XII CONGRESSO RECAJ-UFMG

CRIMINOLOGIA E CYBERCRIMES

SÉRGIO HENRIQUES ZANDONA FREITAS

YURI NATHAN DA COSTA LANNES

LUCAS JERONIMO RIBEIRO DA SILVA

C929
Criminologia e cybercrimes [Recurso eletrônico on-line] organização XII Congresso RECAJ-UFMG: UFMG – Belo Horizonte;

Coordenadores: Sérgio Henriques Zandona Freitas, Yuri Nathan da Costa Lannes e Lucas Jerônimo Ribeiro da Silva – Belo Horizonte: UFMG, 2021.

Inclui bibliografia
ISBN: 978-65-5648-374-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: As novas fronteiras tecnológicas do acesso à justiça e os direitos fundamentais digitais em perspectiva crítica.
1. Direito e Tecnologia. 2. Acesso à justiça. 3. Direitos fundamentais digitais. I. XII Congresso RECAJ-UFMG (1:2021: Belo Horizonte, MG).

CDU: 34

XII CONGRESSO RECAJ-UFMG

CRIMINOLOGIA E CYBERCRIMES

Apresentação

É com muita alegria que o Programa RECAJ-UFMG – Acesso à Justiça pela Via dos Direitos e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais, a SKEMA Business School Brasil e o Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI tornam público à comunidade científica o conjunto dos oito livros produzidos a partir das discussões dos Grupos de Trabalho do XII Congresso RECAJ-UFMG, que teve por tema central "As novas fronteiras tecnológicas do acesso à justiça e os direitos fundamentais digitais em perspectiva crítica".

As discussões nos Grupos de Trabalho ocorreram em ambiente virtual ao longo dos dias 25 e 26 de novembro de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área, além de cento e quarenta e dois pesquisadoras e pesquisadores inscritos no total, provenientes de treze Estados da federação (Alagoas, Amazonas, Bahia, Distrito Federal, Espírito Santo, Minas Gerais, Piauí, Paraná, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina, Sergipe e São Paulo). Marcando um momento em que a terrível pandemia da COVID-19 finalmente dá sinais de apaziguamento, o que somente foi possível por conta da ciência, da vacinação em massa e do trabalho valoroso de todos os profissionais do Sistema Único de Saúde, o evento trouxe, após hiato de quase dois anos, painéis científicos presenciais na nova (e bela) sede da SKEMA Business School Brasil no bairro Savassi em Belo Horizonte-MG.

Os oito livros compõem o produto principal deste congresso, que há mais de uma década tem lugar cativo no calendário científico nacional. Trata-se de coletânea composta pelos cento e seis trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os oito grupos de trabalho geraram cerca de seiscentas páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre diversos temas jurídicos e sua relação com a tecnologia: Acesso à Justiça e Tecnologias do Processo Judicial; O Direito do Trabalho no século XXI; Estado, Governança, Democracia e Virtualidades; e Tecnologias do Direito Ambiental e da Sustentabilidade. No dia 26, serão abordados os seguintes temas: Formas de Solução de Conflitos e Tecnologia; Direitos Humanos, Gênero e Tecnologias do Conhecimento; Inteligência Artificial, Startups, Lawtechs e Legaltechs; e Criminologia e cybercrimes.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de vinte e quatro proeminentes pesquisadores ligados a renomadas instituições de ensino superior do país, dentre eles alguns mestrandos e doutorandos do próprio Programa de Pós-graduação em Direito da UFMG, que indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores e pós-graduandos que coordenaram os trabalhos.

Nesta esteira, a coletânea que ora se apresenta é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e com o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES. Importante lembrar, ainda, da contribuição deste congresso com a formação de novos pesquisadores na seara interdisciplinar entre o Direito e a tecnologia, uma vez que o número de graduandos que apresentaram trabalhos de qualidade foi expressivo. Destaca-se a presença maciça de pesquisadores do Estado do Amazonas, especialmente os orientandos do Professor Doutor Valmir César Pozzetti vinculados à Universidade Federal do Amazonas e à Universidade Estadual do Amazonas.

O Programa RECAJ-UFMG, que desde 2007 atua em atividades de ensino, pesquisa e extensão em acesso à justiça pela via dos direitos e soluções de conflitos, nos últimos anos adota linha investigativa a respeito da conexão entre o acesso à justiça e a tecnologia, com pesquisas de mestrado e doutorado concluídas. Em 25 de junho deste ano, celebrou um termo de cooperação técnica com o Grupo de Pesquisa Normative Experimentalism and Technology Law Lab – NEXT LAW LAB da SKEMA Business School Brasil, que prevê o intercâmbio permanente das pesquisas científicas produzidas pelo NEXT LAW LAB e pelo Programa RECAJ-UFMG na área do Direito e Tecnologia, especialmente as voltadas ao estudo do acesso tecnológico à justiça e a adoção da inteligência artificial no campo do Direito. Desta parceria nascerá, seguramente, novos projetos importes para a comunidade científica deste campo.

Com o sentimento de dever cumprido, agradecemos a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 28 de novembro de 2021.

Prof. Drª. Adriana Goulart de Sena Orsini

Coordenadora do Programa RECAJ-UFMG

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School Brasil

Prof. Dr. Caio Augusto Souza Lara

Professor da SKEMA Business School Brasil e Pós-doutorando vinculado ao Programa RECAJ-UFMG

BITCOINS E CRIMES CIBERNÉTICOS: A LINHA TÊNUE ENTRE O BENEFÍCIO E O PREJUÍZO À SOCIEDADE E AO DIREITO

BITCOINS AND CYBERCRIMES: THE THUNDERLINE BETWEEN BENEFIT AND DAMAGE TO SOCIETY AND LAW

Lunna Luiza Oliveira Pettersen [1]

Resumo

Analisando a crescente expansão das transações econômicas virtuais por meio de bitcoins, constata-se, em consequência, o aumento exponencial de crimes cibernéticos, principalmente o estelionato e a lavagem de dinheiro. Afinal, quando se trata de moedas que permitem sua transação de forma anônima e sem qualquer registro, não poderiam ser outras as consequências. Tem como principal vantagem o fato de não estar vinculado a um determinado sistema bancário, bem como pela possibilidade de transferências virtual a baixo custo, visto que não é necessário o pagamento das respetivas taxas inerentes às instituições financeiras tradicionais. Portanto, esse mercado altera todo o nosso sistema.

Palavras-chave: Crimes cibernéticos, Bitcoins, Legislações, Investigação policial

Abstract/Resumen/Résumé

Analyzing the growing expansion of virtual economic transactions through bitcoins, it is possible to see, as a result, the exponential increase in cybercrimes, mainly embezzlement and money laundering. After all, when it comes to currencies that allow your transaction anonymously and without any registration, the consequences could not be different. Its main advantage is the fact that it is not linked to a particular banking system, as well as the possibility of virtual transfers at low cost, since it is not necessary to pay the respective fees inherent to traditional financial institutions. Therefore, this market changes our entire system.

Keywords/Palabras-claves/Mots-clés: Cybercrimes, Bitcoins, Legislations, Police investigation

[1] Graduanda em direito, no 6° período, na modalidade integral na Escola Superior Dom Helder câmara. E-mail: lunna.petter@gmail.com

INTRODUÇÃO

Com o desenvolvimento da sociedade, surge para o direito a necessidade de se adaptar às suas expectativas e as novas tecnologias. Todavia, na mesma proporção em que a internet tem cada vez mais usuários para os mais variados fins, aumenta também o seu uso, assim como as demais tecnologias, para fins ilícitos. Esta pesquisa visa compreender a causa desses crimes e a falta de regras específicas dirigidas a eles e entender se este é realmente o problema principal. Como a Internet é uma "terra sem lei", os criminosos agem sabendo que sua identificação será dificultosa. Por isso, é mais que necessários esclarecer a linha tênue que existe entre a praticidade e impunidade das redes.

A presente pesquisa se utiliza das legislações, textos doutrinários e pensamentos críticos para discutir o impacto que as novas tecnologias geram na sociedade, tanto virtual, quanto material, e como isso influencia no direito e na realidade dos crimes cometidos virtualmente. Volta-se à vertente metodológica jurídico-sociológica. No tocante ao tipo de investigação, foi escolhido, na classificação de Witker (1985) e Gustin (2010), o tipo jurídico-diagnóstico e jurídico-comparativo. O raciocínio desenvolvido na pesquisa será predominantemente dedutivo.

O prof. Dr. Renato Nunes Bittencourt, e seu artigo "A sociedade de transição", é o marco teórico no qual a presente pesquisa se baseia. Segundo o autor:

> Se por um lado a tecnologia dá aos usuários ampla liberdade e máxima igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as pessoas com as quais se relacionavam virtualmente, além de lhes restringir a capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade.

O autor, visa demonstrar que com a internet surgiram novos meios de difusão e prática de crimes, nos quais tomaram proporções tão grandes que a internet foi perdendo a sua segurança. O anonimato, que deveria promover igualdade, foi o elemento principal para que os criminosos perdessem o pudor, afinal, eles sabem que é muito difícil de serem identificados, saindo impunes e cerceando a liberdade dos outros usuários sem qualquer consequência.

1. A EVOLUÇÃO DAS BITCOINS NO MERCADO ECONÔMICO

> O comércio na Internet chegou ao ponto de se apoiar somente em instituições financeiras como terceiros de confiança para processar pagamentos eletrônicos. Enquanto o sistema funciona bem o suficiente para a maioria das transações, ele ainda sofre da inerente fraqueza do sistema baseado na confiança. Transações completamente não reversíveis não são realmente possíveis, já que as instituições financeiras não podem evitar disputas de mediação. (...) Comerciantes precisam ficar atentos aos seus clientes, perturbando em busca de mais informações que eles podem

> nem vir a usar. (…) não existe nenhum mecanismo que faça pagamentos através de um canal de comunicações sem um terceiro de confiança.

Como se percebe da citação acima, o artigo " Bitcoin: A Peer-to-Peer Electronic Cash System", publicado em 2008 por Satoshi Nakamoto, iniciou o desenvolvimento de uma moeda virtual e descentralizada nunca vista anteriormente: Bitcoin. O artigo descreve a parte administrativa de um sistema financeiro apoiado nas ideias de privacidade, descentralização, desenvolvimento comunitário e distribuição dos bens necessários para manter o sistema funcionando entre seus participantes. Muitos pesquisadores a consideram uma das maiores revoluções desde a criação da Internet, alguns até afirmam que a superou.

1.2 A Bitcoin

"*Vires in Numeris*". Essa frase é o mantra que define sucintamente a ideia por trás da Bitcoin, a "força nos números". De forma simplória, a bitcoin nada mais é que dinheiro! É uma nova forma de dinheiro que não é emitida por nenhum governo. Assim, os Estados não têm o monopólio de cria-las, podendo ser facilmente trocada e resgatada, e o bitcoin é uma dessas ferramentas de troca não-governamentais, na qual ninguém está no controle nem do suprimento, nem do seu fluxo.

Este é um conceito revolucionário, pois não existe banco central, não existe concedente ou concedido. As pessoas podem negociar dinheiro remotamente sem passar por um intermediário.

2. TRANSAÇÕES ECONÔMICAS VIRTUAIS E A FACILIDADE PARA O COMETIMENTO DE CRIMES

No que se remete a relação com o mercado, começou a surgir de forma lenta. A moeda que foi inicialmente usada para comprar objetos sem deixar rastros na *deep web* agora está começando a dar os primeiros passos para sua implementação em vários países.

Nesse ponto, leciona Rodrigo Marcial Ledra Ribeiro:

> Inobstante a isso, o bitcoin ser considerado como bem imaterial não escusaria os seus operadores de desrespeitar regras referentes ao combate às fraudes e corrupção nos termos da Lei 9.613/98. A depender das transações realizadas em bitcoin, por exemplo, as partes podem recair no crime de ocultação de bens, direitos e valores, ao "ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal", nos termos do caput do artigo 1º da mesma lei (…).

Segundo um relatório da empresa especializada Netscout, entre 1º de janeiro e 3 de agosto de 2021, o Brasil sofreu mais de 39 mil ataques cibernéticos, para um total de 6,4 milhões

realizados em todo o mundo, e assumiu a segunda posição entre os maiores alvos em nível mundial, atrás apenas dos Estados Unidos, que lidera o ranking com mais de 1,33 milhões (21,7%).

Segundo o diretor da Netscout Arbor no Brasil, Geraldo Guazzelli:

> Quanto mais tecnologia você traz para o bem, mais portas você abre para o ilícito (...) Cada vez que você evolui com a tecnologia de proteção, o atacante descobre uma nova forma de te invadir (...) e a criticidade vem aumentando de uma maneira significativa na capacidade dos ataques, que vem crescendo de maneira considerável porque o mundo todo gira em cima de tecnologia.

Certamente o diretor Guazzelli abordou a realidade das bitcoins. Dada a crescente utilização da moeda virtual, passou-se a utilizar esse instrumento de valor em operação de câmbio ilegal, como pode ocorrer aquisição de moeda estrangeira, constituindo o crime de evasão nas suas três formas (caput do artigo 22 da Lei 7.492/86, evasão-envio previsto no parágrafo único, primeira parte, da Lei dos Crimes Contra o Sistema Financeiro (LCSF), ou evasão-depósito (última parte do parágrafo único da LCSF)).

3. OS CRIMES CIBERNÉTICOS E AS LEGISLAÇÕES

3.1. Crimes cibernéticos

O anonimato, traz consigo uma falsa sensação de poder, na qual centenas de usuários da Internet cometem os cibercrimes sem remorso algum. Esses, postam conteúdo ofensivo de todos os tipos para milhares de pessoas ou então cometem roubo de senha, sequestro de servidor, invasão de página e outros crimes virtuais.

De forma complementar, explica Rossini (2004):

> A definição de "delito informático" poderia ser talhada como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa, comissiva, praticada por pessoa física ou jurídica, ou seja, crime cibernético pode ser qualquer ato antijurídico e culpável, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

Apesar de ser um paradigma totalmente novo, vários são os casos de crimes cometidos. Por exemplo, a queda (pelo FBI) do mercado online conhecido como Silk Road, famoso por seu amplo uso para a venda de drogas anônimas, resultou na apreensão de 1,5 milhões de bitcoins em circulação. Isso causou uma queda imediata no valor da moeda em 20%.

3.2 legislações acerca do tema

A princípio, foi promulgada a Lei dos Crimes Cibernéticos (Lei 12.737/2012), conhecida como Lei Carolina Dieckmann, que prevê a tipificação de atos como invadir, roubar senhas, violar dados e divulgar informações privadas. O texto foi bastante reivindicado pelo sistema financeiro devido à grande quantidade de fraudes e furtos de senhas na internet.

Em segundo lugar, tem-se a Lei 12.735/12 que determina a instalação de delegacias especializadas para o combate de crimes digitais.

Contudo, as penas cominadas serão maiores se os crimes estiverem sujeitos à Lei de Segurança Nacional, se tiveram divulgado informações confidenciais do Estado (15 anos de prisão) ou se ficar tipificada a prática de outros crimes, tal como a formação de quadrilha.

Nesse sentido, o advogado José Gomes Colhado, especialista em crimes digitais, privacidade e proteção de dados, afirma que a legislação no Brasil ainda é insuficiente para a proteção contra crimes cibernéticos, apesar das mudanças no código penal em 2012. Além da cominação de penas irrisórias, o texto legal exige muitas condições para que uma invasão cibernética seja considerada crime, bem como a violação abusiva do mecanismo de segurança.

Há de se falar também na recente Lei Geral de Proteção de Dados (LGPD), que entrou em vigência em agosto de 2020 com o objetivo de aumentar a segurança para dados pessoais.

Sobre a LGPD, a advogada especialista, Natália Brotto, explica que a lei traz uma mudança de paradigma para dar outros direitos aos donos de dados no Brasil. Segundo ela, “embora a Constituição já garantisse direitos e o Marco Civil a garantia da proteção de dados, não tinha lei geral que protegesse as pessoas físicas de compartilhamento de dados”, e completa dizendo que com a LGPD há uma mudança da titularidade dos dados, que deixa de ser das empresas e passa a pertencer às pessoas físicas, dentro ou fora da internet.

A advogada acredita que o sentimento de impunidade nos crimes cibernéticos não está relacionado à falta de lei, mas sim à identificação dos responsáveis pelo cometimento do crime. Ela explica que “a lei existe, protege. O problema é achar quem fez o crime, conseguir fazer prova que foi a pessoa que praticou a conduta. Não é a falta da lei, a insegurança jurídica na internet. Mas a dificuldade de persecução penal de provar e processar”. De forma estritamente realista e correta, ela avalia o problema de forma não formalista, mas prática e existe mesmo uma demanda enorme no campo investigativo.

De modo contrário a ela, o especialista em gestão de risco cibernético Marco Mendes, da Aon Brasil, avalia que existe sim lacunas e que essa ausência de legislação de proteção de

dados representa um risco significativo e as consequências para a segurança serão sentidas nos próximos anos. Seguindo o pensamento do especialista, somente leis mais abrangentes e efetivas resolveriam a impunidade nos crimes cibernéticos, afinal, no sistema penal brasileiro "não há crime sem lei que previamente o defina". Contudo, se mostra uma visão rigidamente positivista que, apesar de ter seus méritos, não irá conseguir solucionar a problemática.

De acordo com a Pesquisa Global de Gerenciamento de Risco de 2019 realizada pela Aon, os ataques cibernéticos e violações de dados estão em sexto lugar entre os principais riscos para empresas e instituições. E se prevê que suba para o terceiro lugar em 2022.

Sabe-se, qualquer pessoa afetada pode recorrer ao judiciário para fazer valer o seu direito à reparação. No entanto, chegar aos criminosos é uma das maiores problemáticas que existem. Esses problemas são agravados pelo relativo anonimato oferecido pela Internet, bem como pela importância das limitações geográficas e físicas no ciberespaço. Os criminosos podem tirar vantagem de um número ilimitado de vítimas potenciais (Hinduia, 2007).

4. INVESTIGAÇÕES POLICIAIS NOS CRIMES CIBERNÉTICOS

A principal limitação existente relacionada aos crimes cibernéticos é capacidade de policiamento do Brasil (ou a falta dela).

Constata-se na realidade policial que os aplicadores do direito, no âmbito policial, não têm recursos para lidar com esses tipos de crimes e, embora o Ministério da Ciência, Tecnologia e Inovação e o Ministério da Defesa tenham tentado incentivar um maior envolvimento do setor privado na segurança cibernética, seus esforços têm sido muito lentos.

Uma das evidências mais importantes que podemos coletar é o que é conhecido como número de protocolo da Internet (IP). O problema está, ao tentar obter este endereço IP, pois embora estes possam ser determinados pelo provedor de Internet ou pelo administrador do site, a coleta dos dados do usuário que atualmente está acessando é lenta e burocrática. Sem falar nas ferramentas que podem mascarar e disfarçar o número IP, como as proxies, permitindo o anonimato na Internet, embora não sirvam apenas para fins ilegais. Um serviço como o TOR (The Onion Router) pode usar até três endereços errados em diferentes países, dificultando o rastreamento.

De acordo com a Convenção de Budapeste, os procedimentos de investigação que podem ser usados e a obtenção de provas se referem a todos os tipos de dados, incluindo o fluxo de dados (traffic data), que representam ligações entre computadores, contendo informações

sobre o percurso percorrido; dados com informações (contesnt data), ou seja, o conteúdo da própria informação; e os dados pessoais do agente (subscribe data), como nome, endereço e número de acesso, que ficam armazenados no banco de dados do fornecedor.

Contudo, apesar de existir esses meios de investigação, mostram-se bastante precários e ineficazes, muito pela falta de recursos tecnológicos na busca pela os autores dos crimes.

5. LEI 14.155/21 COMO SOLUÇÃO PARA A PROBLEMÁTICA

A partir da publicação da Lei 14.155 de 2021, sancionada pelo presidente Jair Bolsonaro, passa-se a ter esperança para os positivistas de que os crimes cibernéticos como o estelionato e outras fraudes praticados por meios digitais, como celulares e computadores serão potencialmente diminuídos. O texto altera o Código Penal (Decreto-Lei 2.848, de 1940) para agravar penas como invasão de aparelhos, furto qualificado e estelionato ocorridos em meio digital, conectado ou não à internet.

Todavia, apesar da publicação dessa lei, ainda se mostra extremamente difícil acabar com a impunidade, até mesmo aplicar essas novas penas, demonstrando mais uma vez que não é um problema legislativo.

CONCLUSÃO

Constata-se que as citadas alterações não são suficientes para resolver o problema da criminalidade que envolve as criptomoedas, inclusive a maior delas, a bitcoin. São necessárias medidas que vão além das meramente legais. Como o sistema das criptomoedas não vai mudar, isto é, não vai deixar de ser anônimo e de difícil rastreamento, pelo contrário, vai continuar se desenvolvendo, resta concentrar os esforços para garantir que quem ouse se aproveitar de suas atribuições para obter vantagem ilícita não saia impune.

Os especialistas, Kao e Wang (2009) indicam uma abordagem para melhorar a investigação do crime cibernético, que consiste em três etapas: identificação independente de leis digitais, informações correspondentes de diferentes fontes.

Dessa maneira, é mais um problema de recursos policiais, que são utilizados para chegar até os criminosos, do que legislativo, como vimos. Infelizmente, não tem como focar somente na teoria e nos estudos referentes às técnicas legislativas, se elas não tiverem retorno na prática.

REFERÊNCIAS:

BITTENCOURT, R. N. A sociedade de transição (Resenha do livro A sociedade de risco: rumo a uma outra modernidade de Ulrich Beck). **Filosofia** (São Paulo), v.53, p.60, 2010.

BOITEUX, Luciana. **Crimes informáticos: reflexões sobre política criminal inseridas no contexto internacional atual**. Doutrinas Essenciais de Direito Penal. vol. 8, 2010.

BRASIL. **Código Penal**. Decreto Lei n. 2.848/40. Disponível em: http://www.dji.com.br/codigos/1940_dl_002848_cp/cp184a186.htm. Acesso em: 21 abr. 2021.

BRASIL. **Comunicado Bacen n.º 31.379** de 16/11/2017. Alerta sobre os riscos decorrentes de operação de guarda e negociação das denominadas moedas virtuais. Disponível em https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=31379. Acesso: 21 de outubro de 2021.

BUDAPESTE**, Convenção sobre o Cibercrime**, 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoespertinentes-do brasil/docs_legislacao/convencao_cibercrime.pdf.. Acesso em: 21 de outubro de 2021.

Callanan, C. and Jones, N. (2009). **Project on Cybercrime**, University College Dublin, Ireland.

CAPPARELLI, Bruna. **Técnicas investigativas italianas articuladas com a utilização dos denominados captadores informáticos**. Revista Brasileira de Ciências Criminais. vol. 137, 2017.

CASABONA, Carlos María Romeo. **Dos delitos informáticos ao crime cibernético: uma aproximação conceitual e político-criminal**. Doutrinas Essenciais de Direito Penal Econômico e da Empresa. vol. 6, 2011.

CAVALCANTE, Waldek Fachinelli. **Crimes cibernéticos: noções básicas de investigação e ameaças na internet**. 2015. Disponível em: http://www.conteudojuridico.com.br/ artigo, crimes-ciberneticos-nocoes-basicas-de-investigacaoeameacas. nainternet, 54548.html. Acesso em: 21 de outubro de 2021.

CIPOLI, Pedro. **O que é engenharia social.** Canaltech. 2012. Disponível em: http://corporate.canaltech.com.br/o-que-e/segurança/O-queeEngenharia-Social/. Acesso em: 21 de outubro de 2021.

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

Hinduja, S. (2007). **Computer Crime Investigations in the United States**: Leveraging Knowledge from the Past to Address the Future, Internacional Journal of Cyber Criminology, 1 (1), 1-26.

JESUS, Damásio de; MILAGRE, José Antonio, **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

KAO, Da-Yu and WANG, Shiu-Jeng. The IP addres and time in Cyber-crime investigation. Policing: An International Journal of Strategies & Management, 32 (2): 194-208. 2009.

MARIAH, Dourado de Andrade *et al*. CONSIDERAÇÕES SOBRE A APLICABILIDADE DO DIREITO PENAL ACERCA DOS CRIMES VIRTUAIS. **Vertentes do Direito**, [*s. l.*], v. 4, n. 2, p. 191-205, 2017.

NUNES, Leandro Bastos. O bitcoin na condição de meio para a consumação de crimes econômicos. **Conjur**, [*S. l.*], p. 1-1, 30 set. 2021. Disponível em: https://www.conjur.com.br/2021-set-30/nunes-bitcoin-consumacao-crimes-economicos. Acesso em: 21 out. 2021.

RIBEIRO, Rodrigo Marcial Ledra. **Bitcoin no sistema financeiro nacional**, Curitiba, v. 14, n. 33, p. 190-205, jul./set. 2018. Disponível em file:///C:/Users/PRBA/AppData/Local/Temp/7432-30082-1-PB.pdf. Acesso em: 21 de outubro de 2021.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SEGUNDO, Luiz Carlos Coelho Correa. **Crimes Cibernéticos**: Análise das leis 12.735 e 12.737 no que tange a sua real necessidade de existência. Orientador: Profº Gibson Passinho da Silva. 2016. Tese de Conclusão de Curso (Bacharelado em direito) - Faculdade do Estado do Maranhão - FACEM, Maranhão, 2016.

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