Federação Nacional dos Pós-Graduandos em Direito - FEPODI;

Coordenadores: Beatriz Souza Costa, Lívia Gaigher Bosio Campello, Yuri Nathan da Costa Lannes – Belo Horizonte: ESDH, 2017.

Inclui bibliografia
ISBN: 978-85-5505-383-2
Modo de acesso: www.conpedi.org.br em publicações

1. Direito – Estudo e ensino (Graduação e Pós-graduação) – Brasil – Congressos nacionais. 2. Direito Constitucional. 3. Direito ambiental. 4. Direito Administrativo. 5. Direito Civil. 6. Direito Penal. 7. Direitos Humanos. 8. Direito Tributário. 9. Filosofia Jurídica. 10. Gênero. 11. Diversidade Sexual. I. Seminário Nacional de Formação de Pesquisadores e Iniciação Científica em Direito da FEPODI (1:2016 : Belo Horizonte, MG).

CDU: 34

FEPODI
FEDERAÇÃO NACIONAL DOS PÓS-GRADUANDOS EM DIREITO

SEMINÁRIO NACIONAL DE FORMAÇÃO DE PESQUISADORES E INICIAÇÃO CIENTÍFICA EM DIREITO DA FEPODI

Apresentação

É com imensa satisfação que a Escola Superior Dom Helder Câmara e a Federação Nacional dos Pós-graduandos em Direito – FEPODI apresentam à comunidade científica os Anais do Seminário Nacional de Formação de Pesquisadores e Iniciação Científica em Direito. Tal produção resulta do exitoso evento sediado nas dependências da Escola Superior Dom Helder Câmara, em Belo Horizonte-MG, nos dias 10 e 11 de outubro de 2016, que contou com o valioso apoio do Conselho Nacional de Pesquisa e Pós-Graduação em Direito – CONPEDI e da Associação Brasileira de Ensino do Direito – ABEDi.

Trata-se de obra coletiva composta por 263 (duzentos e sessenta e três) resumos expandidos apresentados no seminário e que atingiram nota mínima de aprovação dentre os 318 (trezentos e dezoito) trabalhos submetidos ao evento. As comunicações científicas estão organizadas em 21 (vinte e um) Grupos de Trabalho ligados a diversas áreas do direito, inseridos num ambiente de ricos debates e profundas trocas de experiências entre os representantes das mais diversas localidades do Brasil.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de proeminentes docentes ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores, afim de que eles estejam aptos, após desenvolvimento, a serem publicados posteriormente nos periódicos jurídicos nacionais.

Neste prisma, os presentes anais, de inegável valor científico, já demonstram uma contribuição para a pesquisa no Direito e asseguram o cumprimento dos objetivos principais do evento de fomentar o aprofundamento da relação entre pós-graduação e graduação em Direito no Brasil, bem como de desenvolver os pesquisadores em Direito participantes do evento por meio de atividades de formação em metodologias científicas aplicadas.

Uma boa leitura a todos!

Beatriz Souza Costa

Lívia Gaigher Bosio Campello

Yuri Nathan da Costa Lannes

Coordenadores Gerais do Seminário Nacional de Formação de Pesquisadores e Iniciação Científica em Direito.

CRIPTOGRAFIA: A ALVORADA DA QUEDA DO ESTADO MODERNO? BITCOIN E TOR

CRYPTOGRAPHY: DAWN OF THE FALL OF THE MODERN STATE?BITCOIN AND TOR

Fabricio Bertini Pasquot Polido [1]
Rômulo Inácio da Silva Caldas

Resumo

Novas tecnologias possibilitam ao cidadão comum incorporar à sua vida ferramentas revolucionárias que venham a assistir no manejo de informações. Dentre elas, a criptografia – processo de proteção de dados – confere anonimato quase absoluto nas transações informacionais, inclusive em relação ao Estado, que, por consequência, segue paulatinamente destituído de competências legislativas e de poderes regulatórios, todos fundados na concepção de soberania e territorialidade, arruinando seu controle econômico. Analisar e compreender as tecnologias Bitcoin e Tor, ambas baseadas na criptografia, assim como possíveis implicações para a regulação das atividades econômicas e financeiras pelo Estado, apresentam-se como objetivo principal desta pesquisa.

Palavras-chave: Criptografia, Bitcoin, Tor, Estado, Ordem jurídica transnacional, Territorialidade

Abstract/Resumen/Résumé

Technological enhancement grants the common citizen the possibility to own revolutionary tools to deal with the handling of data. Among those, there is cryptography – a process to protect data – which comes to grant an almost absolute anonymity, including in relation to the State, which, by consequence, slowly loses legislative competence and regulatory power, both grounded on the concept of sovereignty and territoriality, ruining economic control. The analysis and understanding of the technologies Bitcoin and Tor, both powered by cryptography, and it's eventual implications to the State and it's economic regulatory power, are the main objective of this research.

Keywords/Palabras-claves/Mots-clés: Cryptography, Bitcoin, Tor, State, Transnational legal order, Territoriality

[1] Professor Adjunto de Direito Internacional da Universidade Federal de Minas Gerais. Doutor em Direito Internacional pela USP. Diretor do Instituto de Referência em Internet e Sociedade - IRIS

1. CONSIDERAÇÕES INICIAS

A criptografia, de forma simplificada, é um sistema de segurança que consiste em embaralhar - ou criptografrar - o conteúdo de um conjunto de dados qualquer que se queira transmitir, de tal modo que somente seu destinatário tenha acesso à possibilidade de revelar estes dados, por meio de uma espécie de "chave" que irá desembaralhar - ou decriptografar - este mesmo conteúdo. A ideia por trás da criptografia é tornar inviolável a leitura de uma mensagem qualquer, exceto para seu destinatário. (MICROSOFT, 2016).

Desta forma, à medida que as tecnologias modernas vão se popularizando para o grande público, também se expandem as possibilidades do cidadão comum proteger seu anonimato online e de usufruir serviços de forma cada vez mais direta, segura e mesmo secreta, eliminando intermediários e gerando um tipo de inviolabilidade capaz de alienar o alcance do poder estatal, intrinsecamente vinculado a um conceito de territorialidade que o impulsiona a tornar-se agente com instrumentos obsoletos para lidar com questões de grande relevância social, como a própria economia. Tudo por meio da criptografia.

A pesquisa se propõe a uma análise – sem a pretensão de esgotar o tema - de duas tecnologias, Bitcoin e TOR, ambas baseadas em criptografia, e suas respectivas consequências relativas à atuação do Estado, buscando verificar se o Estado está bem preparado, no tocante à sua capacidade coercitiva, para lidar com estas inovações. O presente trabalho pertence à vertente metodológica jurídico-sociológica. No tocante ao tipo de investigação, foi escolhido, na classificação de Witker (1985) e Gustin (2010), o tipo jurídico-compreensivo.

2. BITCOIN

Com bastante astúcia, Milton Friedman (1999, tradução livre[1]) previra: "Algo que falta, mas em breve será desenvolvido, é uma moeda virtual confiável. Um método em que, pela internet, você pode transferir fundos de A para B sem que A conheça B e vice-versa". Friedman estava certo. Acontece que o fisco, igualmente, não fica sabendo das atividades de A ou de B.

Em 2008, veio à luz o Bitcoin, moeda digital independente de um órgão central – nos moldes do Banco Central - que o regule. Por meio de um sofisticado método de criptografia,

[1] One thing that is missing, but will soon be developed is a reliable e-cash, a method where by, on the internet, you can transfer funds from A to B without A knowing B or B knowing A.

supondo uma transação entre A e B, ambos têm chaves criptográficas distintas, que são usadas para legitimar a negociação entre eles através de chaves criptográficas públicas, registradas no *blockchain*, o grande livro-razão público do sistema Bitcoin, de forma tal que não é possível fraudar as transações ou o sistema. (ULRICH, 2014, pág. 18).

Os Bitcoins, como são conhecidas as unidades desta moeda, são negociados por outras moedas tradicionais, como o dólar, real ou euro, em mercados online. As transações são protegidas por novas chaves criptográficas a cada mudança de mãos das moedas, de forma que uma quantia enorme de dinheiro poderia ser transferida de uma extremidade do mundo à outra sem que se saiba quem são os envolvidos na negociação, driblando barreiras geográficas, alfandegarias e fiscais e mesmo criminais.

Estas unidades de moeda são armazenadas em "carteiras digitais", que podem ser programas de computador, apps ou mesmo uma página hospedada na internet, o que torna possível a transferência facilitada de Bitcoins de uma carteira para outra com poucos cliques.

3. NAVEGAÇÃO ANÔNIMA: TOR

TOR - The Onion Router - é uma rede de servidores de internet voluntários (TOR PROJECT, 2016) mais conhecido por ser uma porta de acesso à Deep Web, parte "escondida" e obscura da internet convencional em que é possível, por exemplo, contratar assassinos de aluguel.

Há também usos legítimos para o TOR: o navegador é empregado por jornalistas, dissidentes políticos, *whistleblowers* – como Julian Assange, conhecido por seus vazamentos através do Wikileaks - e pela Marinha dos Estados Unidos para operações de segurança (ESTES, 2013). E está, igualmente, a poucos cliques de distância de qualquer pessoa com internet.

Ao baixar, instalar e abrir a rede TOR, diretamente, gratuitamente e sem restrições, a partir do site que o desenvolve, o usuário conecta-se a uma extensa rede de "nós" digitais. Ao se conectar a um nó, seu IP, espécie de endereço digital do computador, passa a ser protegido por criptografia enquanto um IP diferente do inicial é "emprestado", e este último conecta-se a um novo nó, em um longo caminho de mais nós, mais criptografia e novos IPs, até alcançar a informação inicialmente solicitada pelo usuário. (WHITWAM, 2015).

Este sistema de anonimato é um grande empecilho para o controle do tráfego de dados e identificação de usuários. No documento intitulado *Tor Stinks*, fruto dos vazamentos de Edward Snowden, a Agência de Segurança Nacional – órgão norte-americano – deixa claro

que: “Nunca seremos capazes de acabar com o anonimato de todos os usuários do TOR o tempo inteiro”. (NATIONAL SECUTIRY AGENCY, 2012, tradução livre[2]).

A resposta ao vazamento deste documento não tardou, pois logo seguiu o anúncio dos desenvolvedores do TOR de que é necessário que a comunidade da internet continue trabalhando para melhorar a segurança dos navegadores para que eventuais brechas de segurança sejam corrigidas. (TOR PROJECT, 2013).

4. ESTUDO DE CASO: SILK ROAD

Atuando como centro de comércio ilegal na Deep Web – acessível via TOR - entre os anos de 2011 e 2013 e intermediando o comércio de artefatos ilegais de drogas como maconha, ecstasy, derivados do ópio, drogas psicodélicas e afins, o site Silk Road movimentou precisas 9.519.664 moedas de Bitcoins, algo em torno de U$D1,3 bilhões, valor estimado em 18 de outubro de 2013. (GUGELMIN, 2013).

Eventualmente, os responsáveis pelo site foram pegos, e segundo a juíza encarregada, Katherine Foster, este foi um caso sem precedentes na história, pois foi a primeira vez que o crime “lavagem de dinheiro” foi relacionado a uma moeda digital.

Durante o processo, a questão do quão longe o governo pode ir para descobrir identidades online impulsionou a defesa a questionar que o processo baseou-se em uma invasão de computadores, por parte da polícia, sem mandato algum. A promotoria alegou, contudo, que teve sorte ao encontrar um erro na página do Silk Road, que vazou o IP do site, ligando Silk Road a Ross Ulbricht, identificado como responsável pela página. (BERTRAND, 2015).

E mesmo com todo este trabalho para impedir a operação do Silk Road, em 28/08/2016 – data da escrita deste trecho – encontravam-se em perfeito funcionamento dois substitutos do Silk Road na Deep Web, podendo ser acessados, por meio do navegador TOR, pelos links “reloadedudjtjvxr.onion” e “http://cryptomktgxdn2zd.onion/signin.php”. Também o próprio sistema de trocas do Bitcoin segue suas operações em âmbito global, possibilitando a realização de transferências de valores, legais ou não, de forma que apenas os envolvidos na transação tenham ciência deste quesito.

[2] We will never be able to de-anonymize all Tor users all the time.

5. A CRIPTOGRAFIA NÃO É INFALÍVEL

Por certo, a criptografia não é inviolável. A "força bruta" é aplicada para tentar encontrar a chave que desvende a proteção da informação.

Este processo consiste em testar todas as alternativas possíveis para desbloquear a chave que revele a informação. Considere um simples sistema de PIN de acesso à tela inicial de um smartphone: o código consiste em quatro dígitos, de zero a nove. Aplicando-se a análise combinatória, é possível perceber a existência de 10.000 possibilidades de senha, que deverão ser testadas individualmente até que seja desbloqueada a senha de acesso.

Tal operação beira a impraticidade no âmbito manual, mas é mais facilmente executada por um computador programado para tal. Todavia, à medida que a criptografia é aperfeiçoada, torna-se cada vez mais difícil, se não impossível, violá-la.

Em 2008, Daniel Dantas teve discos rígidos apreendidos na operação Satiagraha, da Polícia Federal. Contando com dados criptografados por meio de programas disponíveis na internet, o sistema de proteção permanece inviolado até a data de hoje, sendo relevante considerar que nem mesmo o FBI foi capaz de encontrar uma brecha na criptografia. (MORENO, 2010).

6. CONSEQUÊNCIAS PARA O ESTADO E AS ESFERAS DE REGULAÇÃO

Conceitua Dallari (2011, pág. 90) que soberania, além de ser elemento fundamental para a existência do Estado moderno, consiste em deter o mais alto poder jurídico em dada delimitação territorial, ou jurisdição, sendo inquestionável o poder decisório acerca da eficácia de qualquer norma jurídica.

Para o exercício desta soberania, o Estado depende de mecanismos de execução legal que condicionem a liberdade e a propriedade, ajustando ambas ao interesse coletivo. Tal atividade é conhecida como "poder de polícia" (MELLO, 2009, pág. 815) e tem como característica a coercitividade de sua imposição (MELLO, 2009, pág. 824). Contudo, é o território o elemento responsável pela delimitação da ação soberana do Estado (DALLARI, 2011, pág. 95) e, logo, do poder de polícia.

Todavia, os novos desafios impostos pela criptografia estabelecem confrontos diretos em relação a tal conceituação.

6.1 TERRITORIALIDADE

Aliando a tecnologia do navegador TOR à transação de Bitcoins, um cidadão comum pode, a partir de alguns poucos comandos, fazer valores exorbitantes transitarem globalmente, de forma anônima, passando por uma infinidade de jurisdições diferentes, implicando em custos burocráticos para investigações e mesmo desavenças quanto ao poder investigativo e de polícia na ausência de tratados internacionais para tanto.

Mas uma das consequências mais preocupantes é a dificuldade ou impossibilidade de estabelecer vinculos, para fins jurídicos, entre o agente, a ação que executa, seus resultados e a ligação de todos os anteriores a jurisdições específicas, haja vista a possibilidade de permanecer em quase absoluto anonimato online, o que parece complementar a observação de Post et al (1996, pág. 1370) quando indicam que não há limites territoriais ao ciberespaço, dado que a transmissão e o custo para a transmissão de dados são quase inteiramente independentes de localidades físicas.

Isto resulta na flexibilização do poder coercitivo do Estado que, condicionado a um conceito de territorialidade que vem se provando impróprio para lidar com novas tecnologias, caminha para a obsolescência quanto à aplicação e eficácia de suas normas à medida que inovações baseadas em criptografia são incorporadas ao cotidiano, estabelecendo desafios para o ordenamento jurídico vigente que, limitado a um território específico, deixa de ser acionado por conta da incapacidade de reconhecer os locais de origem de ações relevantes, assim como os locais onde seus resultados surtem efeitos.

6.2 REGULAÇÃO DA ATIVIDADE ECONOMICA

Em outro *front* da questão, define a Constituição Federal de 1988 que a ordem econômica está sujeita, entre outros, à observação da soberania nacional e tem por objetivo assegurar a todos uma existência digna, conforme os ditames da justiça social.

Assim, o Estado poderá intervir na ordem econômica de três maneiras: impondo normas com seu poder de polícia; criando incentivos e estímulos fiscais; e atuando empresarialmente (MELLO, 2009, pág. 789). Mas como verificado no item anterior, o poder de polícia do Estado tende a se flexibilizar como consequência direta de problemas de jurisdição e territorialidade.

De forma similar, a criação de incentivos e estímulos, execução de políticas fiscais e cambiais, emissão de moeda, fixação de taxas de juros básico e muitas outras operações típicas

de um sistema financeiro moderno tradicional condicionado à soberania nacional também tenderão à impossibilidade à medida que as pessoas passem a usar moedas não vinculadas a um Estado, como o Bitcoin.

No atual estado da tecnologia e de sua regulação, os governos não podem inflacionar Bitcoins emitindo mais moedas, não podem se apropriar da rede Bitcoin ou tampouco desvalorizar a moeda em relação às demais (ULRICH, 2014, pág. 105), pois que a rede de Bitcoins, além de ser descentralizada, é mantida por um grande número de usuários que contribuem com o poder de processamento de seus computadores para garantir proteção e legitimidade às transações (ULRICH, 2014, pág. 19), o que também limita o alcance do Estado para intervir de formas tradicionais na economia.

7. CONSIDERAÇÕES FINAIS

Constata-se, portanto, que os desafios impostos pelo avanço das tecnologias criptográficas representam uma verdadeira ameaça ao Estado moderno, haja vista que os conceitos de territorialidade e jurisdição vão se tornando cada vez mais ultrapassados para lidar com as exigências e encargos de tais inovações.

Assim, o Estado tenderá a exercer cada vez menos controle em sistemas protegidos por criptografias avançadas, ou outras tecnologias que o valham, resultando na paulatina esfacelação de seu poder de polícia e de seu poder regulatório econômico e na eventual fragmentação de sua própria soberania, restando ao Estado agir cada vez mais enquanto ente privado entre os demais e cada vez menos como ente detentor do máximo poder jurídico.

Conclui-se, pois, que a criptografia representa, de fato, uma ameaça para o exercício das competências do Estado, que tende a ter seu poder soberano paulatinamente fragilizado e, desde já, mostra-se carente de novas propostas e soluções para que mantenha seu status de soberano.

8. REFERÊNCIAS

BERTRAND, Natasha. **The case against Silk Road's 31-year-old founder was unprecedented**. Disponível: <http://www.businessinsider.com/the-case-against-silk-road-founder-ross-ulbricht-was-unprecedented-2015-5>. Acesso em: 04 ago. 2016.

DALLARI, Dalmo de Abreu. **Elementos de teoria geral do Estado**. 30. ed. São Paulo: Saraiva. 2011.

ESTES, Adam Clark. **Tor: a internet anônima é o que você realmente precisa?** Disponível em: <http://gizmodo.uol.com.br/giz-explica-tor/>. Acesso em: 28 ago. 2016.

FRIEDMAN, Milton. **Milton Friedman Predicts the rise of Bitcoin in 1999!** 0'08". Disponível em: <https://www.youtube.com/watch?v=6MnQJFEVY7s>. Acesso em: 28 ago. 2016.

GUGUELMIN, FELIPE**. Silk Road: história da loja virtual underground vai virar filme**. Disponível em <http://www.tecmundo.com.br/cinema/45876-silk-road-historia-da-loja-virtual-underground-vai-virar-filme.htm>. Acesso em: 28 ago. 2016.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca. (**Re)pensando a pesquisa jurídica: teoria e prática.** 3. ed. Belo Horizonte: Del Rey, 2010.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 26. ed. São Paulo: Malheiros Editores. 2009.

MICROSOFT. **Data encryption and decryption**. Disponível em < https://msdn.microsoft.com/pt-br/library/windows/desktop/aa381939(v=vs.85).aspx>. Acesso em: 28 ago. 2016.

MORENO, João Brunelli. **Nem FBI consegue quebrar criptografia de banqueiro brasileiro**. Disponível em < https://tecnoblog.net/29192/nem-fbi-consegue-quebrar-criptografia-de-banqueiro-brasileiro/>. Acesso em: 28 ago. 2016.

NATIONAL SECUTIRY AGENCY. **Tor stinks**. Disponível em: < https://edwardsnowden.com/wp-content/uploads/2013/10/tor-stinks-presentation.pdf>. Acesso em: 28 ago. 2016.

POST, David et al. **Law and borders – The rise of law in cyberspace**. Stanford Law Review. Califórnia, v. 48, n.5, maio. 1996.

TOR PROJECT. **Overview**. 2016. Disponível em < https://www.torproject.org/about/overview.html.en#overview>. Acesso em: 28 ago. 2016.

TOR PROJECT. **Yes, we know about the guardian article**. 2013. Disponível em < https://blog.torproject.org/blog/yes-we-know-about-guardian-article>. Acesso em: 28 ago. 2016.

ULRICH, Fernando. **Bitcoin - A moeda na era digital**. São Paulo: Instituto Ludwig Von Mises Brasil. 2014.

WITKER, Jorge. **Como elaborar una tesis en derecho: pautas metodológicas y técnicas para el estudiante o investigador del derecho**. Madrid: Civitas, 1985.