UNIVERSIDADE CATÓLICA DO SALVADOR

CURSO DE DIREITO

ROQUE FELIPE DA SILVA SANTANA

CRIMES CIBERNÉTICOS: ANÁLISE EVOLUTIVA DA LEGISLAÇÃO PENAL BRASILEIRA E SEUS DESAFIOS

SALVADOR - BA

2021

ROQUE FELIPE DA SILVA SANTANA

CRIMES CIBERNÉTICOS: ANÁLISE EVOLUTIVA DA LEGISLAÇÃO PENAL BRASILEIRA E SEUS DESAFIOS

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientadora: Profa. Monica Antonieta M. da Silva.

SALVADOR - BA

2021

CRIMES CIBERNÉTICOS: ANÁLISE EVOLUTIVA DA LEGISLAÇÃO PENAL BRASILEIRA E SEUS DESAFIOS

Roque Felipe da Silva Santana

Monica Antonieta M. da Silva

RESUMO: As facilidades do ambiente virtual, sobretudo o anonimato, tornaram essa ferramenta um meio propício para atos criminosos, tornando-se cabível elucidar quais são os impactos jurídicos dos crimes virtuais, e quais instrumentos legais podem ser considerados no julgamento dos mesmos. Desse modo, este estudo teve por objetivo investigar a aplicabilidade da legislação brasileira contra aos crimes cibernéticos e seus desafios. Foi adotada a metodologia de Revisão Bibliográfica, a busca bibliográfica foi realizada através de base de dados como a BV, BDTD, google acadêmico, com apoio em artigos, teses e dissertações, entre 2010 a 2021. Há a necessidade de uma maior resolutividade e eficácia quanto a aplicabilidade dos mecanismos legais, haja vista a frequência com que esses tipos de crimes vêm sendo cometidos, sobretudo no momento atual de crise sanitária vivenciada pelo mundo decorrente da pandemia do novo corona vírus, e que por conta das medidas restritivas impostas de isolamento social, deixaram os indivíduos mais dependentes das ferramentas digitais e consequentemente mais vulneráveis a esses crimes. Torna-se fundamental preencher as lacunas normativas, diminuindo a impunidade e garantindo um ambiente de segurança aos usuários.

Palavras – chave: Crimes cibernéticos. Código Penal Brasileiro. Investigação Policial. Legislação.

CYBER CRIMES: EVOLUTIONARY ANALYSIS OF BRAZILIAN CRIMINAL LEGISLATION AND ITS CHALLENGES

ABSTRACT: The facilities of the virtual environment, especially anonymity, made this tool a favorable means for criminal acts, making it possible to elucidate what the legal impacts of virtual crimes are, and what legal instruments can be considered in their judgment. Thus, this study aimed to investigate the applicability of Brazilian legislation against cybercrime and its challenges. The Literature Review methodology was adopted, the bibliographic search was carried out through databases such as BV, BDTD, academic google, supported by articles, theses and dissertations, between 2010 and 2021. There is a need for greater resoluteness and effectiveness as the applicability of legal mechanisms, given the frequency with which these types of crimes have been committed, especially at the current time of sanitary crisis experienced by the world due to the new corona virus pandemic, and that due to the restrictive measures imposed on social isolation, left individuals more dependent on digital tools and consequently more vulnerable to these crimes. It is essential to fill regulatory gaps, reducing impunity and ensuring a safe environment for users.

Keywords: Cyber Crimes. Brazilian Criminal Code. Police investigation. Legislation.

SUMÁRIO

1 INTRODUÇÃO

O uso da internet vem se expandindo progressivamente ao longo dos anos, concomitantemente como a quantidade de usuários. Essa crescente evolução se deu por conta da facilidade devido aos amplos recursos que vieram para facilitar a vida de seus adeptos. A busca por informações, entretenimento, diversão, relacionamentos e transações comerciais são algumas das principais atividades por ela advindas.

Por outro lado, facilitou a prática de condutas ilícitas, e atualmente, existem diversos tipos de crimes que são praticados na seara virtual e de consequências incalculáveis à sociedade. Por conseguinte, o Código Penal Brasileiro, que dispunha sobre os delitos informáticos veio a se tornar obsoleto sem conseguir se manter lado a lado com os avanços proporcionado pela evolução tecnológica e pela rapidez e expertise dos criminosos.

Desta forma as condutas praticadas nesse âmbito, não podem ser objetos de ação penal, gerando um grande impacto na sociedade brasileira. Os crimes virtuais mais comuns e que violam os princípios e os direitos fundamentais dos cidadãos estão: Roubo de informações pessoais (privadas); Falsidade Ideológica; Crimes Contra a Honra das pessoas como: Calúnia, Injúria e Difamação; Ameaças de todos os tipos; Racismo (e outras formas de preconceito); Pornografia Infantil.

É de suma importância à compreensão acerca dessa problemática, posto que o fato de não se ter uma legislação específica gera uma camuflagem para tal problema. O grande mundo virtual está atrelado ao nosso mundo real, e no Brasil as leis conseguiram bons avanços ao tipificar algumas condutas de caráter grave, mas que traz lacunas e interpretações duvidosas. Esclarecer informações conflitantes acerca do tema, permitirá promover uma reflexão para maiores estudos relacionados ao tema, contribuindo para a comunidade acadêmica, profissionais e futuros profissionais da área.

Frente ao contextualizado, a presente pesquisa centra-se no seguinte problema: De que maneira a Legislação Brasileira se aplica aos crimes cibernéticos?

O objetivo geral dessa pesquisa é investigar a aplicabilidade da legislação brasileira contra aos crimes cibernéticos e seus desafios e os objetivos específicos: caracterizar os crimes cibernéticos e seus impactos na sociedade brasileira; mostrar a dificuldade da investigação policial no tocante a materialidade e tipificação dos

crimes cibernéticos; examinar o Código Penal Brasileiro e as legislações existentes em relação aos crimes cibernéticos no Brasil.

O presente artigo trata-se de uma pesquisa de Revisão Bibliográfica, sendo considerada uma pesquisa de suma importância, pois serve de subsídio para o desenvolvimento de outros trabalhos de cunho acadêmico.

> A finalidade da pesquisa bibliográfica é colocar o pesquisador em contato com o que já se produziu e registrou a respeito do seu tema de pesquisa, tendo como principal vantagem o fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente. Esta vantagem se torna particularmente importante quando o problema de pesquisa requer dados muito dispersos pelo espaço (GIL, 2009, p. 50).

Nesse tipo de pesquisa torna-se importante a escolha de bases de dados que possibilitem a identificação dos estudos de maneira mais abrangente e obtenção de: artigo em texto completo online; revista/livro disponível em biblioteca; leitura do resumo e texto original; leitura, sumarização e redação. Desse modo, a busca bibliográfica foi realizada através de base de dados como a Biblioteca Virtual (BV), Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), google acadêmico, com apoio em artigos teses e dissertações, condizente a temática, no período de 2010 a 2021, com o objetivo de identificar as produções mais atuais sobre o tema. A coleta de dados deu-se também com subsídio em livros, doutrinas, legislações. Foi realizada uma busca nas bases de dados, utilizando os termos no singular e plural: “crimes cibernéticos”; “Código Penal Brasileiro”; “Investigação Policial”; “Legislação”.

O período em que a coleta bibliográfica foi realizada compreendeu entre agosto de 2020 até o prazo final de entrega do artigo. Os pesquisadores que mais contribuíram para a discussão do tema foram: Souza; Volpe (2015); Souza et al. (2020); Silva; Silva (2019); Dorigon; Soares (2018); Cavalcante (2014) e Barreto (2017), tratando especificamente sobre os impactos dos crimes virtuais na sociedade; a legislação atual que trata sobre esse tipo de crime e sua associação com o CP de 1940 e as dificuldades e barreiras perante sua tipificação.

Foi realizada uma análise descritiva dos estudos apreendidos, buscando estabelecer um entendimento e ampliar o conhecimento sobre o tema pesquisado e elaborar as comparações de resultados.

2 EVOLUÇÃO DOS CRIMES VIRTUAIS E IMPACTOS NA SOCIEDADE BRASILEIRA

As inovações inerentes do mundo tecnológico e digital vieram com uma proposta de facilitar a vida das pessoas por meio de sua dinamicidade, versatilidade e praticidade, permitindo a postagem e publicização de uma variedade de informações em computadores e Gadgets (dispositivo eletrônico portátil) através de fotos, contatos, documentos, vídeos e dados bancários (WINCK et al., 2015).

Contudo, as facilidades do ambiente virtual, sobretudo o anonimato, tornaram essa ferramenta um meio propício para atos criminosos, tornando-se cabível elucidar quais são os impactos jurídicos dos crimes virtuais, e quais instrumentos legais podem ser considerados no julgamento dos mesmos. Desse modo, os crimes cibernéticos tornaram-se comuns em decorrência da inexistência de entendimento público acerca dos seus impactos jurídicos e sociais (RODRIGUES; LIMA; FREITAS, 2020).

A nomenclatura aplicada para a identificação de onde partiu a ação do criminoso tem denominações variadas como Mundo Virtual, Ciberespaço, Espaço Cibernético, Cyberspace, não existindo uma padronização mundial, e varia conforme o país e sua legislação. Foi na década 1960 que começou a surgir os primeiros criminosos, explorando a tecnologia que abarca os computadores e a internet. Utilizavam de conhecimentos para ter acesso às informações sigilosas de usuários, de empresas consideradas importantes, como as multinacionais e de distintos ramos de negócio (SOUZA; VOLPE, 2015).

Na década de 1970, o termo Hacker, de origem norte-americana, foi empregada na classificação de pessoas que desvendavam erros no sistema de rede de internet através do computador. Outra nomenclatura difundida foi o termo Cracker, que, além de conhecer com maiores detalhes as falhas dos computadores, roubavam e apagavam informações importantes de outros usuários na rede (SOUZA; VOLPE, 2015).

O progressivo uso da informática possibilita mais facilmente a coleta e a disseminação de informações de forma ampla. Crimes Cibernéticos, o termo escolhido para este estudo, são delitos cometidos por meio da internet, configurando-se como uma nova modalidade de crimes, com poucas iniciativas de resolução do problema, problema este que só vem evoluindo. Esta nova modalidade de perpetração de atos ilícitos mais organizados, tornam significativamente difícil de encontrá-los, já que para

tal feito é forçoso rastrear a origem do delito e atrelá-lo de alguma maneira a pessoa que o cometeu (SILVA, 2018).

Contudo, cabe destacar, mesmo que os criminosos se certifiquem de que não há rastros perceptíveis para as vítimas, as informações deixadas por eles no computador apresentam maior amplitude do que no ambiente físico, posto que, tudo que é feito na internet produz rastros, como dados que ficam registrados na rede de computadores. Deste modo, esses dados são passíveis de acesso, possibilitando descobrir quem foi o praticante do crime virtual, mesmo que, à primeira vista, não inexista qualquer vestígio. Tais dados incluem o IP do computador ou aparelho de comunicação com acesso à rede usado no ato criminoso e os rastros deixados no acesso a sites virtuais, programas e aplicativos (SOUZA; VOLPE, 2015).

Matsuyama; Lima (2017) conceituam crime crimes cibernéticos como sendo “condutas ilegais que se efetivam mediante a utilização de dispositivos informáticos, conectados ou não a rede mundial de computadores” (p. 02), bem como as ações criminosas contra equipamentos tecnológicos, sistemas de informação ou banco de dados.

Esse tipo de crime pode ser dividido em crimes contra a honra, com destaque para calúnia, difamação e injúria e encontram respaldo no Código Penal Brasileiro nos artigos 138, 139 e 140, respectivamente. O crime de calúnia (artigo 138) e difamação (artigo 139), são crimes de perspectiva objetiva, posto que o delito relaciona-se a estima social e reputação da vítima, sendo o primeiro, necessário a cominação de imputação falsa a determinada pessoa de fato definido como crime, e já o segundo, ofender a reputação da vítima para terceiro. O crime de injúria (artigo 140), é um crime considerado subjetivo, haja vista violar a sua dignidade, decoro e sua estima (RODRIGUES; LIMA; FREITAS, 2020). A legislação pertinente será discutida com mais detalhes adiante.

As condutas ilícitas em sua maioria são punidas pelo Código Penal vigente de 1940. A partir daí começaram a surgir às primeiras legislações com a finalidade de proteger os usuários da internet contra os crimes cibernéticos. A Lei nº 7.646/87, modificada pela Lei nº 9.609/98, tratava acerca a comercialização e a proteção intelectual de programas de computadores no território nacional, reconhecendo como crime suas violações. A referida lei, atualmente, protege a propriedade intelectual de programas de computador, sendo o crime tipificado de falsificação de programas de computador (pirataria).

Em 2012 surgiu à primeira lei brasileira criada exclusivamente para tipificação de crimes cibernéticos. O advento da Lei n° 12.737/2012, intitulada como Carolina Dieckmann, trouxe alterações no Código Penal vigente, acrescentando os artigos 154-A e 154-B, assim, originou-se o tipo penal invasão de dispositivo informático. O Marco Civil da Internet, oficialmente chamado de Lei n° 12.965/2014, é a lei que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

Segundo Tabosa et al. (2017) os crimes cibernéticos podem se dividir em duas categorias:

> -Categoria I: Insere delitos com a finalidade de reunir informações pessoais de forma a prejudicar de alguma maneira a vítima, conceituado de phishing. Por exemplo, a vítima inocentemente instala em seu computador algum tipo de vírus, o autor do crime tem a possibilidade de acessar os seus dados, unicamente, com a intenção de lhe prejudicar.
> -Categoria II: Abarca práticas de assédio e molestamento na internet, violência contra crianças, chantagem e intimidação. Por exemplo, o criminoso se insere em uma sala de bate-papo para interagir com a suposta vítima, estabelecendo uma relação de confiança, visto a facilidade de diálogo entre ambas e a “inocência” da mesma para concretizar relações afetivas. Após a consolidação da relação de confiança, os criminosos manipulam as vítimas de forma a praticarem atos que podem envolver a automutilação.

Essas condutas de violências e crimes referidos sempre estiveram presentes, contudo, nos últimos anos, evidencia-se consequências devastadoras a vida humana ao caluniar, difamar, injuriar, praticar pedofilia e outras práticas consideradas ilícitas, com danos psicológicos, por vezes, irreversíveis às vítimas. Assim, são expostas fotos íntimas, bem como a vida privada, de maneira grotesca e aviltante, roubam-se dados e informações (SOUZA; VOLPE, 2015).

Presencia-se também o aumento vertiginoso de crimes sexuais, como a pedofilia, onde imagens de crianças são compartilhadas frente a uma fiscalização ineficaz e meio incipientes para encontrar os pedófilos (SOUZA; VOLPE, 2015).

Outrossim, aplicativos modernos que possibilitam registrar, armazenar e divulgar o dia a dia em tempo real, fazem parte da vida das pessoas, que sentem a necessidade de compartilhar suas atividades, na maioria das vezes expondo de maneira exagerada sua intimidade, o que de fato, não justifica a prática criminosa. Mesmo assim, sobretudo com as mulheres, surge o crime de exposição à intimidade sexual, que em grande parte das situações é praticado por pessoas que apresentam

algum vínculo afetivo com a vítima, como companheiros, cônjuges ou amantes (SOUZA et al., 2020).

No âmbito da intimidade da vítima e o criminoso, com consentimento ou não, há registros mediante fotografias ou filmagens, de momentos íntimos e de cunho sexual, que na ocasião do término do relacionamento é publicado por este, de maneira a expor de forma inescrupulosa a intimidade da mulher, ou seja, violando a moral e o psicológico da mesma (SOUZA et al., 2020).

Conforme citam Santos et al. (2017) outra consequência dos crimes virtuais na sociedade, pode ser exemplificada pelo *cyberbullying* que é a prática proposital de utilizar a tecnologia digital para enegrecer, ameaçar, ferir ou algum ato com má intenção a outrem. Tal conduta, interfere negativamente na sociedade, na vida pessoal e sanidade mental das vítimas, e primordialmente, violando os direitos fundamentais dos cidadãos.

Ainda para os autores supracitados, evidenciando o alcance da Internet atualmente na sociedade, o cyberbullying não se restringe a determinadas partes do mundo, isoladamente, contrariamente, diz respeito a um fenômeno global acometendo grupos em distintas culturas e configurações. Os mecanismos mais usados pelos praticantes para agredir suas vítimas são os computadores e telefones celulares. No âmbito da educação, a violência é um dos principais motivos do incômodo vivenciado por muitos de seus atores, revelando-se como uma problemática atual da educação moderna.

A criminalidade da informática não trouxe apenas como resultados negativos o nascimento de novos comportamentos ilícitos, além dos já preconizados no ordenamento jurídico brasileiro, executadas com o auxílio do computador (RAMOS, 2017). Outras minudências foram trazidas com o surgimento da internet, já que as novas posturas atingem aos mais diversos bens e interesses da sociedade e a violação de bens jurídicos até então não abrangidos com a prática de um crime.

Os impactos jurídicos advindos dos crimes virtuais são o prejuízo ao bem jurídico tutelado (honra) da vítima, os desafios do Direito e da jurisdição em se aproximar dos avanços tecnológicos e, também, a dificuldade em encontrar os criminosos frente ao anonimato, que serão discutidos mais enfaticamente nessa pesquisa. A responsabilidade para processar e julgar esse tipo de crime, é o Estado do acusado, onde o criminoso se encontra (RODRIGUES; LIMA; FREITAS, 2020).

3 INVESTIGAÇÃO POLICIAL E CRIMES CIBERNÉTICOS

O uso crescente das novas tecnologias é uma característica presente nas sociedades e na vida dos cidadãos, o que torna imprescindível que o Estado possibilite que os mesmos usufruam dessa tecnologia com segurança, reprimindo a criminalidade no meio digital e viabilizando aos usuários comuns o apoio na tecnologia para as mais diversas atividades. A sociedade atual vive parte de suas relações jurídicas virtualmente, cabendo ao Estado erradicar os crimes e garantir a harmonia no meio digital (BRITO, 2020).

O crime virtual e/ou cibernético é um crime em que sua prevenção é bastante complexa, consequentemente de difícil investigação, de busca de provas complicada, cuja comprovação é extremamente difícil e a punição quase inconcebível, sobretudo pela inexistência de leis específicas (SILVA; SILVA, 2019), e anonimato dos criminosos.

A percepção de impunidade ocasionada pela sensação de anonimato é um dos fatores que motivam os criminosos a escolherem os ambientes virtuais para propagar ameaças, insultas raciais, ou para praticarem o denominado cyberbullying, entre outros (ABREU, 2014).

Desse modo, é fato que a investigação virtual no Brasil se depara com inúmeras barreiras construídas pela tecnologia, seja pela criptografia, ou pela inexistência de eficazes acordos internacionais contra os crimes cibernéticos, pela expertise dos criminosos em eliminar as informações rapidamente da rede. É sabido, não obstante, que diante das provas virtuais, esta deve seguir todos os pressupostos das provas comuns, culminando na exigência de uma investigação técnica-pericial (SILVA, 2017).

Sob essa mesma égide, a Polícia Federal e a Polícia Civil são as entidades de segurança pública capazes de iniciar a investigação criminal, em particular, os setores responsáveis pela investigação desse crime em âmbito virtual devem ser capacitados para lidar com eficiência e proatividade considerando todos os tipos de crime dessa natureza e elaborar um planejamento estratégico (WENDT; JORGE, 2013).

Considerando que no processo penal a investigação é uma etapa pré-processual imprescindível para as repercussões penais decorrentes do desrespeito da lei penal, faz-se forçosa a manifesta delimitação de autoria e materialidade do delito para condenação criminal baseado nos crimes virtuais (BRITO, 2020).

Contudo, o inquérito policial concernente aos crimes cibernéticos ainda é incipiente, posto que carece de complementos que auxiliem a polícia na investigação eficaz até chegar no autor e na averiguação da fidedignidade dos fatos (SILVA; MARQUES, 2019). Além da inexistência de uma aplicabilidade mais efetiva da legislação, há carência de procedimentos mais específicos no trato das condicionalidades deste crime, com destaque para a inexistência de informações compartilhadas entre as instituições, sobretudo para aquelas que trabalham particularmente com os sistemas de informação, o que compromete sobremaneira a ação célere da polícia investigativa (SILVA; SILVA, 2019).

Outro ponto a ser destacado é a ausência de registro de usuários que acessam o ambiente virtual nas chamadas lan houses e cyber cafés, bem como uso de documentos ilegais utilizados no preenchimento de cadastros, com vistas a acessar os serviços de internet, e para outras práticas associadas com o crime investigado (CAVALCANTE, 2014).

Importa salienta, de acordo com Ramos (2017), que no momento que o usuário acessa a rede de internet, lhe é cominado um número de IP – Internet Protocol, sendo que este possibilita que o usuário seja identificado, ou a investigação da ocorrência de determinado crime. O ponto chave é que este número só é designado ao usuário no momento da conexão, ou seja, ao desligar o modem, o endereço de IP será conferido a outra pessoa, na ocasião em que esta não tenha optado por um IP Fixo.

O IP quando solicitado ao provedor de acesso à internet, deve constar da data, momento da conexão e o fuso horário do sistema, visto que tais dados são fundamentais, posto que que sem as mesmas, há impedimento na quebra de sigilo das informações (RAMOS, 2017).

De acordo com Dorigon e Soares (2018), os proxies são servidores que atuam intermediando as requisições dos seus usuários, requerendo recursos ou serviços de outros servidores, ou seja, se conformam como um elo entre o usuário e tudo que é acessado por este no meio virtual. Assim, será constado o endereço IP do servidor proxy de quem teve acesso ao conteúdo disposto na internet e não do usuário que de fato acessou.

Os servidores proxies foram implementados com a finalidade de omitir o endereço IP do usuário para protegê-lo de possíveis crimes na rede, assim como contra fraudes e roubo de informações. Todavia, existem aqueles com o propósito de omitir a identificação dos usuários com fins de impedir a identificação do autor de

crimes, e a obter, por conseguinte, a não resolução do crime praticado (DORIGON; SOARES, 2018).

São os denominados proxys anônimos, método destinado a prática de atividades na internet de maneira a não deixar vestígios, com a finalidade de proteger o usuário, tais como suas informações pessoais ao esconder o endereço IP que fora atribuído, assegurando a não publicização dos dados de identificação do computador que originou um dado evento na internet (DORIGON; SOARES, 2018).

Para Abreu (2014) um importante elemento que dificulta à repressão dos crimes virtuais é a celeridade das informações inerentes ao mundo virtual. Na maioria das vezes, durante o processo de investigação penal, é preciso que os órgãos competentes tenham acesso as informações pessoais de usuários mais rapidamente e de maneira precisa, frente a potencial facilidade de desaparecimento das provas virtuais, ressaltando que nem sempre isso seja possível.

Conforme o doutrinador, não obstante as diligências executadas pelos operadores do Direito, frequentemente os provedores, na iminência de ordens judiciais, por barreiras técnicas, não conseguem bloquear todos os elementos violadores em circulação eficazmente ou mesmo levar ao conhecimento das autoridades com precisão os dados pessoais de todos que cometem a prática delituosa.

Ademais, nos crimes cibernéticos determinar o juízo competente é mais complexo haja vista que estes crimes são frequentemente cometidos contra qualquer um, independentemente do local, e causam danos por vezes irreparáveis e de proporções incalculáveis. Desse modo, torna-se mister enfatizar a essencialidade da implementação de uma inteligência e uma expertise na inteligência da polícia para tornar mais eficaz as investigações, reduzindo a impunidade sobre esses crimes (SILVA; MARQUES, 2019).

É cediço esclarecer que para que esta política seja concretizada é preciso ter acesso às informações específicas acerca da incidência desses crimes e de suas condições, perfil das vítimas, o horário mais comum da prática criminosa e o modus operandi do crime, de uma política organizada que oriente e coordene setores responsáveis, primordialmente pela investigação dos crimes (SANTOS; MARTINS; TYBUCSH, 2017).

Elemento essencial na garantia da eficácia da ação do investigador é, ao ter ciência da prática de um crime cibernético, projetar qual foi o instrumento que os

criminosos utilizaram para o ato ilícito. O crime pode ter se conformado com o uso de programas maliciosos, e-mails, websites, programas que propagam informações, grupos de debate, redes sociais, páginas de comércio eletrônico, entre inúmeros outros. De acordo com o meio utilizado para praticar o crime, distintas serão as ferramentas para se desvendar a autoria (CAVALCANTE, 2014).

Cavalcante (2014) defende que com a crescente utilização de smartphones, tablets e computadores portáteis, mais conexões sem fio ou redes wireless vão surgindo, o que permite acessar gratuitamente à internet. Contudo, estas conexões possibilitam o acesso de pessoas não identificadas, aumentando as oportunidades para criminosos, visto que dificultam sua localização, e facilitam a inserção com finalidade criminosa.

Nesse sentido, o combate ao crime cibernético também necessitou se moldar à nova realidade, posto que o progresso da tecnologia viabiliza o acesso absoluto dos criminosos ao mundo cibernético. Para conseguir a identidade de quem praticou ato ilícito na internet, é necessário solicitar aos provedores de aplicações de internet as informações de acesso do usuário que realizou determinada postagem (SILVA, 2017).

Ramos (2017, p. 50) relata que" há uma escassez de profissionais qualificados para esse tipo de investigação, visto que para a elucidação desses tipos de crimes tornam-se necessários a participação de profissionais extremamente capacitados" e especializados para trabalhar com a perícia volvida em investigações de crimes cibernéticos, de maneira a prover os requisitos técnicos de coleta e guarda, com a finalidade de impedir o surgimento de questionamentos sobre a identidade da prova e a veracidade de sua obtenção.

Concernentes a investigação policial e emissão do laudo pericial, a capacitação do investigador ou perito relaciona-se de maneira direta ao êxito ou não das provas abstraídas. Estes profissionais devem estar capacitados para, por meio do uso das mais modernas tecnologias, obter indícios que possibilitem a aquisição de provas, a preservação do local e dos instrumentos e métodos utilizados na ação da conduta ilícita (RAMOS, 2017).

Por derradeiro, a lei para garantir sua aplicabilidade e eficácia e produzir resultados, se inicia na ocasião em que o legislador emprega de maneira transparente e completa a tipificação dos crimes. Sem isso, além dos desafios na identificação dos autores dos crimes, apenas resta a dificuldade em puni-los adequadamente. Com isso, advém o fato de que, geralmente, investigações e processos sobre crimes

cibernéticos no Brasil não culminam em desfechos eficientes e expressivos, justificada pela legislação incipiente, associada a precariedade de ferramentas digitais e tecnológicas à disposição das polícias (MEDEIROS; UGALDE, 2020).

4 LEGISLAÇÃO BRASILEIRA E CRIMES CIBERNÉTICOS

Os crimes cibernéticos fazem alusão a todos aqueles crimes que se materializam em meio virtual, possuindo classificações. A primeira classificação diz respeito aos crimes puros, cuja finalidade é alcançar o sistema de um computador, seja o ambiente físico ou de informações, comumente pela ação dos hackers; os crimes mistos, o foco em si não é o computador, mas o que a vítima possui, por assim dizer, a internet é usada com finalidade de cometer o crime, com destaque para transferências ilegais de bens ou valores; os crimes comuns, que se valem da internet para concretizar o crime, já validado em lei, como por exemplo a pornografia infantil, já enfatizado no Estatuto da Criança e do Adolescente.

A segunda classificação abarca os crimes próprios, cuja pratica acontece exclusivamente através dos computadores e os crimes impróprios, que alcançam o bem comum, no qual o ambiente virtual somente é uma das alternativas da prática do crime, e pode ser executado por outros meios.

De acordo com Barreto (2017), os crimes perpetrados em ambiente virtual estão crescendo progressivamente, deixando os consumidores vulneráveis e suscetíveis a se tornarem vítimas. Ademais, a legislação brasileira é esparsa e não acompanha a diversidade de tipos de crimes cibernéticos existentes, inexistindo um preceito específico que concretize uma taxatividade a esses crimes, sequer uma delimitação jurídica adequada.

Concernentes aos crimes cibernéticos impróprios, grande parte das ações são punidas com respaldo no obsoleto Código Penal de 1940. Cabe destacar nessa classificação os crimes contra a honra e os de fraude, furto, chantagem, falsificação, apropriação indébita, falsa identidade, etc (BARRETO, 2017).

Frequentemente, é aplicado o princípio da analogia como único meio hábil a não deixar o infrator cibernético impune. Contudo, tal princípio não é aplicável no Direito Penal, por ferir do princípio da taxatividade, sendo necessária a criação de leis mais específicas.

São exemplos de normas aplicadas, com a utilização da analogia, aos crimes virtuais: Calúnia (art. 138 do Código Penal); Difamação (art. 139 do Código Penal); Injúria (art. 140 do Código Penal); Ameaça (art. 147 do Código Penal); Furto (art. 155 do Código Penal); Dano (art. 163 do Código Penal); Apropriação indébita (art. 168 do Código Penal); Estelionato (art. 171 do Código Penal); Violação ao direito autoral (art. 184 do Código Penal); Pedofilia (art. 240 e 241 da Lei nº 8.069/90 – Estatuto da Criança e do Adolescente); art. 234 (Pornografia Infantil); Crime contra a propriedade industrial (art. 183 e ss. da Lei nº 9.279/96); Interceptação de comunicações de informática (art. 10 da Lei nº 9.296/96); Interceptação de E-mail Comercial ou Pessoal (art. 10 da Lei nº 9.296/96); Crimes contra software – "Pirataria" (art. 12 da Lei nº 9.609/98).

Os doutrinadores Medeiros e Ugalde (2020) traçam um resumo acerca dos crimes cibernéticos mais comuns. Os crimes contra a honra encontram-se dispostos nos art. 138, 139 e 140 do Código Penal, com aplicação em crimes cometidos tanto em ambiente virtual, quanto fora dele.

> Artigo 138 CP: Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa. § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
>
> Artigo 139 CP: Difamar alguém, imputando-lhe fato ofensivo à sua reputação. Pena - detenção, de três meses a um ano, e multa.
> Exceção da verdade
> **Parágrafo único** - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.
>
> Artigo 140 CP: Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa.

O art. 234[1] do Código Penal trata acerca da pornografia infantil: Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno: Pena - detenção, de seis meses a dois anos, ou multa.

A pornografia infantil é um ato de violência sexual perpetrado contra crianças e adolescentes, reconhecido como crime pelo Estatuto da Criança e Adolescente (ECA),

[1] **§ 1º**. Incorre na mesma pena quem:
I - vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo;
II - realiza, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter;
III - realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno.

mediante a lei federal 8.069/1990, com alteração dada pela lei 11.829/2008. Em 2014, a Central Nacional de Denúncias de Crimes Cibernéticos confirmou como o crime cibernético mais comum, a pornografia infantil. Em 2015, o mesmo órgão identificou 43.182 denúncias anônimas de pornografia infantil com o envolvimento de 17.433 sites distintos (dos quais 5.142 foram excluídos) resididas em 4.956 hosts diversos, com conexão à Internet por meio de 3.956 números IPs distintos, cominados para 54 países distribuídos nos 5 continentes (REIS, 2017).

Atentando ao artigo 240 e 241, da Lei 8.069/1990, do ECA, encontra-se a tipificação criminosa de pedofilia:

> "Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
>
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
>
> § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
>
> "Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa."

Já o artigo 171, do CP: *"obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.* E os crimes contra a propriedade intelectual que lesam expressamente o direito autoral, encontra respaldo no artigo 184: *Violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.*

Barreto (2017) pontua que a Lei nº 7.232/84 é considerada uma das primeiras leis voltadas para os crimes virtuais, e determinou princípios e diretrizes acerca da Política Nacional de Informática (PNI) através da implementação do Conselho Nacional de Informática (CONIN).

Por conseguinte, surgiram outras legislações com vistas a proteção do bem jurídico em âmbito virtual e suas relações no meio. A Lei nº 7.646/87 sofreu revogação através da Lei nº 9.609/98, e tratava sobre o amparo intelectual e comercialização de programas de computadores no Brasil, reconhecendo como crime suas violações (BARRETO, 2017):

> Art. 35. Violar direitos de autor de programas de computador:
> Pena – Detenção, de 6 (seis) meses a 2 (dois) anos e multa.
>
> Art. 37. Importar, expor, manter em depósito, para fins de comercialização, programas de computador de origem externa não cadastrados:
> Pena – Detenção, de 1 (um) a 4 (quatro) anos e multa.

Em 2001, na Hungria, houve a criação através do Conselho da Europa, a Convenção de Budapeste, que versa sobre os crimes em meio virtual, mundialmente, com prioridade a uma política de combate ao crime com vistas a proteger a sociedade contra crimes cibernéticos, mediante legislação específica e do apoio internacional; contudo, o Brasil não acatou a referida convenção.

Outrossim, um importante avanço refere-se à promulgação da Lei 12.735 de 30 de novembro de 2012, sofreu alteração com a finalidade de modificar os aparatos legais já existentes, com a seguinte redação:

> Art. 1º: Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências (BRASIL, 2012, s/p).

Nesta mesma senda, a Lei Federal n° 12.737/2012 se inseriu buscando a tipificação de crimes praticados no cerne virtual, expressamente repudiados pela sociedade, todavia, não eram devidamente punidos perante a inexistência de cominação legal.

A referida lei versa acerca da tipificação dos crimes cibernéticos; modifica o Decreto-Lei nº 2.848, do CP; e é apelidada de “Lei Carolina Dieckmann”, referindo-se ao fato de que na ocasião em que o Projeto de Lei prosseguia na Câmara de Deputados a atriz foi vítima de crime virtual, tendo suas fotos íntimas expostas sem a sua anuência (RODRIGUES, 2020).

A aludida lei teve origem através do Projeto de Lei nº 2793/2011, que foi exposto em 2011, pelo então Deputado Paulo Teixeira (PT-SP), de acordo com Almeida et al. (2015), com tramitação urgente no Congresso Nacional, comparado aos demais projetos que versavam acerca dos crimes informáticos e que foram apreciados.

A lei alterou o CP, e acrescentou os artigos 154-A e 154-B, modificando os artigos 266 e 298 que já existiam:

> **Art. 154**-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
>
> **Art. 154**-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e 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. (Incluído pela Lei nº 12.737, de 2012)

Um outro avanço alcançado no âmbito virtual no Brasil foi, conforme defende Matsuyama e Lima (2017), “O Marco Civil da Internet”, por meio da promulgação da lei n.12.965/2014. A referida lei determinou princípios, garantias e responsabilidades para a utilização da internet no Brasil.

Para os doutrinadores supracitados, como garantias inovou no sentido de garantir a liberdade de expressão e a privacidade de seus usuários, com destaque para a neutralidade de rede, ou seja, tratamento de acesso a rede de internet de maneira igualitária, sem discriminação, limitação, bloqueio ou cobrança de maneira diferenciada dos serviços existentes na internet.

Nesse sentido, cabe trazer à baila, o artigo 21, da Lei 12.965/2014:

> “Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.
>
> **Parágrafo único**. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Conforme a lei, os provedores de internet tinham por obrigação proteger o registro de suas atividades e de seus usuários, na ocasião da navegação em suas plataformas e serviços, para de acordo com Ribeiro (2020) garantir a segurança as pessoas sejam jurídicas ou físicas, que utilizavam o meio digital, pondo fim ao termo de “terra sem lei”.

Nessa nova conjuntura, importa salientar, o episódio ocorrido em 2015, tendo o WhatsApp como protagonista, que por meio de sua conduta protetiva com os dados

de seus usuários, entrou na mira das decisões judiciais que decidiram a exposição da comunicação destes para apoiar as investigações criminais. Perante a não autorização em conceder tais informações pela empresa responsável pelo aplicativo, a justiça determinou que fosse suspenso o serviço em todo território nacional (RIBEIRO, 2020).

Mais recentemente, passou a vigorar a Lei 14.155/21, que traz maior rigidez as penas dos delitos de furto e estelionato perpetrados no cerne digital incluindo computadores, celulares e tablets. Modifica a lei n. 2.828 do CP, endurecendo as punições tais como invasão de dispositivo, furto qualificado e estelionato cometidos nesse ambiente, com conexão ou não à internet (GANEM, 2017)

Para o crime de furto, trouxe a pena de reclusão de quatro a oito anos. Já a pena do crime de invasão de dispositivo informático contido no art. 154-A do CP, passou de três meses a um ano de detenção, para, de um a quatro anos de prisão, adicionando-se um terço a dois terços se da invasão gerar dano econômico. Quanto ao crime de estelionato, este terá detenção de quatro a oito anos e multa quando a vítima for ludibriada e entregar seus dados através das redes sociais. Na utilização de servidor fora do país, crime praticado contra idoso ou vulnerável, a pena para estelionato também acresce.

Por derradeiro, as leis aqui descritas e detalhadas vieram com a finalidade de reformular e atualizar as legislações que dificultavam a tipificação de tais crimes no meio virtual, almejando cumprir os princípios que subsidiam o Direito Penal, tais como, o da legalidade e a proibição da analogia, com foco na proteção do usuário. Não obstante, as mesmas são insuficientes, considerando a impunidade e a lacuna normativa no combate aos crimes cibernéticos, necessitando-se urgente de aparatos legais mais específicos e eficazes.

5 CONSIDERAÇÕES FINAIS

O estudo mostrou que atualmente os crimes cibernéticos vem tomando amplas proporções no Brasil e em todo mundo, impactando significativamente a sociedade, violando os direitos fundamentais dos cidadãos, haja vista a facilidade que os criminosos encontram ao adentrar nesse ambiente e a dificuldade em encontrar os criminosos frente ao anonimato e a rapidez na destruição de provas.

A comprovação dos crimes cibernéticos é complexa e de difícil investigação, primordialmente pela inexistência de leis específicas e pela condição de anonimato dos criminosos. Há carência de procedimentos mais específicos no trato das condicionalidades deste crime; necessidade de capacitação e qualificação de profissionais; ausência de registro de usuários que acessam o ambiente virtual nas chamadas lan houses e cyber cafés; a celeridade das informações inerentes ao mundo virtual dificulta o acesso aos criminosos, além disso, estes crimes são frequentemente cometidos contra qualquer um, independentemente do local. Todos esses fatores consequentemente contribuem para a impunidade dos crimes.

A literatura apontou que a legislação brasileira contra os crimes cibernéticos é esparsa, se tornando um grande desafio frente a materialidade e tipificação desses tipos de crimes, bem como a punição eficaz aos seus autores. Dentre os crimes, cabe destacar os crimes contra a honra e os de fraude, furto, estelionato, chantagem, falsificação, apropriação indébita, falsa identidade, pedofilia, pornografia infantil, etc, presentes no Código Penal de 1940, sendo a pornografia infantil considerado um dos crimes mais comuns. Um avanço importante na legislação faz alusão a Lei Federal n° 12.737/2012, “Lei Carolina Dieckmann”, o “Marco Civil da Internet”, por meio da promulgação da lei n.12.965/2014 e mais recentemente, a Lei 14.155/21, que traz maior rigidez as penas dos delitos de furto e estelionato.

Por derradeiro, cabe enfatizar o alcance dos objetivos desse estudo, que mesmo diante de inserção e inovação nos mecanismos legais, ao descrevê-los, foi possível demonstrar a necessidade de uma maior resolutividade e eficácia quanto a suas aplicabilidades, bem como nas ferramentas de investigação criminal, haja vista a frequência com que esses tipos de crimes vêm sendo cometidos, sobretudo no momento atual de crise sanitária vivenciada pelo mundo decorrente da pandemia do novo corona vírus, e que por conta das medidas restritivas impostas de isolamento social, deixaram os indivíduos mais dependentes das ferramentas digitais e consequentemente mais vulneráveis a esses crimes. Torna-se fundamental preencher as lacunas normativas, diminuindo a impunidade e garantindo um ambiente de segurança aos usuários.

REFERÊNCIAS

ABREU, Eduardo Franco. **Os entraves à repressão aos crimes cibernéticos**, 2014. Disponível em: https://edufranco91.jusbrasil.com.br/artigos/142294529/os-entraves-a-repressao-aos-crimes-ciberneticos. Acesso em: 12 jun 2021.

AJEJE, Gisele Ajeje de Carvalho. A **persecução penal no crime cibernético e a aplicabilidade da norma penal**. 2018. Número total de folhas, 55. Trabalho de Conclusão de Curso, Graduação em Direito – Faculdade Anhanguera, Campinas, 2018.

ALMEIDA, Jessica de J. et al. Crimes cibernéticos. **Caderno de Graduação-Ciências Humanas e Sociais-UNIT-SERGIPE**, v. 2, n. 3, p. 215-236, 2015.

BAPTISTA, Rodrigo. Lei com penas mais duras contra crimes cibernéticos é sancionada, maio 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada. Acesso em: 14 jun. 2021.

BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei n. 12.737/2012,** março 2017. Disponível em: http://www.conteudojuridico.com.br/consulta/artigos/49678/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012. Acesso em: 14 jun 2021.

BRASIL. **Lei 12.735 de 30 de novembro de 2012.** Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 28 mai. 2021

BRITO, Maximo. **A pratica das feke news e a falsa sensação de anonimato**, 2020. Disponível: https://mximobrito.jusbrasil.com.br/artigos/899194957/a-pratica-das-feke-news-e-a-falsa-sensacao-de-anonimato. Acesso em: 12 jun 2020.

BRITTO, Gladstone Avelino; FREITAS, Maristella Barros. Ciberataques em massa e os limites do poder punitivo na tipificação de crimes informáticos. **Revista de Direito Penal, Processo Penal e Constituição**, v. 3, n. 2, p. 1-16, 2017.

CARNEIRO, Adeneele Garcia. Crimes Virtuais: Elementos Para uma Reflexão Sobre o Problema na Tipificação. In: **Âmbito Jurídico**, Rio Grande, 15, n. 99, abr. 2012.

CAVALCANTE, Waldek Fachinelli. **Crimes Cibernéticos: noções básicas de investigação e ameaças na internet.** 2016. Disponível em: https://www.conteudojuridico.com.br/open-pdf/cj054548.pdf/consult/cj054548.pdf. Acesso em: 12 jun 2021.

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 23, n. 5342, 15 fev. 2018. Disponível em: https://jus.com.br/artigos/63549. Acesso em: 12 jun. 2021.

MATSUYAMA, Keniche Guimarães; LIMA, JAA. Crimes cibernéticos: atipicidade dos delitos. 2017. Disponível em:< joaoademar.qlix.com.br/3cbpj.pdf>. Acesso em: 20 nov 2019.

MEDEIROS, Gutembergue Silva; UGALDE, Júlio César Rodrigues. **Crimes Cibernéticos: Considerações Sobre a Criminalidade na Internet,** setembro 2020. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/. Acesso em: 12 jun 2021.

NASCIMENTO, Cláudia Rufino do et al. Crimes Cibernéticos à Luz Da Lei 12.737/2012: Avanços e Retrocressos. **Revista de Trabalhos Acadêmicos-Universo Recife**, v. 4, n. 2, 2017.

RAMOS, Eduardo Dulcetti. **Crimes cibernéticos: análise evolutiva e legislação penal brasileira**. 2017. 64 f. TCC (Graduação) - Curso de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017.

RIBEIRO, Raphael. A importância do marco civil da internet na preservação e utilização da prova criminal em ambiente digital. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498**, v. 16, n. 16, 2020.

RODRIGUES, Mariane; LIMA, Inayá Farias de; FREITAS, Rafael de. Crimes cibernéticos à luz dos crimes contra a honra. **ANAIS CONGREGA MIC-ISBN: 978-65-86471-05-2 e ANAIS MIC JR.-ISBN: 978-65-86471-06-9**, v. 16, p. 354-359, 2020.

SANTOS, Juliana Andrade; RODRIGUES, Marília Santos; SILVA, Juliana de Oliveira Musse. Cyberbullying: Violência Virtual com Consequências Reais. In: **Congresso Internacional de Enfermagem**. 2017. Disponível em:< https://eventos.set.edu.br/index.php/cie/article/view/5460/0>. Acesso em: 20 nov 2019.

SANTOS, Izabella O.'Hara Alves dos; CARVALHO, Grasielle Borges Vieira de. Atuação da polícia civil de Sergipe nos crimes contra a honra praticados em meio virtual. **Caderno de Graduação-Ciências Humanas e Sociais-UNIT**, v. 4, n. 1, p. 41, 2017.

SANTOS, Liara Ruff dos; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. **Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo.** IV Congresso Internacional de Direito e Contemporaneidade, Santa Maria/RS, 8 a 10 de novembro de 2017.

SILVA, Rafael; MARQUES, Daniel. CRIMES CIBERNETICOS E SUA COMPETENCIA. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498**, v. 15, n. 15, 2019.

SILVA, Ingryd Martins. **A infiltração policial como técnica especial de investigação no ambiente cibernético.** 87f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal Fluminense, Macaé, 2017.

SILVA, S.T. da. **Crimes Cibernéticos**. 2018. Disponível em:https://repositorio.pgsskroton.com.br/bitstream/123456789/20424/1/SILENE%20TOMAZ%20DA%20SILVA.pdf. Acesso em: 20 nov 2019.

SILVA, Gleice Kelly Paixão. **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos na deep web e dark web**. 2019. Disponível em:http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7911. Acesso em: 20 nov 2019.

SILVA, Kaique Rodrigues da; SILVA, Rubens Alves da. crimes cibernéticos: necessidade de novas ferramentas de investigação com encargos no ônus da prova. **Revista Artigos. Com**, v. 12, p. e2480-e2480, 2019.

SOUZA, Henry Leones; VOLPE, Luiz Fernando Cassilhas. **Da ausência de legislação específica para os crimes virtuais**. Congrega. Mostra de Iniciação a Pesquisa, Centro Universitário da Região da Campanha, 2015.

SOUZA, Luiza Catarina Sobreira et al. "Pornografia De Vingança": Uma análise acerca das consequências da violência psicológica para a intimidade da mulher. **Interfaces Científicas-Direito**, v. 8, n. 2, p. 103-116, 2020.

TABOSA, Bianca M. Batista et al. A psicopatia em sua dimensão virtual: um olhar acerca do fenômeno baleia azul. **Revista Eletrônica de Direito da Faculdade Estácio do Pará**, v. 4, n. 5, 2017.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos (2a. edição): Ameaças e procedimentos de investigação**. Brasport, 2013.

WINCK, Daniela et al. **A legislação e os cybercrimes**. Seminário de Iniciação Científica e Seminário Integrado de Ensino, Pesquisa e Extensão, 2017.