CESED - CENTRO DE ENSINO SUPERIOR E DESENVOLVIMENTO
UNIFACISA – CENTRO UNIVERSITÁRIO
CURSO DE BACHARELADO EM DIREITO

LEONARDO VENTURA VILAR

A BARBÁRIE DOS CRIMES CIBERNÉTICOS COMETIDOS NA *DARK WEB* E A PARTICIPAÇÃO DIRETA DO *BITCOIN* COMO MEIO DE PAGAMENTO

CAMPINA GRANDE
2020

LEONARDO VENTURA VILAR

A BARBÁRIE DOS CRIMES CIBERNÉTICOS COMETIDOS NA *DARK WEB* E A PARTICIPAÇÃO DIRETA DO *BITCOIN* COMO MEIO DE PAGAMENTO

Trabalho de Conclusão de Curso - Artigo Científico – apresentado como pré-requisito para obtenção do título de Bacharel em Direito pela UniFacisa – Centro Universitário.
Área de Concentração: Direito Privado/ Direito da Propriedade Intelectual, mídia, tecnologia e inovação.
Orientador: Prof.º Dr. João Ademar de Andrade Lima.

CAMPINA GRANDE – PB

2020

FICHA CATALOGRÁFICA

Trabalho de Conclusão de Curso - Artigo Científico – A BARBÁRIE DOS CRIMES CIBERNÉTICOS COMETIDOS NA *DARK WEB* E A PARTICIPAÇÃO DIRETA DO *BITCOIN* COMO MEIO DE PAGAMENTO, como parte dos requisitos para obtenção do título de Bacharel em Direito, outorgado pela UniFacisa – Centro Universitário.

APROVADO EM_____/_____/_____

BANCA EXAMINADORA:

_____

Prof.º da UniFacisa,
João Ademar de Andrade Lima, Dr.
Orientador

_____

Prof.º da UniFacisa, Nome Completo do
Segundo Membro, Titulação.

_____

Prof.º da UniFacisa, Nome Completo do
Terceiro Membro, Titulação.

A BARBÁRIE DOS CRIMES CIBERNÉTICOS COMETIDOS NA *DARK WEB* E A PARTICIPAÇÃO DIRETA DO *BITCOIN* COMO MEIO DE PAGAMENTO

Leonardo Ventura Vilar[1]
João Ademar de Andrade Lima[2]

RESUMO

Apesar de trazer diversos benefícios para a sociedade, o ciberespaço pode ser um ambiente propício para a prática de crimes virtuais, os chamados cibercrimes. Desse modo, o presente estudo tem como objetivo analisar as potencialidades as quais a *dark web* e o *bitcoin* possuem e podem embaraçar a determinação de autoria em crimes cibernéticos. A temática abordada no artigo se mostra relevante pela necessidade de redirecionamento das autoridades para os novos meios de cometer crimes, e assim, reaver os métodos contemporâneos de combate ao cibercrime buscando técnicas que tornem a web um lugar seguro e garantir a aplicação da lei penal no ciberespaço. Haja vista que os cibercrimes cometem crimes bárbaros e permanecem impunes em virtude das técnicas para não ter sua identidade revelada. O presente artigo é de natureza predominantemente bibliográfica, de caráter qualitativo, exploratório e dedutivo. Nesse sentido, foram escritos quatros tópicos, primeiramente analisandos a cibercultura, bem como o cibercrime; depois distinguindo as camadas da internet; logo após desmistificando a tecnologia bitcoin e sua aptidão para funcionar como meio de pagamento e manter o anonimato; e, por fim, discutiram-se as potencialidades das tecnologias para funcionar concomitantemente em busca do incremento ao anonimato dos cibercrime, bem como a importância das autoridades se atualizarem para reprimir os novos tipos de crime, ou seja, o cibercrime.

PALAVRAS-CHAVE: Direito. Crimes Cibernéticos. Deep Web. *Dark web*. *Bitcoin*. Anonimato.

ABSTRAC

Despite bringing several benefits to society, cyberspace can be a favorable environment for the practice of virtual crimes, the so-called cybercrimes. Thus, this study aims to analyze the potential that the dark web and bitcoin have and can hinder the determination of authorship in

[1] Graduando do Curso Superior em Direito. leoventur@live.com
[2] Professor Orientador. Graduado em Direito pela Universidade Federal da Paraíba (UFPB) e em Computação pelo Centro Universitário Claretiano. Doutor em Ciências da Educação pela Universidade de Trás-os-Montes e Alto Douro. Docente do Curso Superior em Direito da UNIFACISA das disciplinas de Direito de Propriedade Intelectual, Direito Digital, Ética e Direito Aplicado à Informática e Introdução ao Estudo do Direito.

cybercrime. The theme addressed in the article is relevant due to the need to redirect authorities to new ways of committing crimes, and thus recover contemporary methods of combating cybercrime, seeking techniques that make the web a safe place and ensure the application of criminal law in cyberspace. Given that cybercrimes commit barbaric crimes and remain unpunished due to the techniques for not having their identity revealed. This article is predominantly bibliographic in nature, qualitative, exploratory and deductive. In this sense, four topics were written, firstly analyzing cyberculture, as well as cybercrime; then distinguishing the layers of the internet; shortly after demystifying bitcoin technology and its ability to function as a means of payment and maintain anonymity; and, finally, the potential of technologies to work concomitantly in search of increasing the anonymity of cybercrime was discussed, as well as the importance of the authorities updating themselves to repress new types of crime, that is, cybercrime.

KEYWORDS: Right. Cyber Crimes. Deep Web. Dark web. Bitcoin. Anonymity.

1 INTRODUÇÃO

Diante das novas tecnologias temos novas formas de comunicação e até mesmo de transacionar o dinheiro, o ciberespaço tem proporcionado maior conforto na vida de seus usuários e tem tornando cada vez mais o mundo globalizado. No entanto, as novas tecnologias também ofereceram para as organizações criminosas novos métodos de cometer atos ilícitos caracterizando o cibercrime. Em virtude das novas formas de cometer crimes surge um debate acerca da eficácia dos métodos investigativos das autoridades.

Recorrentemente podemos observar que as autoridades anunciam que o cibercrime não é um método seguro para cometer crimes em virtude da fácil identificação dos usuários que cometem crimes através das redes. As autoridades buscam desestimular o cibercrime com afirmações neste sentido e de fato é uma afirmação verdadeira, mas existe uma certa disparidade entre o cibercrime desleixado e o experiente.

O cibercrime experiente não utiliza os meios de acesso tradicionais para ter acesso ao ciberespaço. A internet é complexa e dispõe de várias camadas que não tem a atenção das autoridades investigativas. Dentre as novas tecnologias empregadas como meio para o

cometimento de cibercrimes das mais variadas espécies citamos o *bitcoin* que resumidamente funciona como meio de pagamento.

Os crimes bárbaros que ocorrem no ciberespaço não estão incluídos no debate público, bem como no noticiário. As variedades dos crimes são impressionantes. A necessidade da atenção global voltada para as novas tecnologias a fim de impor medidas que desestimulem de fato o cibercrime são urgentes não bastando afirmações rasas e sem fundamentos por parte das autoridades.

A Lei nº 12.735, de 30 de novembro de 2012 em seu Art. 4º, demonstra total preocupação no combate aos crimes cibernéticos de modo que obriga os órgãos responsáveis desenvolver setores e equipes especializadas no combate aos cibercrimes.

Com base no exposto, indagou-se nesta pesquisa se as camadas da web é um lugar seguro para a prática do cibercrime; se o *bitcoin* possui potencialidades para servir como meio de pagamento no ciberespaço, tendo em vista as afirmações da inexistência do anonimato por parte das autoridades e da sociedade; se o mercado da *dark web* possui aptidão para funcionar concomitante ao *bitcoin*; e se as potencialidades das tecnologias trazem desafios para as autoridades investigativas.

O presente artigo teve como proposta e objetivo geral analisar as medidas e circunstâncias as quais a *dark web* e o *bitcoin* podem embaraçar a determinação de autoria em crimes cibernéticos.

Para responder a problemática levantada nesta pesquisa, foram elencados os seguintes objetivos específicos: I - Apresentar a natureza jurídica dos crimes cibernéticos; II - conhecer sob uma perspectiva teórico-conceitual os princípios da *dark web* e seu suposto anonimato; III - estudar o *bitcoin*, bem como o suposto anonimato e sua descentralização; IV - discutir até que ponto as potencialidades das tecnologias estudadas podem embaraçar a determinação de autoria em crimes cibernéticos.

A importância do tema consiste na inserção dos operadores do direito das novas práticas criminosos na *web*, especificamente, na *dark web*, local que impera a anarquia, o anonimato, a desregulamentação estatal e, principalmente, agentes intencionados em cometer crimes das mais variadas espécies. Não obstante, é imprescindível criar um debate acerca do assunto entre os operadores do direito com a finalidade de que sejam levantados questionamentos argumentativos quanto a coibição dos crimes cibernéticos e o anonimato dos agentes

praticantes, os quais se utilizam de tecnologias inovadoras e sofisticadas, proporcionando aos mesmos um ambiente virtual supostamente seguro para a prática dos seus delitos.

Além do exposto, o presente estudo debruça-se em contribuir com as atuais discussões e soluções acerca da utilização de criptoativos como meio de pagamento para as práticas de cibercrimes, visto que ainda são poucos os estudos e contribuições teóricas que tratam das consequências dos avanços tecnológicos sobre os crimes cibernéticos e o fator potencializados da utilização de uma moeda a qual não possua a regulamentação e emissão pelo Estado.

Sendo assim, o presente trabalho foi dividido em quatro tópicos, partindo da natureza jurídica do ciberespaço e cibercrime, bem como da distinção da *deep web* e da *dark web* que facilmente podem ser confundidas, além de analisar o funcionamento da tecnologia *bitcoin* no ciberespaço mais profundo da *web*, e ainda, analisar a eficácia dos métodos empregados que buscam o anonimato no ciberespaço; por fim, finalizando o debate acerca do suposto anonimato das tecnologias estudadas, bem como a importância das autoridades mundiais remeter sua atenção para este ciberespaço que cada vez traz inovações e técnicas sofisticadas que exigem maior especialização por parte dos órgãos investigativos.

2 O CIBERESPAÇO E OS CRIMES CIBERNÉTICOS

2.1 CONCEITUAÇÃO DO CIBERESPAÇO

Para que se possa iniciar um diálogo acerca do ciberespaço e os crimes que ocorrem nesse meio, se faz necessário conceituar o que é ciberespaço. À medida que as tecnologias e a própria sociedade evoluem, criam-se novas tecnologias com o intuito de abranger a leitura e a escrita, inicialmente. Nesse sentido, o ciberespaço transforma letras, que são sensíveis e concretas, em *bytes* digitais. Tudo funciona de forma diferente, pois a página em branco é a página do software utilizado para textos – como *Word* ou *Google Docs* – e a caneta torna-se o teclado; o texto deixa de ser palpável e torna-se virtual, até que passe, ou não, para uma página impressa, ele está em um campo virtual – o ciberespaço (MONTEIRO, 2007).

Isto posto, pode-se entender que o ciberespaço é um espaço virtual, presente em quase todos os ambientes na sociedade atual – seja por meio de smartphones, computadores, entre outras tecnologias.

Ainda em busca do conceito de ciberespaço, cientificamente, LÉVY (2000) preceitua que este é um espaço de comunicação aberto pela conexão e interconexão da rede mundial de computadores (*World Wide Web*), juntamente com a memória dos computadores. Essa

definição mais ampla do autor ainda agrega o "o conjunto dos sistemas de comunicação eletrônicos (aí incluídos os conjuntos de rede hertzianas e telefônicas clássicas), na medida em que transmitem informações provenientes de fontes digitais ou destinadas à digitalização" (MONTEIRO, 2007, n. p.).

Sobre o local de existência do ciberespaço, Souza *et al* (2013) sugeriu que:

> O ciberespaço existe em um local indefinido, desconhecido e, dentro de tal obscuridade, encontramos uma série de incertezas e possibilidades. Apesar das dúvidas e inseguranças, o ciberespaço tem se tornado a principal referência geográfica utilizada para conectar pessoas, organizações, empresas e diversos grupos sociais. Esta modalidade de ambiente – a dimensão virtual – tem alcançado e promovido a globalização, a participação social, inserção do indivíduo no mundo das informações e o exercício da cidadania (SOUZA *et al*, 2013, p. 5)

LÉVY (2000) ainda levantou hipóteses de como o ciberespaço iria preencher a vida humana nos próximos séculos, o que de fato está ocorrendo atualmente, quando arguiu que:

> Esse novo meio tem a vocação de colocar em sinergia e interfacear todos os dispositivos de criação de informação, de gravação, de comunicação e de simulação. A perspectiva da digitalização geral das informações provavelmente tornará o ciberespaço o principal canal de comunicação e suporte de memória da humanidade a partir do próximo século. (LÉVY, 2000, p. 92-93).

Assim, é importante ressaltar a ocupação dos meios de comunicação em massa, mesmo que de forma virtual, a partir do ciberespaço. A grande maioria dos métodos de comunicação atuais são baseados no ciberespaço, e é por isso que surge a cibercultura.

2.2 CIBERCULTURA E AS INFLUÊNCIAS NO ÂMBITO DO DIREITO

A comunicação digital gerou um novo comportamento humano. A interação entre milhões de pessoas de todos os horizontes através de um caótico mundo virtual criou novas formas de pensar. A cibercultura representa esse conjunto de transformações sociais que têm sua origem no desenvolvimento do ciberespaço. Com a informatização social, no início dos anos 1970, o mundo digital evolui e adentra cada vez mais as casas das pessoas. Nesse sentido, quando o século XXI se inicia, também começa uma nova fase social, chamada de sociedade da informação. Este novo mundo conectado é um dos grandes desafios da filosofia contemporânea.

A natureza planetária do mundo virtual indica que a cibercultura não está condicionada pelos mesmos fatores que a cultura tradicional – como religiões, tradições e contextos locais. A cibercultura não é representante de uma determinada cultura. É uma nova cultura formada

pela integração de várias culturas e condicionada por fatores tecnológicos. Esse mundo virtual tem uma tendência anárquica; não obedece ordens ou hierarquias. Sua origem se deu através da fusão de iniciativas isoladas. Iniciou com a criação dos primeiros computadores, passando pela popularização dos computadores pessoais, seguindo até a criação das primeiras redes. Depois disso, temos a impressão que o mundo virtual criou vida própria. No entanto, essa é uma falsa impressão. O fermento que faz crescer o ciberespaço é nossa necessidade de comunicação.

Essa sociedade, baseada principalmente pela popularização da internet e da computação sem fio, como os sistemas *Wi-Fi*, *Bluetooth* e 4G (e até 5G, a partir do ano de 2018), por exemplo, criam profundas transformações que culminam em uma nova cultura, chamada de cibercultura (LEMOS, 2013).

Lemos (2002) afirma que "a cibercultura solta as amarras e desenvolve-se de forma onipresente, fazendo com que não seja mais o usuário que se desloca até a rede, mas a rede que passa a envolver os usuários e os objetos numa conexão generalizada" (LEMOS, 2002, n.p.).

Sobre a era que estamos vivendo, Lemos (2013) ainda traz que

> Estamos na era da conexão. Ela não é apenas a era da expansão dos contatos sobre forma de relação telemática. Isso caracterizou a primeira fase da internet, a dos "computadores coletivos" (CC). Agora temos os "computadores coletivos móveis (CCm) (LEMOS, 2013, n. p.).

Isto posto, com a conectividade e a mobilidade em pleno desenvolvimento, a internet sem fio e os smartphones de última geração fazem com que os pensadores contemporâneos desenvolvam novos pensamentos acerca da privacidade, da privatização e do acesso e relação com os espaços públicos. Nesse sentido, não somente os pensadores, mas também os legisladores e juristas devem adaptar as legislações à medida que a sociedade se modifica. Desse modo, um exemplo de legislação que é diretamente ao ciberespaço e a cibercultura é a LEI Nº 12.965, DE 23 DE ABRIL DE 2014, conhecida como Marco Civil da Internet Brasileira, a qual dispõe sobre princípios, garantias, direitos e deveres para o uso da internet no Brasil, determinando diretrizes para a atuação em todo o território nacional, com suas particularidades.

Inclusive, a legislação citada define o uso da internet no Brasil de forma a oferecer o direito de acesso à internet de todos, conforme prescreve em seu Art. 4º:

> A disciplina do uso da internet no Brasil tem por objetivo a promoção: I - do direito de acesso à internet a todos; II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e IV -

> da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Todos esses processos que envolvem garantia ao acesso e democratização do mesmo fazem parte do conceito de cibercultura. Também é importante se ater às palavras de Souza et al, quando afirmam que:

> O ciberespaço constitui, portanto, um espaço de práticas sociais cuja função não é a de inibir ou acabar com práticas antigas; a escola virtual, como forma de organização do ensino, substituindo a escola real, a comunidade virtual como substituta da comunidade real, e pôr fim a cidade virtual em substituição a cidade real (SOUZA et al, 2013, p. 7).

Portanto, o ciberespaço não deseja excluir práticas antigas e sim agregar essas práticas em um ambiente virtual, saudável, de comunicação e cultura, de cidadania, de oferecer informações mais rápidas e práticas, com uma acessibilidade cada vez maior. O ciberespaço e a cibercultura ampliam as possibilidades de democratização, ou disseminação de políticas públicas, formas diretas de participação do povo, facilitação de acessos, divulgação e troca de informações (LÉVY, 2000).

Porém, apesar do mencionado, o ciberespaço e a cibercultura abrem um novo campo, de forma virtual, para a prática de condutas ilícitas. Essas práticas ilícitas podem ser feitas através da própria *web*, por meio de golpes e crimes por meio das camadas mais profundas da internet, como a *dark web*.

2.3 CIBERCRIMES

Os crimes cibernéticos tem se tornado cada vez mais frequente e podemos afirmar que será um tema muito debatido na contemporaneidade. O Governo dos Estados Unidos fez um pronunciamento afirmando que se reunira com trinta países para debater acerca dos crimes cibernéticos especialmente os casos de ransomware, ou seja, os crimes de sequestro de dados, entre diversos outros, e ainda, buscar impedir a utilização ilícita de criptoativos (PODER360, 2021).

Para prosseguir com esta pesquisa, é necessário conceituar os crimes cibernéticos que, segundo (Peck, P. P,2020, p. 11), são os crimes praticados em ambiente virtual com utilização de internet, o computador é uma ferramenta dispensável para que o crime ocorra em ambiente virtual, haja vista que pode ocorrer através de outros dispositivos eletrônicos também, sendo o fator mais relevante os conhecimentos tecnológicos e ferramentas que possibilitem executar os crimes. O pensamento do Autor (NASCIMENTO, 2019, p.6), baseado com o entendimento da

INTERPOL, é no mesmo sentido: “No que tange a conceituação, cibercrime (INTERPOL, 2015) é a atividade criminosa ligada diretamente a qualquer ação ou prática ilícita na internet”.

Os tipos de crime são diversos, podemos afirmar que não existem limitações para as práticas criminosas no ciberespaço conforme a classificação a seguir;

Os crimes impróprios são os crimes praticados no mundo físico ou material como no ciberespaço.

Os crimes próprios são os cometidos no ciberespaço, ou seja, é necessário que ocorra em um ambiente virtual para que o crime seja consumado.

Dentre os crimes, como apontado anteriormente, são diversos, para exemplificar podemos citar os seguintes;

Ataque de ransomware (tipo de ataque cibernético), ataques cibernéticos (onde os hackers acessam dados do governo ou da empresa), roubo e venda de dados da empresa, fraude de identidade (roubo e uso de informações pessoais), lavagem de dinheiro (utilizando criptoativos), pornografia infantil (utilizando a dark web) calúnia, e difamação.

Dentre as motivações para o cometimento dos crimes cibernéticos, é possível pontuar o suposto anonimato, ou seja, a percepção de preservação de identidade diante dos aparatos tecnológicos que proporcionam o cometimento de crimes de amplitude internacional; é notório que dentro do território brasileiro, é possível cometer um crime em ambiente virtual com resultado em outro país, a exemplo, o crime de sequestro de dados.

3 A *DARK WEB* E SUAS CAMADAS

Ordinariamente, é utilizado por doutrinadores a imagem de um *iceberg* para ilustrar as camadas da internet, que se dividem em: *surface web*, *deep web* e *dark web*.

A *surface web*, considerada como a primeira camada da *web*, representa entre 6% e 10% de toda a internet, sendo constituída por páginas, sites e conteúdo que utilizam a arquitetura de redes de clientes e servidor, ou seja, existem determinadas máquinas criadas apenas para promover serviços aos clientes; tais páginas hospedam páginas *web* de acesso básico como serviços de e-mail, banco de dados, arquivos e diversos serviços que fazem parte do cotidiano de pessoas comuns (BARRETO E SANTOS, 2019, p. 17).

Segundo Barreto e Santos, "A *deep web* é, portanto, composta por redes de computadores que têm como características o anonimato, a criptografia, a descentralização e a codificação aberta, e cujo conteúdo não é 'visível' pelas ferramentas de busca convencionais." (BARRETO E SANTOS, 2019, p. 19).

Em se tratando da segunda camada, a *deep web* é onde as informações são armazenadas para manutenção da rede e não são facilmente acessíveis, ou seja, é onde se encontram as informações que só podem ser acessadas por pessoas que possuem os endereços e credenciais exigidas, a exemplo, o banco de dados acadêmicos e registros médicos.

A *dark web*, considerada a terceira e última camada da *web*, tem sua utilização justificada em seu anonimato de alto nível, que proporciona uma suposta segurança aos usuários. Com palavras certeiras, Barreto e Santo conceitua o seguinte:

> [...] A dark *web*, ou *darknet*, é a rede da *deep web* ou parte dela com características de um alto grau de anonimato e segurança exigido e é utilizada, como regra, para o cometimento de ilícitos criminais e práticas escusas. É empregada por usuários de internet, ativistas políticos, hackers e criminosos, notadamente por garantir privacidade nas comunicações e/ ou a não aplicação da lei penal (BARRETO E SANTOS, 2019, p. 21).

A *dark web* é uma camada da *web* que não é acessível por meio de navegadores padrão, como *Google Chrome* ou *Mozilla Firefox*. Qualquer tipo de informação pode ser encontrado na *dark web*; ela só é *dark*, palavra em inglês que significa sombrio, escuro, devido a sua acessibilidade mais limitada. Em apertada síntese a *dark web* consiste em sites que ocultam os endereços de IP da Internet. Para acessar os sites da *dark* na *web* é necessário um navegador criado para este fim e desta maneira o usuário que acessa os sites pretendidos tem o seu endereço de IP oculto no próprio site.

Para acessar esses tipos de redes, existem diversos métodos, mas o padrão é o navegador denominado como Tor (*The Onion Routing*). No entanto, não basta acessar o navegador, é preciso identificar os endereços desejados, não possuindo o mesmo mecanismo de busca utilizado pelo *Google*, que ao pesquisar qualquer palavra, surgem diversos resultados. A sútil diferença da *deep web* e *dark web* consiste que a última é utilizada, em muitos casos, para a prática de crimes, enquanto a *deep web* é destinada para a manutenção da rede.

O funcionamento do navegador Tor envolve os dados em várias camadas de criptografia (como uma cebola) e os envia por uma rede de "roteadores cebola". A palavra "cebola" indica as camadas que os dados devem penetrar: ao contrário da navegação normal, o computador não se conecta diretamente ao servidor no qual o site está localizado. Em vez disso, vários servidores estão envolvidos na conexão para garantir o maior anonimato possível.

Cada roteador pelo qual os dados passam retira a camada de criptografia e envia uma mensagem parcialmente descriptografada ao próximo destino. Esse processo se repete até que a mensagem chegue ao destino desejado. Essa técnica mantém o anonimato da *dark web*, mas é consideravelmente mais lenta. (BUENO, 2020).

Para exemplificar o funcionamento da rede Tor, foram destacadas as três camadas que a compõe:

A primeira camada: ponto de entrada (servidor 1) se dá pela rede Tor (*The Onion Router*), a qual contém o endereço IP do computador do usuário. Com isso, a rede Tor conecta o computador do usuário a outro servidor (servidor 2), também chamado de nó. Todos os dados trafegados são criptografados, criando uma ponte entre o computador do usuário e o nó.

A segunda camada: nó Tor (servidor 2) tem apenas conhecimento do nó de entrada, porém, não do seu computador e tampouco do endereço de IP. Os dados trafegados por meio dele são criptografados e, com isso, não é possível que haja leitura dos dados pelo nó. Além do ponto de entrada, o nó da rede Tor conhece apenas o próximo nó, também chamado de nó de saída (servidor 3), isto é, o servidor que efetivamente irá conectar o usuário ao site que deseja acessar na *dark web*.

A terceira camada: nó de saída (servidor 3) estabelece uma conexão real com o servidor da *web*, permitindo que a página de destino desejada seja localizada. A partir do nó de saída, é possível chegar aos serviços legítimos que terminam com .onion, a exemplo. Os serviços com o sufixo de domínio .onion não podem ser acessados se não pela rede Tor.

Percorrido todas as camadas descritas acima, a jornada em busca do objetivo na *dark web* está concluída e o usuário poderá ter acesso a página que deseja; a mesma é armazenada no servidor *web*. Por fim, o servidor *web* conhece apenas o endereço IP do nó de saída e não o originário, sejam os demais servidores ou do próprio computador do usuário.

O acesso a *dark web* em si não é ilegal. Afinal, a *dark web* serve apenas para fornecer o anonimato, no entanto, há opiniões mediáticas de que ela promove atividades ilegais. Fatos também contribui para pensamentos neste sentido, o caso Skill Roads que foi descoberto pelas autoridades era um mercado negro funcionando plenamente na *dark web* oferecendo serviços ilícitos e recebia como pagamento o *bitcoin*.

4 O *BITCOIN* E SUAS PARTICULARIDADES

O *bitcoin* foi criado no ano de 2008 por Satoshi Nakamoto, que até os dias atuais não teve sua identidade revelada. Para melhor compreensão da tecnologia é necessário conceituá-lo. A princípio, é possível destacar que o *bitcoin* possui imensa popularidade e pioneirismo em transações digitais, tendo inovado a forma como os "dinheiros" são transacionados. É importante salientar que existem diversos criptoativos, mas que não deixam de ser utilizados por cibercriminosos, especificamente a *Monero*, a qual proporciona maior grau de privacidade aos seus usuários, mas suas peculiaridades não serão tema central desta pesquisa.

Exemplificando o que é o *bitcoin*:

> [...] *bitcoin* é uma forma de dinheiro, assim como o real, o dólar ou o euro, com a diferença de ser puramente digital e não ser emitido por nenhum governo. O seu valor é determinado livremente pelos indivíduos no mercado. Para transações *online*, é a forma ideal de pagamento, pois é rápido, barato e seguro. Você lembra como a internet e o e-mail revolucionaram a comunicação? Antes, para enviar uma mensagem a uma pessoa do outro lado da Terra, era necessário fazer isso pelos correios. Nada mais antiquado. Você dependia de um intermediário para, fisicamente, entregar uma mensagem. [...] O que o e-mail fez com a informação, o *bitcoin* fará com o dinheiro. Com o *bitcoin* você pode transferir fundos de A para B em qualquer parte do mundo sem jamais precisar confiar em um terceiro para essa simples tarefa. É uma tecnologia realmente inovadora (ULRICH, 2014, p. 15).

Segundo o autor, o *bitcoin* é uma tecnologia que busca revolucionar o sistema financeiro, substituindo o papel-moeda, o qual, no Brasil, é produzido a partir de solicitações do Banco Central à casa da moeda, de modo a nutrir a macroeconomia do país. Assim, para garantir a legitimidade do dinheiro, o papel-moeda só pode ser emitido através de demandas das principais autoridades monetárias, como o Bacen (Banco Central do Brasil) no caso do Brasil. A Casa da Moeda é responsável pela "fabricação" do dinheiro, sob ordens do Banco Central, que depois distribui a moeda escritural pelos bancos comerciais e instituições financeiras do país.

No mesmo sentido leciona Andreas M. Antonopoulos citado por Telles (2020, p. 23):

> *Bitcoin* é dinheiro digital, mas é muito mais que isso. Dizer que o *bitcoin* é dinheiro digital é como dizer que a internet é um telefone sofisticado. É como dizer que a internet se resume a e-mail. O dinheiro é apenas sua primeira aplicação. O *bitcoin* é uma tecnologia, é uma moeda e é uma rede internacional de pagamentos e câmbios completamente descentralizada. Não depende de bancos. Não depende de governos.

A legislação brasileira por meio da Instrução Normativa Nº 1.888, DE 3 DE MAIO DE 2019, em seu Art. 5, inciso I, conceitua os criptoativo de modo geral:

> criptoativo: a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal; e.

Deste modo, subtraímos dos ensinamentos dos autores e da legislação que o *bitcoin* é uma tecnologia descentralizada que não possui vínculo com nenhuma forma de governo ou autoridade monetária. A velocidade das transações e o baixo custo do *bitcoin* são considerados um dos fatores cruciais para sua utilização, levando em consideração, também, que os usuários podem transferir *bitcoins* em escala global, sem necessidade de instituições financeiras para confirmar as transações.

É importante frisar que o *bitcoin* funciona por *peer-to-peer* (de ponto a ponto), ou seja, igualmente a *deep web* e *dark web*, não existe um servidor central para que seu funcionamento seja eficaz, uma vez que o mesmo se dá por meio de redes de computadores que permitem que cada um dos pontos ou *nós* da rede funcione tanto como cliente quanto como servidor.

O funcionamento da rede ocorre em uma tecnologia denominada "*blockchain*". De acordo com Bueno (2020), a *blockchain* é uma tecnologia de registro de dados imutável em um livro compartilhado, distribuído entre múltiplos pontos que os confirma, ou seja, cada ponto é uma máquina responsável pela manutenção de uma cópia idêntica do livro de registro. Os dados podem ser de diversas naturezas, governos já estudam adotar a tecnologia para registro de dados, mas no caso do *bitcoin*, se trata de um meio de transmissão digital de valores.

A *blockchain* é um método de registro síncrono de dados, com informações de transações, combinando tecnologia criptográfica em vários computadores que formam uma rede distribuída, com isso podemos afirmar que temos várias máquinas espalhadas por todo o globo registrando as transações (minerando) *bitcoin*.

A *blockchain* coleta os dados de transações por um determinado período de tempo em unidades de bloco, verifica uns aos outros entre computadores, conecta e acumula registros

públicos como uma cadeia, se trata de um grande banco de dados que possui o histórico de todas as transações do *bitcoin*. Também conhecido como "razão distribuída". Para que a rede funcione é necessário que todos os pontos mantenham cópias idênticas do livro razão, ou seja, cada operação precisa ser registrada em todas as cópias do livro e em ordem cronológica a fim de evitar o problema de gasto duplo, ou seja, garantir que os *bitcoins* das transação não tenham sido previamente gastos (TELLES, 2020).

A característica mais importante desta tecnologia é que ela é gerenciada de forma descentralizada, não existe um servidor central como os bancos possuem para garantir seu valor, as transações não exigem a participação de um terceiro para que as confirmem. A dúvida que surge é sobre como está *blockchain* funciona quem estaria por trás de todo trabalho para registrar todas as informações e evitar fraude na rede. O trabalho denominado "mineração" é o que contribui para isso, ou seja, é o que permite a descentralização do *bitcoin* e quem desempenha este papel são indivíduos e empresas corporativas engajadas no trabalho de mineração e são chamados também de "mineradores".

Como citado acima a mineração é a tarefa de registrar as transações comerciais do *bitcoin* mas para isso é necessário que os mineiros aprovam os registros de transações utilizando suas máquinas (computadores) para resolver enigmas matemáticos esotéricos e o direito de aprovação é concedido apenas ao mineiro que soluciona o quebra cabeça primeiro, e como recompensa este obtém frações do *bitcoin* após a conclusão do trabalho de aprovação.

Como o funcionamento da rede ocorre de modo descentralizado não existindo o controle de usuários ou até mesmo de transações. Podemos verificar na *blockchain* apenas as transações que ocorreram, mas não significa que conseguimos identificar os usuários que estão movimentando o ativo *bitcoin*.

A criptografia da rede, *bitcoin* é um dos pontos que alavancou o sucesso da tecnologia garantindo que as transações e os dados sejam de conhecimento apenas dos usuários que estão transacionando entre si, ou seja, em apertada síntese a criptografia busca preservar as informações de um terceiro que não esteja na transação.

O funcionamento da rede ocorre na *blockchain* do seguinte modo:

> [...] Tal mecanismo exige que a cada usuário sejam atribuídas duas "chaves", uma privada, que é mantida em segredo, como uma senha, e outra pública, que pode ser compartilhada com todos. Quando a Maria decide transferir *bitcoins* ao João, ela cria uma mensagem, chamada de "transação", que contém a chave pública do João, assinando com sua chave privada. Olhando a chave pública da Maria, qualquer um pode verificar que a transação foi de fato assinada com sua chave privada, sendo, assim, uma troca autêntica, e que João é o novo proprietário dos fundos. A transação – e portanto uma transferência de propriedade dos *bitcoins* – é registrada, carimbada

> com data e hora e exposta em um "bloco" do *blockchain* (o grande banco de dados, ou livro- -razão da rede *bitcoin*). [...] ULRICH, 2014, p. 18).

Exemplificando o exposto podemos comparar a chave pública com um endereço de e-mail, ou seja, para que o usuário envie um e-mail ele necessita de um endereço de identificação e com o *bitcoin* não é diferente está chave pública é necessária para que o *bitcoin* seja enviado para carteira digital pois se trata do endereço desta e de certo modo um meio de autenticidade das transações. A chave privada podemos comparar como uma senha do e-mail, ela é como uma assinatura da transação, ou seja, com ela é possível transacionar os *bitcoin* da carteira digital. Ambas as chaves são imprescindíveis para que uma transação com o *bitcoin* seja realizada (BUENO, 2020).

Podemos pontuar como a próxima características que contribui para a suposta utilização ilícita da tecnologia *bitcoin* o seu caráter transfronteiriço, ou seja, a possibilidade de transferi-lo em escala global e em quantidades exorbitantes para carteiras digitais (*wallet*) ou *exchanges* permitindo a conversão dos criptoativos em qualquer outra moeda local e todo esses fatos podem ocorrer em questões de poucos minutos e com baixo custo de operação.

A inexistência física é outro fator que contribui para sua suposta utilização ilícita. Atualmente os criminosos são presos em flagrante com volumosos de dinheiro em sua residência ou até mesmo em fiscalização de voos internacionais. Nos dias atuais cada vez mais estará em desuso esta prática de transporte de dinheiro ilícito. Criminosos experiente pode converter grandes quantias de dinheiro de papel em um arquivo digital (*bitcoin*) e enviar para qualquer lugar do mundo onde se encontrem uma *exchange* (corretora) ou simplesmente manter em uma carteira digital física que possui um sistema de segurança de ponta.

Dentre as maneiras usuais de ter acesso ao *bitcoin* podemos elencar três: mineração, utilização de serviços de corretora virtual ou receber de outro usuário.

Como elencado anteriormente, a mineração é um processo de registro de dados que tem como consequência a remuneração em frações de *bitcoins* aos mineradores que primeiro solucionem os cálculos.

A segunda alternativa de ter acesso ao *bitcoin* é criando uma conta pessoal em uma corretora virtual denominada (*exchange*) bastante similar as corretoras de investimentos tradicionais, o cliente consegue enviar fundos através de uma conta bancária, depósito por boleto ou até mesmo utilizando o cartão de crédito sem maiores complicações este poderá adquirir diversos criptoativos especialmente, o *bitcoin*. Caso seja necessário, as corretoras convertem o *bitcoin* e diversos criptoativos em moedas locais de diversos países, bem como

oferecem o serviço de guarda seus ativos digitais igualmente uma carteira (*wallet*). É importante ressaltar que para criar uma conta em uma corretora é necessário fornecer informações pessoais.

A terceira maneira de ter *bitcoins* sobre sua custódia é recebendo como destinatário de outro usuário que o tenha. Para isto é necessário que o mesmo crie uma carteira virtual (*wallet*) e forneça seu endereço para o usuário remetente. É uma transação entre indivíduos, sem passar por uma corretora. Mas é um dos métodos mais arriscados considerando que as transações são irreversíveis e as possibilidades de erros de remessa ou problemas financeiros são altas.

Deste modo surge a curiosidade de como obter uma carteira virtual (*wallet*). O usuário pode criar uma carteira através de um software criado para este fim, este tipo de carteira fica hospedada na *web* com o acesso através de um site específico, ou, ainda, usar uma carteira móvel fornecida por aplicativos de *smartphone* e ainda podemos pontuar a carteira que funciona em dispositivos de hardware móveis criada unicamente para este fim. Pouco utilizada, mas não irrelevante, podemos citar a carteira de papel que o usuário possui um papel impresso com o endereço e uma chave privada. Dentre todas as possibilidades devemos ressaltar que não é necessário o fornecimento de documentos pessoais para criação das carteiras virtuais.

5 POTENCIALIDADES DAS TECNOLOGIAS ESTUDADAS NO EMPREGO DO ANONIMATO NA *DARK WEB*

O *bitcoin* foi adotado por alguns comércios legais e o primeiro país a aceitá-lo como moeda oficial foi El Salvador em 2021. Ainda no mesmo ano a China que já baniu o *bitcoin* em outras ocasiões, mas o mercado continuava operando, emitiu um novo comunicado através do Banco Central informando que as transações com criptoativos serão consideradas ilegais, incluindo o *bitcoin*. Desta vez o país proibiu também o funcionamento de sites estrangeiros que ofereçam serviços no país, estes passam a ser criminalizados pelo governo chinês (PODER360, 2021).

A presidente do Banco Central Europeu, Christine Lagarde, durante uma conferência, deixou explícita sua opinião sobre a tecnologia, expondo a necessidade de uma regulamentação a nível global do *bitcoin*, justificada em uma suposta utilização ilícita para os crimes de lavagem de dinheiro e por ser um criptoativo bastante especulativa (PORTAL *bitcoin*, 2021).

As características inerentes ao *bitcoin* são alguns dos fatores que ensejam essas práticas proibitivas por parte dos governos. Para os Estados, não é interessante uma tecnologia descentralizada com um suposto anonimato, alcance global, especulativa e que busca

revolucionar o sistema financeiro; tal postura é enxergada como uma afronta às autoridades mundiais.

Durante todo o trabalho adotamos cuidadosamente o termo suposto anonimato do *bitcoin* em virtude do *Federal Bureau of Investigation* (FBI) que afirma ser possível rastrear as transações com *bitcoin*. É uma afirmativa correta, como afirmado anteriormente todas as transações com *bitcoin* são públicas, imutáveis e podem ser verificadas na *blockchain* por qualquer pessoa.

Observando o recente caso que ocorreu durante a elaboração desta pesquisa podemos confirmar que é possível rastrear as transações com *bitcoin*. O caso ocorreu com a empresa de oleoduto da Colonial Pipeline com sede nos Estados Unidos que sofreu um ataque de cibercriminosos (*hackers*) que sequestraram os dados da empresa e em troca solicitaram o resgate dos dados em pagamento de *bitcoin* e para isto foi necessário os hackers enviar o endereço de sua carteira de *bitcoin* e com isto o FBI juntamente com a empresa realizaram o pagamento e posteriormente rastrearam todas as movimentações que o endereço fornecido pelos cibercriminosos transacionou e de algum modo conseguiram recuperar o valor enviado após acessar a carteira com a chave privada, quebrando a criptografia do *bitcoin* (BRASIL123, 2021).

Mas para que seja possível este tipo de rastreabilidade é preciso ter acesso a chave pública do usuário, ou seja, ao seu endereço *bitcoin* ou de sua carteira digital. Tendo este endereço é possível pesquisar na *blockchain* todas as movimentações que este usuário recebeu/enviou, estarão todas disponíveis para visualização.

Para rastrear as transações de um endereço o interessado deve primeiramente ter o endereço da chave pública como esta; "1P4fz4ARB8eMvtSAYbHCP1UYbN65VPqXY9" ao obter o código o próximo passo é acessar o site *Blockchain*.com para pesquisar a chave e deste modo ter acesso a todas movimentações do endereço pesquisado, bem como aos valores transacionados e para quais endereços foram enviados.

Com isto todos os outros endereços que transacionou com o pesquisado terá sua chave pública exposta e deste modo verificamos um certo tipo de rastro público. É importante ressaltar que possuir o endereço público de uma carteira não significa ter acesso e permissão para transacionar os ativos que ali se encontram, é possível apenas realizar uma simples verificação do histórico das transações, bem como sobre os valores.

Conforme o exposto verificamos a possibilidade de rastrear as transações, mas não significa que ao obter o endereço da carteira o indivíduo terá o acesso à chave privada do

endereço, se assim fosse o ativo poderia ser gasto por qualquer usuário remetente que tivesse o endereço da carteira destinatária, podemos considerar um pseudônimo. O FBI afirma ser possível obter o endereço da chave privada, mas até o momento não foi verificada esta possibilidade como também não houve transparência na informação do órgão responsável.

Especialistas entendem que o êxito do FBI em violar a carteira do cibercriminoso que invadiu o Colonial Pipeline está mais relacionado a um armazenamento desleixado e não uma vulnerabilidade de criptografia da tecnologia ou métodos inovadores. Para Nic Carter, especialista na área coloca como impossível a possibilidade do FBI ter violado a carteira dos cibercriminosos para ele o mais provável é que as autoridades conseguiu acessar servidores que os hackers armazenavam informações de chave privada, caracterizando uma falha de TI e não uma vulnerabilidade da tecnologia *bitcoin* (CNBC,2021).

O mero rastreio das transações não significa que as autoridades conseguirão facilmente vincular o endereço da carteira a uma identidade, o anonimato da identidade vai mais além.

Uma das técnicas que funciona de modo adequado para vincular uma transação de *bitcoin* com uma identidade é buscando o endereço de IP do usuário que permite ter sua localização exata, senão vejamos:

> Vincular uma identidade do mundo real a um endereço *bitcoin* não é tão difícil quanto se possa imaginar. Para começar, a identidade de uma pessoa (ou pelo menos informação de identificação, como um endereço IP) é frequentemente registrada quando alguém realiza uma transação de *bitcoin* em uma página *web* ou troca dólares por *bitcoins* em uma casa de câmbio de *bitcoins*. Para aumentar as chances de manter o pseudônimo, seria necessário empregar softwares de anonimato como Tor, e ter o cuidado de nunca transacionar com um endereço *bitcoin* no qual poderia ser rastreada a identidade do usuário (ULRICH, 2014, p. 21).

Segundo o autor, vincular uma identidade de um cibercriminoso ao endereço *bitcoin* é uma tarefa relativamente fácil em virtude da informação do endereço de IP, mas consideramos uma técnica sem muita eficácia que obtém êxito com usuários desleixados. O problema reside no fato das técnicas que os cibercriminosos utilizam para potencializar o anonimato e driblar as autoridades, ou seja, a combinação do navegador Tor (*dark web*), mixers e *decentralized exchanges* famosas (DEX).

Fato interessante e curioso é o advento do *bitcoin* que coincide com o momento em que a *dark web* mudou completamente. A tecnologia *bitcoin* criada para funcionar como um meio de pagamento com alcance global é literalmente compatível com a *dark web*, que usada de modo correto é altamente anônima. A utilização do *bitcoin* como método de pagamento dentro da *dark web* reduz consideravelmente os riscos de ter sua identidade revelada, bem como torna

de difícil identificação o endereço de IP dos usuários em virtude da conexão com as camadas de criptografia, daí o termo “cebola”.

Considerada uma combinação perfeita para aqueles que buscam preservar sua identidade e consequentemente reflete como um problema para as autoridades que não dispõem de recursos eficientes para analisar e investigar o mercado que sobrevive na camada mais profunda da *web*.

Os mixers são mais um meio de incrementar o anonimato da tecnologia *bitcoin*. É um serviço que permite que os usuários tenham seus *bitcoin* misturado com ativos de outros usuários, ou seja, o serviço realiza diversas transações com diversos usuários para que seja criado um rastro de transações aleatórias buscando assim o anonimato.

O serviço funciona literalmente na busca do incremento ao anonimato e podemos pontuar que sua utilização é frequente considerando as ofertas de diversas empresas que o realizam. É importante ressaltar que para execução do serviço não é necessário preencher nenhum tipo de informação pessoal para verificação de identidade.

As *decentralized exchanges* são corretoras que funciona entre os usuários em um *blockchain* própria igualmente o funciona da tecnologia *bitcoin*, no entanto, ela permite que os usuários troquem seus *bitcoin*, sem qualquer envolvimento de intermediários ou informação de identidade.

Para negociar em uma corretora centralizada, como *Binance*, *Novadax*, Mercado *Bitcoin*, *CoinBase*, é necessário fornecer algumas informações pessoais e passar por algumas etapas de verificação de identidade e em seguida é possível enviar fundos através de depósitos bancários ou até mesmo cartão de crédito. Os cibercriminosos evitam transacionar em corretoras centralizadas em virtude das etapas de verificação de identidade.

É importante ressaltar que a instrução normativa nº 1.888/2019, de 03 de maio de 2019, da Secretaria Especial da Receita Federal do Brasil dispõe sobre a obrigatoriedade das corretoras que atuam no território brasileiro em prestar informações sobre as operações dos usuários com criptoativos. A mesma traz a obrigatoriedade de os usuários prestarem informações quando os valores ultrapassarem R$ 30.000,00 (trinta mil reais) e esta obrigação se estende às transações que os residentes ou domiciliados no Brasil realizam em *exchanges* domiciliadas no exterior.

A referida instrução normativa busca regulamentar também as *exchanges* descentralizadas conforme prescreve em seu Art. 5°, parágrafo único:

> Incluem-se no conceito de intermediação de operações realizadas com criptomoedas, a disponibilização de ambientes para a realização das operações de compra e venda de criptoativo realizadas entre os próprios usuários de seus serviços.

Mesmo com a previsão citada acima não obstante a utilização das *exchanges* descentralizadas por cibercriminosos que a preferem ao invés das centralizadas. As famosas dex têm a fama de não trabalhar com as implementações de políticas de coleta de dados, bem como com protocolos que exigem a identificação dos clientes (Bueno, 2020).

Deste modo podemos observar a ineficácia da Lei nº 12.735, de 30 de novembro de 2012, que dispõe no art. 4º: "Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado". A internet vai além da superfície como desmembrada anteriormente, ou seja, as autoridades precisam se especializar cada vez mais e buscar investimentos para promover investigações na *dark web* e impor limites aos cibercrimes que gozam de total liberdade para praticar condutas delituosas.

CONSIDERAÇÕES FINAIS

Não restam dúvidas que a tecnologia *bitcoin* conjugada ao uso da internet impõe barreiras para as autoridades investigativas. A tecnologia *bitcoin* é uma inovação que trouxe novos desafios para todos os tipos de órgãos investigativos e até mesmo para os órgãos fiscalizadores. O Estado não pode ignorar as mudanças que ocorrem no ciberespaço, bem como os crimes destes.

O advento da nova tecnologia trouxe alterações sobre a forma que o dinheiro é transacionado e consequentemente os cibercriminosos tiram proveito das novas formas de transacionar e cada vez mais se especializam em maneiras de obter o anonimato no ciberespaço.

O direito se mostra proativo de legislações que abarcam o cibercrime, não poderíamos ter o mesmo pensamento quando pensamos no cibercrime da *dark web* que para muitos esta ainda é um enigma cheio de percalços. O desprovimento dos equipamentos adequados, bem como das equipes que não dispõem de especialização adequada são fatores que enfraquecem a eficácia da norma em relação aos crimes da camada mais profunda da *web*.

Considerando que o objetivo geral da pesquisa foi analisar o suposto anonimato do cibercrime na *dark web* concomitantemente a tecnologia *bitcoin* como meio de pagamento, tomando por base o disposto na legislação existente, o presente artigo consistiu em estudo bibliográfico, de caráter qualitativo, exploratório e dedutivo, objetivando proporcionar maior

visibilidade do cibercrime bem como dos métodos empregados na busca do anonimato e, assim, possibilitar uma reflexão maior sobre a implementação de medidas para identificação da autoria dos cibercrime, ainda que tenhamos leis que implementa métodos investigativos, ainda há uma necessidade na eficácia dos medidas adotadas, considerando-se a falta de eficácia e da carência no conhecimento sobre as peculiaridades das tecnologias estudadas.

O *bitcoin* demonstra ser o mais suscetível de ter sua criptografia desmembrada em virtude das corretoras centralizadas que possuem obrigação de fornecer informações sobre operações que ultrapassem determinado valor, bem como quando notificadas pelas autoridades podem fornecer informações de cunho pessoal e consequentemente de todas as transações. A legislação facilitou bastante o trabalho das autoridades, filtrando as transações de determinado valor que consideram relevante e consequentemente não necessitam realizar esforços para obter a chave pública do usuário que desejam investigar, ficando a cargo da corretora informar.

Neste sentido podemos afirmar a vulnerabilidade do *bitcoin*, no entanto, a *dark web* conjugada ao *bitcoin* e aos métodos de mixers bem como a utilização de corretoras descentralizadas (DEX) intensifica o anonimato dos usuários e consequentemente gera dificuldades para as autoridades determinar a autoria dos cibercrime que se utilizam das tecnologias para transacionar no ciberespaço, nós levando à estaca zero em relação ao anonimato. As tecnologias citadas geram um anonimato totalmente compatível e poderoso e durante esta pesquisa não encontramos métodos que comprovem a vulnerabilidade da criptografia do uso concomitante das tecnologias. As DEX não trabalham com a política de repassar informações para as autoridades ou governo. As técnicas utilizadas pelas autoridades servem apenas para os usuários desleixados.

A ineficiência do Estado brasileiro para coibir e investigar os crimes cibernéticos resulta na sensação de impunidade e um cenário, não somente de insegurança, bem como de que o ambiente digital é uma "terra sem lei". Há uma imediata necessidade de capacitação e especialização das autoridades investigativas a fim de proporcionar aos profissionais novos métodos e ferramentas que auxiliarão nas investigações da autoria dos cibercrimes, uma vez que adentrar nas camadas mais profundas da *web*, é necessário habilidades e ferramentas digitais específicas e certeiras para que haja maestria nas investigações e a obtenção exata dos autores dos crimes.

O banimento do *bitcoin* na busca do enfrentamento do cibercrime não é recomendado em virtude de sua descentralização, haja visto as tentativas frustradas da China ao tentar banir a tecnologia e considerá-la ilícita. O mais sensato é buscar o enfrentar os cibercrimes

desmistificando o anonimato imposto pelas tecnologias com cooperação internacional e investimentos em equipamentos de ponta e especialização das autoridades.

Conforme o estudo e as análises realizadas, podemos concluir que para buscar o enfrentamento dos cibercrimes é necessário entender o funcionamento das tecnologias que são empregadas para o uso do incremento ao anonimato. As DEX e os *mixers* merecem atenção das autoridades e para isto é necessário que exista investimento em medidas de cooperação jurídica internacional em virtude do caráter transfronteiriço das tecnologias estudadas e ainda uma regulação a nível global. O estado deve oferecer especialização e ferramentas adequadas para os agentes desmistificar o anonimato dos cibercrimes. A necessidade de uma regulamentação da tecnologia *bitcoin* é notória a fim de retirar sua criptografia que a faz ter aptidão para funcionar como meio de pagamento na *dark web*.

O anonimato conjugado das tecnologias deve servir como referência para os debates contemporâneos contribuindo para uma adequada regulamentação da tecnologia *bitcoin* em busca de sua exclusão da *dark web*, bem como qualquer outro ativo alternativo ao *bitcoin*.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves; SANTOS, Hericson. **Deep Web Investigação no submundo da internet**. Rio de Janeiro: BRASPORT, 2019.

BRASIL 123. **Como o FBI rastreou o bitcoin se ele não é rastreável?** Disponível em: <https://brasil123.com.br/como-o-fbi-rastreou-o-*bitcoin*-se-ele-nao-e-rastreavel/> Acesso em 30 ago. 2021.

BRASIL. **INSTRUÇÃO NORMATIVA Nº 1.888, DE 3 DE MAIO DE 2019**. 2019. Disponível em: <https://www.in.gov.br/web/dou/-/instru%C3%87%C3%83o-normativa-n%C2%BA-1.888-de-3-de-maio-de-2019-87070039> Acesso em 10 ago. 2021.

_____. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 01. out. 2021.

BUENO, Thiago Augusto. **Bitcoin e crimes de lavagem de dinheiro**, 1ª ed. Campo Grande: Contemplar, 2020.

CNBC. ***The FBI likely exploited sloppy password storage to seize Colonial Pipeline bitcoin ransom***. Disponível em: <https://www.cnbc.com/2021/06/08/fbi-likely-exploited-sloppy-password-storage-to-seize-colonial-ransom.html> Acesso em 01 set. 2021.

GIBSON, Willian. **Neuromancer**. São Paulo: Aleph, 2003

IGNACIO, Bruno. **Mercados na dark web faturam quase US$ 2 bi em criptomoedas**. TECNOBLOG. Disponível em: <https://tecnoblog.net/408625/mercados-na-dark-web-faturam-quase-us-2-bi-em-criptomoedas/>. Acesso em: 12 maio 2021.

LEMOS, A. **O que é Cibercultura?** 2013. Disponível em <https://profwagner.wordpress.com/2013/09/05/o-que-e-cibercultura/> Acesso em 21 set 2021.

LÉVY, Pierre. **Cibercultura**. São Paulo: Ed.34, 2000.

MONTEIRO, S. D. O Ciberespaço: o termo, a definição e o conceito. DataGramaZero - **Revista de Ciência da Informação - v.8 n.3** 2007.

NASCIMENTO, S. P. **Cibercrime**: Conceitos, modalidades e aspectos jurídicos-penais. Âmbito jurídico. Disponível em: <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em: 20 maio 2021.

PECK, P. P. **Segurança Digital** - Proteção de Dados nas Empresas. [São Paulo - SP]: Grupo GEN, 2020. 9788597026405. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026405/>. Acesso em: 08 Jun 2021.

PIRES, H. F. Bitcoin: a moeda do ciberespaço. **Rev. Geousp – Espaço e Tempo (Online), v. 21, n. 2, p. 407-424**, agosto. 2017. ISSN 2179-0892. Disponível em: <http://www.revistas.usp.br/geousp/ article/view/134538>. Acesso em: 27 maio 2021.

PODER 360. Biden planeja reunião com 30 países para combater cibercrimes. Disponível em: <https://www.poder360.com.br/tecnologia/biden-planeja-reuniao-com-30-paises-para-combater-cibercrimes/> Acesso em 27 out. 2021.

PODER 360. Bitcoin cai 8% após China determinar ilegalidade na transação de criptomoedas. Disponível em: <https://www.poder360.com.br/economia/*bitcoin*-cai-8-apos-china-determinar-ilegalidade-na-transacao-de-criptomoedas/> Acesso em 21 ago. 2021.

PORTAL DO BITCOIN. Bitcoin precisa de regulamentação global, diz presidente do Banco Central Europeu. Disponível em: <https://portaldo*bitcoin*.uol.com.br/*bitcoin*-precisa-de-regulamentacao-global-diz-presidente-do-banco-central-europeu/> Acesso em 20 ago. 2021.

SOUZA, Liziane Menezes; PULGA, Mariele Oliveira; WOLTMANN, Angelita; SOUTO, Raquel Buzatti; FALCONI, Adalberto Fernandes; PEREIRA, Raoni Paiva; Luis Gustavo Durigon. **Fundamentos Dos Crimes Virtuais:** Da Cibercultura À Prática Ilícita No Ciberespaço. XV SEMINÁRIO INTERNACIONAL DE EDUCAÇÃO NO MERCOSUL. 2013.

TELLES, Christina Mariani da Silva. ***Bitcoin*, Lavagem de Dinheiro e Regulamentação**, Curitiba: Juruá, 2020.

ULRICH, Fernando. ***Bitcoin*: a moeda na era digital**, 1ª Edição. São Paulo: Instituto Ludwig Von Mises Brasil, 2014.