MINISTÉRIO PÚBLICO DO ESTADO DO CEARÁ
ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DO CEARÁ
CENTRO DE ESTUDOS E APERFEIÇOAMENTO FUNCIONAL

REVISTA ACADÊMICA ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DO CEARÁ

ANO 12, Nº2 (JUL./DEZ. 2020) SEMESTRAL
FORTALEZA-CE

ISSN FÍSICO: 2527-0206
ISSN ELETRÔNICO: 2176-7939

NATUREZA JURÍDICA DO CRIME DE *RANSOMWARE* E A UTILIZAÇÃO DA CRIPTOMOEDA COMO MEIO DE IMPUNIDADE[1]

LEGAL NATURE OF RANSOMWARE CRIME AND THE USE OF CRYPTOCURRENCY AS A MEANS OF IMPUNITY

Luiz Eduardo dos Santos Pereira Gomes [2]
Luana Esteche Nunes [3]
Michael Felipe Wilmers[4]

RESUMO

O avanço da tecnologia facilita a vida do ser humano e cria novas fragilidades inerentes ao mundo tecnológico, os quais ficam à mercê de criminosos que invadem os sistemas operacionais "sequestrando" os dados existentes, exigindo pagamento pelo resgate, denominando-se *"ransomware"*. As investigações desses crimes exigem um árduo trabalho, tornando o delito quase um crime perfeito. Assim, pretende-se expor o tema, tipificar a conduta, bem como apresentar como esses indivíduos atuam e qual a forma de se evitarem essas práticas, o que faz por meio de análise de legislação e de doutrina, concluindo-se que a falta de legislação pode resultar em impunidade.

Palavras-chave: *Bitcoin*. Internet. Sequestro de dados.

1 INTRODUÇÃO

O crescimento do número de domicílios com acesso à internet vem acontecendo de forma impressionante, estimando-se que no ano de 2018, segundo dados da agência

1 Data de Recebimento: 08/11/2020. Data de Aceite: 23/11/2020.
2 Aluno regular do Curso para Doutorado em Direito Penal pela Universidade de Buenos Aires; Pós-Graduado Lato Sensu especialização em Direito do Trabalho pela Pontifícia Universidade Católica de Minas Gerais; Advogado OAB/MG 147.978. E-mail: eduardo.ilheus@gmail.com. Currículo Lattes: http://lattes.cnpq.br/2513799893477268. ORCID: https://orcid.org/0000-0002-9728-0074.
3 Aluna regular do Curso para Doutorado em Direito Civil da Universidade de Buenos Aires; Mestre em Propriedade Intelectual e Transferência de Tecnologia; Coordenadora do Procon, Guarapuava/PR; E-mail: luanaesteche@yahoo.com.br. Currículo Lattes: http://lattes.cnpq.br/0738352354928414. ORCID: https://orcid.org/0000-0003-4486-185X.
4 Aluno regular do Curso de Direito em Centro Universitário Campo Real. E-mail: michaelwilmers@gmail.com. Currículo Lattes: http://lattes.cnpq.br/2175691309177530. ORCID: https://orcid.org/0000-0002-3823-6612.

especializada da Organização das Nações Unidas – ONU, "3,9 bilhões de pessoas, o equivalente a 51,2% da população mundial possuem acesso à internet" (AGÊNCIA BRASIL, 2018). Já o Instituto Brasileiro de Geografia e Estatísticas – IBGE calcula que "no ano de 2018 o volume de casas conectadas à internet correspondia a 79,1% da população brasileira" (GOMES, 2020). E esse cenário não é diferente ao que se refere às empresas, onde o uso de computadores e da internet passou a ser uma das principais ferramentas de trabalho ou de armazenamento de dados, eis que gera uma maior capacidade competitiva, melhor eficiência e agilidade.

O uso da tecnologia também trouxe uma nova modalidade do crime de extorsão, pelo qual o criminoso, mediante a implantação de um vírus ou *malware* malicioso, realiza o sequestro dos dados da máquina invadida, segredos industriais e comerciais de grande valor econômico, o qual é, posteriormente, criptografado e cuja senha só será fornecida mediante o pagamento de quantia em dinheiro, o que se dá, normalmente, por meio de moeda digital ou criptomoeda.

A problemática se instaura por ocasião da dificuldade de rastreamento do beneficiário da transferência de valores em transações com criptomoedas, a qual não é regulamentada no cenário nacional, dificultando a identificação dos autores dos crimes, propiciando a impunidade, chegando a ser intitulado como o crime "quase perfeito".

O tema do presente estudo é atual e de especial relevância, visto que segundo Wakka (2019) o Brasil é um dos países com mais ataques de *ransomware*. "Com isso, o nosso país representa 10,75% das ameaças do setor em todo o mundo. O estudo é baseado em 48 milhões de ameaças bloqueadas em 2018, sendo que 1,8 bilhão é relativo à *ransomware*". Ainda, apenas no ano de 2019 houve um aumento de 109,95% nas denúncias que se referem a crimes cibernéticos, dentre eles o chamado "sequestro de dados". (WAKKA, 2019).

Nessa esteira, busca-se, com o presente artigo, dissecar o tema, sem intenção de esgotá-lo, analisando o papel da criptomoeda no pagamento do "resgate dos dados" e suas consequências quanto à apuração de autoria e punição dos criminosos. Utilizando-se da metodologia qualitativa, por meio da consulta em textos - artigos, resumos e ensaios – relacionados ao tema, e a partir da doutrina e legislação aplicáveis ao caso, pretende-se demonstrar a tipificação que a prática se enquadra, bem como demonstrar a (in)eficácia das normas frente à forma que são tratadas essas ocorrências, visto que se trata de tema de segurança nacional.

2 A UTILIZAÇÃO DA INTERNET COMO ALIADA AO CRIME

Analisando sob o viés econômico, o cenário que a internet trouxe às empresas se mostrou como uma realidade até então desconhecida, pois se tornaram grandes aliadas, tornando-se a principal ferramenta de trabalho, armazenamento de dados, bem como de *marketing*, pois gera uma maior capacidade competitiva, melhor eficiência e agilidade nos serviços.

Ocorre que essa inovação trouxe consigo uma série de consequências até então não exploradas, especificamente no que se refere aos dados armazenados na internet, o chamado "banco de dados", pelo qual se compõem as informações mais relevantes de uma empresa, possuindo valor imensurável, visto que possui informações que vão desde dados de colaboradores até conteúdos sigilosos e importantes para a manutenção da própria instituição.

A busca de fragilidades pelos criminosos é constante, os quais viram na internet uma nova oportunidade, visto que os crimes nesse seguimento passaram a ser comuns. De início, os crimes de invasão a dispositivo eletrônico não possuíam intuito financeiro, mas já traziam enormes prejuízos às vítimas, as quais tinham seu banco de dados e sistema informático invadidos e destruídos, causando danos milionários.

A exemplo disso podem ser citados os crimes cometidos por Michael Calce, em 2000, conhecido pela alcunha de "MafiaBoy", o qual invadiu sistemas como o Yahoo, Amazon e CNN. (Folha de São Paulo, 2000). Indivíduos como Calce são conhecidos como *hackers,* nomenclatura dada àqueles indivíduos que "agem de forma maliciosa, planejando satisfação econômica ou pessoal. Suas atividades geralmente giram em torno de roubo de informações, extermínio de dados e entrada ilegal em sistemas privados." (AGUILAR, 2017, p. 16).

A grande preocupação com *hackers* é quanto a sua possibilidade de praticar diversos atos com os dados obtidos de forma indevida, considerando que passaram a realizar ataques aos computadores de grandes empresas, "sequestrando" seu conteúdo e gerando enorme prejuízo intelectual, patrimonial e moral às vítimas. Viu-se, então, uma possibilidade de se obter vantagem econômica em face à empresa proprietária dos dados, cujo crime se dá com a implantação de vírus ou *software* malicioso, também chamado de *malware*, o qual invade e captura os dados constantes no computador, que serão objetos de criptografia e cuja senha só é fornecida mediante ao pagamento de quantia em dinheiro.

No Brasil, um dos casos de grande repercussão, envolvendo o sequestro de dados, ocorreu com a atriz Carolina Dieckmann, no ano de 2012, quando teve fotos íntimas "sequestradas" mediante a exigência de pagamento da importância de R$ 10.000,00

(dez mil reais) para que não houvesse a sua divulgação. A autoria do crime foi posteriormente apurada com a identificação do "IP" (*Internet Protocol*) do dispositivo utilizado para realizar o crime, uma espécie de impressão digital que propicia a identificação. (GLOBO.COM, 2012).

Recentemente, outro caso tomou proporção mundial, no ano de 2017, o qual encenou um verdadeiro "espetáculo", envolvendo por 5 dias cerca de 150 países, sendo o *malware* denominado *Ransomware WannaCry* infectou mais de 340 mil máquinas. (PROOF, 2017). O que chama a atenção nessa espécie de *software* malicioso é a tecnologia utilizada, visto que o *ransomware wannacry* bloqueia/criptografa os dados das vítimas, disponibilizando um aviso na tela do dispositivo, destruindo o arquivo em determinado prazo, assim como o valor a ser pago para sua recuperação, o que se dá mediante transferência de criptomoedas.

A questão passou a ser objeto de atenção e discussão por parte do legislador brasileiro com a edição do "Marco Civil da Internet", Lei nº 12.965/2014, a qual tem por objetivo regulamentar um território sem lei, dispondo princípios, garantias, direitos e deveres para o uso da internet no Brasil, em especial preocupação com a proteção da privacidade dos usuários. (BRASIL, 2014).

Apesar disso, a punição de autores de cibercrime nem sempre se torna possível, diante da complexidade dos crimes e da necessária qualificação dos investigadores, cujo presente estudo analisa o dispositivo desde o Código Penal Brasileiro até a utilização da criptomoeda como meio para pagamento do "resgate".

2.1 Dos cibercrimes na legislação nacional

Até recentemente, o Brasil não possuía legislação específica tratando de crimes virtuais/cibercrimes, práticas que cada vez mais têm preocupado os indivíduos, principalmente empresas.

O conceito de crime cibernético ainda é variante em solo brasileiro, considerando que diversos autores o conceituaram sem que, no entanto, haja uma denominação comum. Ao entender de Machado e Vianna (2013, p.29), para que um delito seja considerado como informático deve-se considerar que o objeto protegido é a inviolabilidade das informações e dados informáticos, protegidos por intermédio da Constituição Federal, art. 5º, X. Dessa forma, segundo o autor, "simples utilização pelo agente de um computador para a execução de um delito, por si só, não configuraria um crime informático, caso o direito afetado não seja a informação automatizada". (MACHADO; VIANNA, 2013, p. 29).

De acordo com PINHEIRO (2007, p. 250) os crimes virtuais são um crime de meio,

pois a internet é utilizada como meio de prática criminosa e a caracterização dos crimes virtuais diz respeito ao meio empregado para praticá-los, visto que utilizam-se da internet para a sua prática:

> O crime virtual é, em princípio, um crime de meio, ou seja, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, aquele cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, mas que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa é que é virtual, não o crime. (PINHEIRO, 2002, p. 250).

A tipificação específica desses fatos no Brasil ocorreu no ano de 2012, somente após a repercussão causada pelo caso Carolina Dieckmann, o que motivou o Legislativo Brasileiro a aprovar a Lei nº 12.737 de 2012, popularmente conhecida pelo nome da atriz vítima de *ransomware*. A referida lei alterou o Código Penal Brasileiro e acrescentou os artigos 154-A e 154-B, os quais tratam do crime de "Invasão de dispositivo informático", *in verbis:*

> Invasão de dispositivo informático
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços

> se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
> Ação penal
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (BRASIL, 2012).

Essa tipificação foi um marco na legislação brasileira, que até então somente poderia punir os crimes em que houvesse uma externalização do resultado causado pela invasão – dano, ofensa à honra, prejuízo econômico etc.). A partir da Lei, assim que ocorre a invasão do dispositivo, mesmo que o indivíduo não consiga efetivamente atingir a finalidade do delito, consuma-se o crime – é o que a doutrina, costumeiramente, trata como crime formal (GONÇALVES, 2016, p. 321-322).

Em análise dos tipos penais, percebe-se que o legislador se atentou, precipuamente, com a "invasão" do dispositivo, preocupando-se com o fim de agir do indivíduo, qual seja o de obter, adulterar, destruir os dados e informações ou instalar vulnerabilidades – leia-se *software* – para obter vantagem ilícita sobre o titular do dispositivo, sem que o mesmo tenha autorizado. Importante destacar o excerto legal, mesmo porque, em exposição de motivos da Lei, expõe-se como objetivo delimitar a finalidade específica do tipo penal para que não houvesse o enquadramento em todo e qualquer caso de "invasão":

> Estabelece a necessidade de intenção específica de "instalar vulnerabilidades, obter vantagem ilícita ou obter ou destruir dados ou informações não autorizados" - ou seja, pune-se apenas quando a conduta do agente estiver relacionada a determinado resultado danoso ou quando o objetivo do agente for efetivamente censurável e

> não se confundir com atividades legítimas da Internet, excluindo-se assim, mais uma vez, os casos de mero acesso a informações, ou os casos de obtenção de informações que, por sua natureza, não seriam passíveis de restrição de acesso. (BRASIL, 2011, p. 6).

Outro apontamento relevante está contido no §3º do novo artigo 154-A do Código Penal, o qual nos traz a qualificação do delito, nos casos em que os dados se tratam de "conteúdo de telecomunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas". (BRASIL, 2012). Destaca-se essa previsão, porque a maioria dos ataques a dispositivos tem como objetivo a obtenção desses dados, pois informações dessa monta possuem valor incomensurável, considerando que são dados imprescindíveis, principalmente quando a vítima se trata de uma empresa.

Uma inquietude passou a se apresentar por ocasião da nova modalidade de cibercrime, mediante à conduta do apossamento de dados constantes no equipamento informático com criptografia, a qual apenas é extinta com o pagamento de valores pecuniários. E isso se faz diante da análise da qualificadora do crime de "Invasão de dispositivo informático", que possui como preceito secundário: "pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, **se a conduta não constitui crime mais grave**." (BRASIL, 2012, grifo nosso).

Qual a natureza jurídica clara do crime de sequestro de dados ou *ransomware*, somando-se ao fato da criptografia posterior dos dados, juntamente com a ameaça de destruição dos arquivos caso não haja pagamento do resgate, um crime de sequestro de dados ou de extorsão?

2.1.1 Ransomware e sua tipificação penal

O crime de sequestro de dados ou *ransomware* não é tipificado no ordenamento penal brasileiro, e se caracteriza pela obtenção de acesso ao sistema informático, mediante uso de ardil, mediante o engano ou não do proprietário ou titular da máquina, seguindo-se de inserção de um código fonte com o intuito de bloquear o acesso por usuário que não possua a senha decodificadora. Após, a conduta delituosa segue pela comunicação da vítima da prática delituosa, e da exigência de montante de dinheiro para que haja a liberação e recuperação dos dados criptografados. De acordo com Araujo (2019, p.70),

> Este vírus faz parte de uma classe específica de *malwares* que é utilizada nas chamadas extorsões digitais, pois obriga suas vítimas a pagarem determinado valor em troca do completo controle de seus dados. Essencialmente, existem duas classes: a Locker, que impede

> que a vítima acesse o equipamento infectado, praticamente inutilizando-o, e a Crypto, que bloqueia o acesso aos dados armazenados no equipamento infectado, utilizando criptografia.

Apesar da terminologia utilizada ser "sequestro de dados", temos que ela não se enquadra ao tipo jurídico de sequestro, pois não existe a pessoa física a ser sequestrada, veja-se: "Art. 159 – Sequestrar **pessoa** *com o fim de obter, para si ou para outrem, qualquer vantagem, como condição ou preço do resgate/Pena – r*eclusão, de oito a quinze anos." (BRASIL, 1940, grifo nosso).

O crime de extorsão, por sua vez, é classificado como crime contra o patrimônio e previsto no artigo 158 do Código Penal Brasileiro: "Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa." (BRASIL, 1940). Dessa forma, o objetivo precípuo do tipo penal é a obtenção de vantagem manifestamente indevida, mediante à utilização de medidas coativas, caracterizando uma espécie de constrangimento ilegal, com o intuito de auferir vantagem econômica. De acordo com as lições de Nucci (2020, p. 1030) o crime de extorsão se caracteriza por

> Constranger (tolher a liberdade) alguém, mediante grave ameaça (violência moral, consistente no prenúncio de um acontecimento desagradável, com força intimidativa, desde que importante e sério) ou violência (violência física, isto é, o constrangimento físico voltado à pessoa humana) a fazer, tolerar que se faça ou deixar de fazer alguma coisa, com o fim de obter indevida vantagem econômica. Embora não mencionado expressamente no tipo, acrescentamos a possibilidade de se dar extorsão pela redução da possibilidade de resistência (violência imprópria).

Segundo o autor, a diferença precípua entre o crime de extorsão e o de roubo encontra-se no fato de que a extorsão exige a participação ativa da vítima: quando ela faz algo, tolera que se faça ou deixa de fazer, com o fim de alcançar a vantagem desejada a depender da colaboração da vítima. Da mesma banda são os ensinamentos de Capez (2012, p. 491), para quem

> A característica básica desse crime é que o agente coage a vítima a fazer, não fazer, ou tolerar que se faça algo, mediante o emprego de violência ou grave ameaça. Em suma, estamos diante de uma forma do crime de constrangimento ilegal, acrescida contudo de uma

> finalidade especial do agente, consubstanciada na vontade de auferir vantagem econômica.

O crime de extorsão resta classificado, no ordenamento jurídico brasileiro, como um crime patrimonial e não contra a pessoa, visto que, sobretudo, tutela a inviolabilidade patrimonial da vítima, a qual pode se tratar de qualquer pessoa, mesmo que para sua consumação necessite de emprego de violência, ou grave ameaça à integridade corporal ou psíquica.

A consumação do crime independe do resultado alcançado e defendida por alguns doutrinadores, como Guilherme Nucci (2020, p. 1032), por não haver a necessidade da redução do patrimônio da vítima para sua consumação, sendo o alcance da vantagem indevida mera configuração de objetivo, por parte do criminoso, e não elemento essencial para a configuração do tipo penal, entendimento que é adotado pelo Superior Tribunal de Justiça mediante à sumula 96, o qual não é absoluto.

Há quem defenda que o crime de *ransomware* se trata de diversos outros crimes em concurso, consubstanciados pela invasão de dispositivo informático, sabotagem informática, intimidação e extorsão, mediante concurso material. (MASSENO; WENDT, 2017). Entretanto, temos que o crime de *ransomware* não é uma nova modalidade criminosa, mas sim uma mera variação da prática do crime de extorsão, mediante à exigência de pagamento indevido para a liberação de arquivos pelo criminoso apossados e criptografados. Coaduna do presente entendimento Crespo (2015) ao definir que

> A prática do *ransomware* é, portanto, configurada como crime de extorsão, ainda que o resgate/valor não seja pago, já que se trata de crime formal (independe de resultado, o que se nota pela redação típica). Entendemos que no caso da difusão do vírus para propiciar o bloqueio dos dados, a tipificação do §1º do art. 154-A do Código Penal restaria absorvida pela consunção.

Após concretizada a invasão do dispositivo eletrônico e criptografia dos dados "sequestrados", o criminoso passa então para a fase de extorsão propriamente dita, a partir da cobrança de resgate em troca do código que libera o acesso aos arquivos. Apesar das orientações das autoridades policiais para que o valor do resgate não seja pago, a autoria do crime é de difícil rastreabilidade, assim como a recuperação dos "dados sequestrados". Logo, a vítima acaba, por muitas vezes, optando pela realização do pagamento em decorrência da importância e valor das informações constantes no banco de dados.

Como forma de dificultar a atuação da polícia e da investigação do crime, os autores têm preferido que o pagamento do resgate se dê por criptomoedas, o que o fazem não

somente em decorrência de seu elevado valor econômico, mas pela facilidade que a moeda traz para os *hackers*, a qual gera uma dificuldade de rastreabilidade do destinatário da quantia econômica.

3 CRIPTOMOEDAS NO CONTEXTO DO CRIME DE EXTORSÃO DIGITAL E A IMPUNIDADE

A criptomoeda é conhecida por diversos nomes, com diferentes variações, como os *bitcoins*, por exemplo, que é a mais popular e promissora do mercado, definida como "dinheiro, assim como o real, dólar ou euro, com a diferença de ser puramente digital e não emitido por nenhum governo" (ULRICH, 2014, p. 111). Ainda,

> Trata-se de uma moeda digital descentralizada, ou seja, ela não depende de um emissor central e pode ser transacionada para qualquer pessoa em qualquer parte do planeta sem intermediários, e, inclusive, sem limite de valor. Sem muito aprofundamento, para utilizá-la cada usuário terá de criar uma "carteira" (um programa). Ela serve para acumular os seus endereços bitcoin." (ULRICH, 2014, p. 98).

Sua principal característica é a não intervenção estatal diretamente ou por autoridades reguladoras, culminando na dificuldade do rastreio, somada à facilidade de se realizar as transações, juntamente com o alto valor econômico, faz com que a moeda se torne o atrativo principal de barganha pelos dados raptados. Isso implica uma série de problemas, ao passo que a prática dos *hackers* pode se tornar impune, pois, ainda que o fato tenha ocorrido, sem a identificação do agente é impossível que ocorra a punibilidade. Conforme consigna Leonardi (2005, p.270), "se não há uma maneira de saber quem alguém é, onde ele está, nem o que fez ou está fazendo, o sistema jurídico – que é dependente dessas informações para exercer sua força coercitiva – parece perder sua efetividade."

A criptomoeda é uma abstração, na medida em que apenas existem no campo virtual e na marginalidade da ordem econômica, cujas movimentações são assinadas digitalmente, sem qualquer regulação ou intervenção estatal, cujas contas não podem ser rastreadas e nem bloqueadas. A moeda se torna severamente atrativa, porque diminui o custo da transação realizada, diante da ausência do terceiro intermediador, sendo os próprios correntistas que aprovam e realizam as transações.

A dificuldade de rastreamento das transações realizadas com *bitcoins* ou criptomoedas se configura em razão do registro das transações se darem por intermédio de uma

corrente chamada de "sobreposição de blocos", pela qual, segundo Nakamoto (2008 *apud* CARDOSO; COSTA; SILVEIRA, 2018, p. 8):

> O protocolo é definido como uma cadeia de assinaturas digitais em que cada proprietário transfere a moeda para um novo proprietário, e então em seguida é executada uma assinatura digital em um *hash* da transação anterior, a chave pública do próximo proprietário e adicionando estes ao final da moeda.

O registro das transações realizadas por intermédio das criptomoedas é gravado junto ao *blockchain,* que se termina como um livro-razão distribuído publicamente, seguindo um mecanismo de consenso, cujo conceito se pode encontrar na doutrina de Shaikh e Lashari (2017, p. 169).

> *Blockchain* é um sistema de armazenamento que mantém registro de todas as transações digitais que são executadas usando moedas. É o sistema de transações que transfere os ativos digitais diretamente na carteira do blockchain sem qualquer exigência de terceiros como banco ou instituição financeira. Esta tecnologia fornece um sistema onde seu dinheiro chega diretamente a você sem qualquer envolvimento de bancos; e você pode usar isso instantaneamente valor para seus fins pessoais ou comerciais.

O *blockchain*, de código aberto, pode ser acessado por todos os usuários das *bitcoins*, os quais podem verificar as transações realizadas na rede como uma forma de controle coletivo, pois cada participante terá acesso aos códigos públicos do usuário que realizou a transação, assim como sua validação. Entretanto, tal sistemática não significa dizer que o titular ou signatário da transação seria facilmente identificado, pelo contrário. Veja-se a doutrina de Vicente (2017, p.91).

> Todas as transações efetuadas em Bitcoin *s*ão automaticamente registradas no *blockchain* (cadeia de blocos), que nada mais é do que um registro público de todas as transações efetuadas na rede. Cada peer tem uma cópia do *blockchain*, o que lhe dá autonomia de verificar qualquer Bitcoin existente na rede. Essas transações podem ser rastreadas apenas com a chave de cada transação, confirmando assim a sua autenticidade, porém não é possível rastrear o usuário que está realizando essa transação, nem o remetente e nem o destinatário, assim a moeda gera a principal característica dela, que é a anonimicidade.

E é em decorrência dessa anonimicidade das criptomoedas e/ou bitcoins, por meio da utilização de pseudônimos na realização das transações, que têm sido cada vez mais utilizadas como meio de pagamento do resgate nos crimes de "sequestro de dados", visto que o pagamento e a titularidade do verdadeiro destinatário da moeda digital muitas vezes não podem ser identificados. De acordo com Nawari e Ravindran (2019, p. 12), o sistema de gerenciamento de bitcoins se pauta em princípio da privacidade e confiança, eis que

> A privacidade é obtida por meio da criptografia de dados e garante que as transações sejam autenticadas e verificadas. A privacidade é uma parte crucial do BCT para fortalecer a segurança e tornar o sistema distribuído na rede mais difícil de violar. Confiança (consenso): Confiança significa usar o poder da rede para verificar a transação de dados. O modelo de confiança (consenso) é verdadeiramente o coração dos aplicativos de *blockchain*. A confiança é o que entrega os princípios de confiança, trocas e propriedade. A confiança é o que permite que o *blockchain* desloque o sistema de transação, mas isso só pode acontecer quando o comércio e a propriedade são tratados por livros-razão distribuídos/compartilhados. (NAWARI; RAVINDRAN, 2019, p. 12).

Na opinião de Ulrich (2014, p. 20-21), a questão da anonimicidade é mera atenção midiática diante da utilização de codinomes para a realização das transações, fazendo uma analogia das transações realizadas por meio da transferência de *bitcoins* com aquelas realizadas mediante à tradição em dinheiro vivo, considerando que ambas não possuem terceiro intermediário. Acontece que a diferença se instala sobre as transações realizadas mediante à transferência de *bitcoins, que* se dá entre duas chaves públicas, cuja transação é registrada no *blockchain*, cujas chaves podem ser facilmente identificadas por seus usuários.

Portanto, para o autor, mesmo que tais chaves não estejam vinculadas a nenhuma identidade concreta e sim a um pseudônimo, a identidade do titular da transação fica registrada ao menos mediante à identificação do IP da máquina do computador, pelo qual foi realizada, ou mediante casa de câmbio, pela troca de bitcoins por dólares. Concordando o autor ao fato de que "os usuários de Bitcoin desfrutam de um nível muito maior de privacidade do que usuários de serviços tradicionais de transferência digital, os quais precisam fornecer informação pessoal detalhada a terceiros intermediários que facilitam a troca financeira." (ULRICH, 2014, p. 22).

Apesar de haver uma árdua possibilidade de identificação do criminoso, que recebe

o resgate dos dados sequestrados mediante pagamentos por intermédio de *bitcoins*, esse é um meio de pagamento que dificulta e muito a identificação do criminoso, sendo a extorsão mediante ao pagamento do resgate por criptomoeda considerada como o crime quase-perfeito. Nesse contexto é o entendimento de Shimabukuro (2018, p. 71).

> Da mesma maneira que provar a propriedade de *bitcoins* desafia investigadores, a descoberta de uma identidade de um criminoso cibernético pode revelar não só o crime foco daquela investigação, mas todo o seu histórico de delitos. O *blockchain* não diferencia transações legais das ilícitas, tudo está registrado em seu extenso livro de registros digital. A tecnologia sempre trabalha para os dois lados, cada novo problema requer forças para evoluir o sistema, tanto do lado das autoridades quanto dos criminosos. E sempre podemos contar com o erro humano, principalmente no lado do criminoso. Criar estruturas que garantam nossa privacidade, mas que também façam a proteção dos crimes digitais é o desafio da nossa geração.

Já, Araujo (2019, p.75), argumenta que, assim como os criminosos se utilizam das redes de computadores para aplicar o golpe, também conseguem maquiar facilmente o IP do computador utilizado, o que facilita a impunidade:

> Como forma de proteção, cada transação efetuada é impressa na rede bitcoin, de modo que não há possibilidade de tentar gastar aquela moeda em mais de uma transação. As transações são públicas, mas ninguém sabe quem são as pessoas que estão por trás dos pontos de início e fim, em tese, garantindo o anonimato. Por óbvio que usuários comuns, podem deixar outros rastros em suas transações, como seu número de IP. Sabemos que os criminosos facilmente podem mascarar seu IP original. Por tais fatores, os cibercriminosos preferem essa moeda em suas empreitadas. (ARAUJO, 2019, p.75).

Os criminosos têm logrado êxito com os ataques realizados por *ransomware*, cujos pedidos de resgate se deram por intermédio de bitcoins, a exemplo do ataque que paralisou o sistema de transporte de São Francisco, nos Estados Unidos, quando a empresa acabou cedendo o pagamento de resgate no valor de US$ 75 mil, seguindo-se de diversos outros ataques do mesmo ou de maior porte. De acordo com Mello (2016):

> O FBI (Federal Bureau of Investigation, a Agência Federal de Investigação dos Estados Unidos) estima que os ransomwares arre-

> cadaram cerca de US$ 1 bilhão no ano de 2016, bem como que uma das maiores organizações criminosas faturou próximo a US$ 27 milhões com suas fraudes, sendo que o Brasil concentra cerca de 92% dos ataques da América Latina.

A combinação de sequestro de dados mediante ao pagamento de criptomoeda/bitcoins, é uma questão que vem desafiando a investigação policial, assim como o ordenamento jurídico em si, na medida de que a criptomoeda não impede a apuração da autoria do crime, mas dificulta, e muito, o trabalho da autoridade policial. É possível identificar o autor do crime, se ele for displicente e descuidado, pela identificação do IP da máquina utilizada, ela não tenha sido maquiada, ou mediante à identificação por ocasião da conversão da moeda virtual em dinheiro convencional, desde que haja a necessidade da utilização de serviços bancários para isso.

Outra questão que agrava e dificulta a persecução criminal, é a possibilidade de "lavar" a própria criptomoeda por meio de um sistema denominado *mixer*, os quais consistem no processo de misturar suas criptomoedas com as de demais pessoas, restituindo o valor equivalente por intermédio de diversas transações. Na opinião de Grzywotz (2019, p.280) o uso do *mixing – service* não necessariamente implica na ocultação das *bitcoins*, mas obscurece a relação entre o remetente e seu destinatário, tonando-a nebulosa em decorrência mediante dissimulação, o que por certo vem dificultar a origem dos *bitcoins*. Essa prática favorece a mistura de valores adquiridos legal e mediante ato criminoso, ocultando e dissimulando sua origem e natureza, pela prática, agora, do crime de lavagem de dinheiro.

À dificuldade de obtenção de prova nos crimes cibernéticos ainda se soma o princípio penal da territorialidade, diante da falta de fronteiras que o crime virtual possui, tendo em vista que o criminoso pode possuir um provedor internacional, maquiar seu IP por outro localizado em outro país, e praticar o crime no Brasil. Instaura-se não apenas um conflito de jurisdição, mas também de aplicação da lei penal no espaço, eis que cada país possui ordenamento jurídico próprio, assim como definições dos princípios e excessos à privacidade, somando-se ao elevado volume de informações constante das redes, bem como da necessidade de condução da investigação, agora não apenas por servidores capacitados juridicamente, mas também que entendam da tão complexa matéria de tecnologia de informação.

De acordo com Zumas (2020), um relatório emitido pela empresa *CipherTrace*, publicado em 2018, apontou elevado crescimento dos crimes virtuais, resultando na lavagem de cerca de 1.3 bilhões de dólares, por intermédio das ferramentas de *mixers*, o que demonstra a popularidade da utilização da moeda no meio criminoso.

No Brasil, inexiste instrumento normativo que regule a utilização da criptomoeda, tendo sido, porém, objeto de diversos projetos de lei que visam a sua regulamentação, assim como o PL nº 3825/2019, de autoria do Senador Flávio Arns, o qual institui a necessidade do Banco Central em regular e fiscalizar as operações realizadas com criptomoedas (BRASIL, 2019). Entretanto, o Banco Central Brasileiro já se manifestou, por intermédio do Comunicado 31.379, não reconhecer as criptomoedas como moeda, bem como não possuir qualquer intenção de regulamentá-las, pois, na época (2017), as transações ainda não apresentavam tais riscos. (BANCO CENTRAL DO BRASIL, 2017).

Entretanto, diante do crescimento e do grande volume de transações envolvendo criptomoeda, o Banco Central voltou a se manifestar emitindo, em 2019, um parecer reconhecendo as criptomoedas como bens e agregando-as junto à balança comercial. A receita Federal, por sua vez, emitiu a primeira regulamentação, tendo como objeto a criptomoeda, para que passe a ser obrigatório às corretoras que operam as criptomoedas informarem as transações realizadas e seus respectivos titulares. (BRASIL, 2019). Países como Argélia, Bolívia, Marrocos, Nepal, Paquistão e Vietnã proibiram a utilização de criptomoedas, seguidos de outros que proibiram apenas a movimentação de criptomoeda de forma nacional, mas toleraram, quando essa se dá em território estrangeiro.

Da análise da pesquisa realizada, bem como da legislação existente, constatamos que a utilização da criptomoeda, sem qualquer intervenção estatal, diminui o custo das operações de crédito, entretanto, traz uma insegurança social, pois passou a ser amplamente utilizada para fins ilícitos e forma de pedido de resgate. Não significa dizer que a criptomoeda, por si só, gera a impunidade, e que a mesma é irrastreável e totalmente anônima, mas sim que mediante o emprego de ardil, e da ampla capacitação dos criminosos sua utilização pode maquiar e dificultar a persecução criminal, o que pode resultar na impunidade do delinquente.

Os Tribunais Superiores Brasileiros ainda não se manifestaram de forma específica quanto à questão da utilização da criptomoeda nos crimes denominados como sequestro de dados, entretanto, países como os Estados Unidos já estão bem avançados em matéria de regulação.

4 CONSIDERAÇÕES FINAIS

O avanço da tecnologia, assim como traz benefícios para a população por intermédio da aproximação de fronteiras e da facilitação de serviços, também se traduz no aperfeiçoamento do *"modus operandi"* de autores de crimes, e isso nos restou clarificado com o surgimento dos crimes cibernéticos, em especial o que atualmente se denomina "sequestro de dados", o qual, conforme se verificou, mostra-se como uma modalidade do

crime de extorsão, visto que os indivíduos criptografam os dados e somente os liberam mediante o pagamento que ocorre, preferivelmente, por meio de criptomoedas.

A criptomoeda veio para subverter o controle do Estado do sistema financeiro, caracterizando-se como uma moeda única, que não possui fronteiras, nem está sujeita à territorialidade, sendo por alguns sociólogos e doutrinadores comparada como um sistema anárquico, diante da não regulamentação e falta de controle estatal, como forma de proteção dos segredos individuais e financeiros perante ao estado, gerando uma emancipação econômica e social do indivíduo.

Entretanto, essa falta de controle estatal, e a tendência ao anonimato das operações realizadas por intermédio da criptomoeda vêm dificultado, e muito, a investigação de crimes que envolvam sua utilização, ao passo que, por meio de alta qualificação e conhecimento técnico, os criminosos conseguem maquiar os rastros digitais, fazendo com que o sequestro de dados pelo pagamento de resgate por *bitcoins* seja considerado um crime quase perfeito.

Restou claro, por meio desse trabalho de pesquisa e da análise de seus resultados que não é a criptomoeda um meio de pagamento totalmente anônimo, mas sua utilização desafia a investigação e o sistema de persecução criminal tradicional, exigindo cada vez mais que os inquéritos e que as denúncias sejam orientadas por servidores altamente capacitados, os quais não bastam apenas possuir conhecimentos jurídicos mas também tecnológicos, eis que os crimes passam a ser cometidos por pessoas altamente capacitadas. O surgimento da criptomoedas e sua utilização no *intercriminis* lança um desafio às técnicas investigativas tradicionais, diante das novas facetas criminosas, assim como ao próprio Estado, mediante à instauração de um sistema financeiro à margem de controle, o qual vem movimentando grande quantidade de ativos financeiros.

A falta de legislação que regule as transações também é um fator que dificulta a punibilidade do criminoso, assim como sua identificação. Entretanto, um dos maiores desafios é o surgimento de uma legislação internacional, a qual possa regular de forma eficaz e homogênea, diante da característica da internacionalidade das transações realizadas.

No cenário internacional é inegável que, atualmente, não se tem nenhum mecanismo confiável de identificação dos titulares de transações realizadas mediante *bitcoins*; pelo contrário, o que verificamos é a existência de ferramentas que facilitam a obscuração da origem e do destino dos ativos mediante criptomoeda, o que vem sendo utilizado, também, para a realização do crime de lavagem de dinheiro.

A pesquisa realizada demonstrou que carecemos de políticas que enfrentem o tema com a seriedade que merece, pois, mesmo que estejamos repletos de inovações nesses últimos anos, a regulamentação do ambiente virtual está defasada e não é suficiente. E, ainda, quando analisamos a seara penal, tratando-se dos cibercrimes, o atraso é ain-

da mais preocupante, visto que as penas se mostram ínfimas com relação à gravidade das práticas.

A necessidade de um tratado internacional, que enfrente a questão, é premente e de máxima urgência, diante da transnacionalidade das transações, assim como da grande possibilidade, a depender da técnica e do *modus operandi* do criminoso, que um crime que utiliza a criptomoeda como meio de pagamento venha privilegiar a impunidade.

LEGAL NATURE OF RANSOMWARE CRIME AND THE USE OF CRYPTO-CURRENCY AS A MEANS OF IMPUNITY

ABSTRACT

The advancement of technology facilitates the life of the human being and creates new weaknesses inherent in the technological world, which are at the mercy of criminals who invade operating systems "hijacking" the existing data demanding payment for the ransom, called "ransomware". Investigating these crimes requires hard work, making crime almost a perfect crime. Thus, it is intended to expose the theme, to typify the conduct, as well as to present how these individuals act and how to avoid these practices, which is done through analysis of legislation and doctrine, concluding that the lack of legislation can result in impunity.

Keywords: Bitcoin. Internet. Data hijacking.

REFERÊNCIAS

AGUILAR, Amanda Albuquerque. **Responsabilidade civil dos bancos nos casos de danos e fraudes causados por hackers**. 2017. Trabalho de Conclusão de Curso (Direito) - Universidade do Estado do Amazonas, Manaus, 2017. Disponível em: http://repositorioinstitucional.uea.edu.br/handle/riuea/912. Acesso em: 26 nov. 2020.

ARAUJO, Fábio Lucena de. Aspectos jurídicos no combate e prevenção ao *ransomware*. In.: **Revista da pós-graduação lato sensu em direito da Estácio**, v. 1, n. 1, p. 67-93, 2019. Disponível em: http://revistaadmmade.estacio.br/index.php/latodireito/article/view/7200. Acesso em: 06 set. 2020.

BANCO CENTRAL DO BRASIL. **Comunicado nº 31.379, de 16 de novembro de 2017.** Brasil, 2017. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=31379. Acesso em: 23 set. 2020.

BITCOIN Price Today & History Chart. **Coinlib.** Coinlib provides live and historic

cryptocurrency prices, portfolio, alerts, news, charts and detailed coin data. 2020. Disponível em:https://coinlib.io/coin/BTC/Bitcoin?utm_source=foxbit.com.br&utm_medium=clwidget&utmcampaign=full_v2v. Acesso em 22 de set. de 2020.

BRASIL. **Decreto-Lei 2.848, de 07 de dezembro de 1940.** Código Penal. Rio de Janeiro, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/del-2848compilado.htm. Acesso em: 03 jul. 2020.

BRASIL. **Exposição de motivos da Lei 12.737 de 2012**. Brasília, 2011. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=A04E4AB6AE105A84C7786AF441C4FAE5.proposicoesWebExterno2?codteor=944218&filename=Tramitacao-PL+2793/2011. Acesso em: 05 set. 2020.

BRASIL. **Instrução normativa RFB nº 1.888, de 3 de maio de 2019**. Brasil, 2019. Disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592. Acesso em: 20 set. 2020.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Brasília, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 01 set. 2020.

BRASIL. **Projeto de Lei nº 3825 de 2019.** Disciplina os serviços referentes a operações realizadas com criptoativos em plataformas eletrônicas de negociação. Autoria: Senador Flávio Arns (REDE/PR). Brasília, 2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7973487&ts=1594035403660&disposition=inline Acesso em: 25 set. 2020.

CANADÁ detém primeiro suspeito do maior ataque contra a rede de computadores, ocorrido em fevereiro. *In*: **Folha de São Paulo.** São Paulo, 20 de abril de 2000. Disponível em: https://www1.folha.uol.com.br/fsp/mundo/ft2004200011.htm. Acesso em: 15 jul. 2020.

CAPEZ, Fernando. C**urso de direito penal, parte especial:** dos crimes contra a pessoa a dos crimes contra o sentimento religioso e contra o respeito aos mortos. Vol. 2, 12. ed. São Paulo: Editora Saraiva, 2012.

CARDOSO, Amilde Adilio; COSTA, Erico Souza; SILVEIRA, Fernando Alves. **Criptomoedas e Blockchain nos processos de inovação social.** *In*: II Congresso Sul Catarinense de Administração e Comércio Exterior. 2018. Disponível em: http://periodicos.unesc.net/admcomex/article/view/4461. Acesso em: 16 set. 2020.

CRESPO, Marcelo. Ransonware e sua tipificação no Brasil. **Canal Ciências Criminais**. Disponível em: https://canalcienciascriminais.com.br/ransonware-e-sua-tipificacao-no-brasil/. Acesso em: 15 set. 2020.

GOMES, Helton Simões. **Internet chega a 80% das casas, e TV digital aberta cresce, diz IBGE**. Publicado em 29 de abril de 2020. Disponível em: https://www.uol.

com.br/tilt/noticias/redacao/2020/04/29/internet-chega-a-80-das-casas-do-brasil-e-presenca-de-tv-cai-diz-ibge.htm#:~:text=De%20acordo%20com%20o%20IBGE,7%20milh%C3%B5es%20de%20lares%20online. Acesso em: 30 jun. 2020.

GONÇALVES, Victor Eduardo Rios. **Direito Penal Esquematizado:** parte especial. 6. ed. São Paulo: Editora Saraiva, 2016.

GRZYWOTZ, Johanna. **Virtuelle Kryptowährungen und Geldwäsche**. Berlin: Duncker & Humblot, 2019.

LASHARI, Intzar Ali; SHAIKH, Zaffar Ahmed. Blockchain Technology the New Internet. In.: **International Journal of Management Sciences and Business Research**, vol. 6. Abril, 2017. Disponível em: https://www.researchgate.net/publication/322254665_Blockchain_Technology_The_New_Internet. Acesso em: 16 set. 2020.

LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet.** São Paulo: Editora Juarez de Oliveira, 2005.

MACHADO, Felipe; VIANNA, Túlio. **Crimes informáticos.** Belo Horizonte: Editora Fórum, 2013.

MAIS da metade da população mundial está conectada à internet, diz ONU. **Agência Brasil.** Genebra – Suíça. Publicado em 07 de dezembro de 2018. Disponível em: https://agenciabrasil.ebc.com.br/internacional/noticia/2018-12/mais-da-metade-da-populacao-mundial-esta-conectada-internet-diz-onu#:~:text=A%20ag%C3%AAncia%20especializada%20da%20ONU,popula%C3%A7%C3%A3o%20mundial%2C%20utiliza%20internet%20atualmente. Acesso em: 30 jun. 2020.

MASSENO, Manuel David; WENDT, Emerson. O ransomware na Lei: apontamentos breves de Direito Português e Brasileiro. *In*.: **Direito & TI.** 17 de julho de 2017. Disponível em: http://direitoeti.com.br/artigos/o-ransomware-na-lei-apontamentos-breves-de-direito-portugues-e-brasileiro/. Acesso em: 10 set. 2020.

MELLO, Roberta. Dados contábeis entram na mira dos cybercriminosos. In.: **Fenacon - Federação Nacional das Empresas de Serviços Contábeis e das Empresas de Assessoramento, Perícias, Informações e Pesquisas.** 19 de outubro de 2016. Disponível em: http://www.fenacon.org.br/noticias/dados-contabeis-entram-na-mira-dos-cybercriminosos-1197/. Acesso em: 20 set. 2020.

NAWARI, Nawari O.; RAVINDRAN, Shriraam. Blockchain and building information modeling (BIM): Review and applications in post-disaster recovery. *In*.: **Buildings**, v. 9, n. 6, p. 149, 2019. Disponível em: https://www.mdpi.com/2075-5309/9/6/149. Acesso em: 18 set. 2020.

NUCCI, Guilherme de Souza. **Manual de direito penal.** 16. ed. Rio de Janeiro: Editora Forense, 2020.

PINHEIRO, Patrícia Peck. **Direito Digital.** 2. ed. São Paulo: Saraiva, 2007.

POLÍCIA encontra hackers que roubaram fotos de Carolina Dieckmann. *In*.: **Globo.com.** Publicado em 13 de maio de 2012. Disponível em: http://glo.bo/XNEVtu. Acesso em: 12 jul. 2020.

SHIMABUKURO, Adriana. **As investigações na era das moedas digitais.** *In*: Crimes cibernéticos: 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 18 set. 2020.

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

VICENTE, Rafael José. A criptomoeda como método alternativo para realizar transações financeiras. In.: **Maiêutica-Tecnologias da Informação**, v. 2, n. 01, 2017. Disponível em: https://publicacao.uniasselvi.com.br/index.php/TI_EaD/article/view/1692. Acesso em: 17 set. 2020.

WAKKA, Wagner. Brasil é o 2º país com mais ameaças de ransomware no mundo, aponta estudo. *In*.: **Canaltech.** Publicado em 13 de março de 2019. Disponível em: https://canaltech.com.br/seguranca/brasil-e-o-2o-pais-com-mais-ameacas-de-ransomware-no-mundo-aponta-estudo-134683/. Acesso em: 30 jun. 2020.

WANNACRY: o primeiro ransomworm na indústria de cibersegurança. *In*.: **PROOF.** 2017. Disponível em: https://www.proof.com.br/blog/wannacry-ransomworm/. Acesso em: 20 jul. 2020.

ZUMAS, Vytautas Fabiano Silva. Criptomoedas, criptocrime e criptoinvestigação. **DireitoNet.** 08 de maio de 2020. Disponível em: https://www.direitonet.com.br/artigos/exibir/11637/Criptomoedas-criptocrime-e-criptoinvestigacao. Acesso em: 20 set. 2020.