FACULDADE TRÊS PONTAS – FATEPS

DIREITO

RODRIGO DE SOUSA

CIBERCRIMES: O Uso da Internet como Instrumento Para a Prática de Delitos e a Evolução da Legislação Penal Brasileira no Combate aos Crimes Virtuais

Três Pontas

2022

RODRIGO DE SOUSA

CIBERCRIMES: O Uso da Internet como Instrumento Para a Prática de Delitos e a Evolução da Legislação Penal Brasileira no Combate aos Crimes Virtuais

Trabalho apresentado ao curso de Direito da Faculdade de Três Pontas – FATEPS, como pré-requisito para obtenção do grau de bacharel em Direito, sob orientação do Prof. Rodrigo Teófilo Alves.

Três Pontas

2022

RODRIGO DE SOUSA

CIBERCRIMES: O Uso da Internet como Instrumento Para a Prática de Delitos e a Evolução da Legislação Penal Brasileira no Combate aos Crimes Virtuais

Artigo Científico apresentado ao Curso de Direito da Faculdade Três Pontas – FATEPS, como pré-requisito para obtenção do grau de Bacharel em Direito pela Banca examinadora composta pelos membros:

Aprovado em / /

Prof. (Me.) (Ma.) (Esp.) (Dr.) Rodrigo Teófilo Alves

Prof. (Me.) (Ma.) (Esp.) (Dr.) Nome do professor

Prof. (Me.) (Ma.) (Esp.) (Dr.) Nome do professor

OBS.:

SUMÁRIO

CIBERCRIMES: O Uso da Internet como Instrumento Para a Prática de Delitos e a Evolução da Legislação Penal Brasileira no Combate aos Crimes Virtuais

Rodrigo de Sousa[1]
Rodrigo Teófilo Alves[2]

RESUMO

Este trabalho analisa a praticidade do meio virtual, especialmente o formato anônimo que é uma forte característica de tal área, o qual transformou esse instrumento em um meio favorável para práticas criminosas, tornando-se oportuno questionar quais são as consequências jurídicas dos delitos virtuais e quais ferramentas legais podem ser ponderadas no julgamento de tais crimes. Dessa forma, este estudo teve por intuito averiguar a aplicação da legislação brasileira em combate aos crimes cibernéticos. Foi utilizada a metodologia de Revisão Bibliográfica, a procura bibliográfica foi realizada por intermédio de base de dados virtuais tais como a BDTD, google acadêmico, com base em artigos, dissertações e teses, entre os anos de 2010 a 2022. Há a carência de um maior estudo no tocante a aplicabilidade dos instrumentos legais, tendo em vista a regularidade com que esses tipos de delitos vêm sendo praticados, especialmente no tempo atual, no qual houve uma crise na sanitária em caráter global por conta da pandemia do Coronavírus, as quais devido às determinações impostas de isolamento social tornaram as pessoas mais dependentes dos dispositivos virtuais

---

[1] Rodrigo de Sousa atualmente está cursando Direito na Faculdade Três Pontas – FATEPS, com colação de grau prevista para o ano de 2023.

[2] Rodrigo Teófilo Alves possuí graduação em Direito pela Faculdade de Direito de Varginha - FADIVA (2001) pás graduação em Direito Processual Civil e do Trabalho, pela Faculdade Cenecista de Varginha (FACECA 2010/2011). Mestre em Adolescência e Conflitualidade pela Universidade Bandeirante de São Paulo (2013). Ex-assessor Jurídico do TJMG. no período de 2005 a 2012, tendo atuando junto as Comarcas de Varginha (Vara Criminal e Execução Penal), Três Pontas (2ª Vara Civele Criminal) e Pitangui (2ª Vara Cível e Criminal). Ex-assessor Jurídico do TJMG atuando junto à 2ª Vara Cível, Criminal e Execução Penal da Comarca de Três Pontas no período de 07/2013 a 06/2015. Ex assessor Jurídico do TJMG atuando junto à 2ª Vara Criminal e Execução Penal da Comarca de Três Corações no período de 07/2015 a 01/2019. Advogado licenciado da 20ª Subseção Varginha, sob nº. 93503, em virtude de desempenho de cargo público. Atuou como assistente administrativo da Faculdade Cenecista de Varginha (MG) CNEC-FACECA, junto ao EAJAC (Escritório de Assistência Jurídica à Comunidade) como advogado. Professor de curso de graduação em Direito no Centro Universitário do Sul de Minas (UNIS-MG), na Faculdade Três Pontas (FATEPS) ministrando aulas de Direito Penal I, II, III e IV. Professor de Pós graduação junto ao UNIS, nas modalidades presencial e EAD. É membro do grupo para autorização e implantação do Curso de Direito nas Faculdades Integradas de Cataguases (FIC) e no Centro Universitário do Sul de Minas, ambas mantidas pelo Grupo UNIS. Professor em cursos preparatórios para o exame da Ordem dos Advogados do Brasil na Escola Mineira de Direito (EMD). Atualmente é Assessor Jurídico do TJMG atuando junto à 12 Vara Criminal e Execução Penal da Comarca de Varginha/MG.

e desse modo mais vulneráveis a esses crimes. O estudo evidenciou que as lacunas regulatórias devem ser preenchidas para reduzir a impunidade e garantir um ambiente seguro para os usuários na rede mundial de computadores.

Palavras-chave: Crimes Cibernéticos. Código Penal Brasileiro. Legislação.

1 INTRODUÇÃO

Trata-se de um estudo sobre a utilização da internet como ferramenta para realização de crimes e como o Direito Penal tem se portado na atualização da legislação no tocante ao combate aos delitos praticados virtualmente. Os Cibercrimes são os crimes cometidos por intermédio de meios informáticos, utilizando a internet como base para cometimento de delitos. Com a chegada da pandemia as pessoas começaram a utilizar mais os dispositivos eletrônicos conectados a rede de internet o que contribuiu muito para o crescimento dos tais crimes. A simplicidade do crime ocasionou uma "migração" do crime tradicional para o mundo virtual, visto que a menor exposição do criminoso (OLIVEIRA 2022). Pelo fato de serem crimes conceituados como silenciosos, visto não ameaçarem de modo direto a vítima como nos delitos tradicionais é necessário a adaptação da legislação para inibir tais condutas, assim punindo e aumentando a segurança da sociedade.

É dever do Direito identificar essas novas formas criminais que transgridam os princípios da liberdade e segurança os quais lesam a cidadania das pessoas, pois se tratam de novos delitos. A lei n. 12.737/2012 foi um enorme avanço, pois ela trata sobre tipificação infrações informáticas, ajudando no combate a cibercrimes, contudo, decorrido dez anos da criação desta lei o Brasil ainda carece de equipes designadas a melhorias das leis relativas à informática, com leis especializadas e de teor mais rígidos. Com a gradativa evolução tecnológica agregada ao mundo conectado, as distâncias foram reduzidas, com isso houve uma alta na utilização de equipamentos eletrônicos conectados a rede, tendo como efeito a aproximação de diferentes culturas e grupos, possibilitando a pessoas de todo o mundo poderem se socializar, diminuindo cada vez mais a distância com o avanço da tecnologia.

Portanto, o Direito deve se adequar a esta nova realidade, caminhando junto com a segurança da informação, para que esta nova sociedade digital não se torne um pesadelo para aquelas que a usam e acabam por ter suas imagens e/ou seus patrimónios comprometidos. É

característica do Direito seguir a evolução da sociedade, assim é necessária a criação de novos dispositivos legais para se adequar no que for necessário.

2 A PROGRESSÃO DOS CRIMES VIRTUAIS E SUAS CONSEQUÊNCIAS NA SOCIEDADE BRASILEIRA

2.1 CIBERCRIME: DEFINIÇÃO E CARACTERÍSTICAS

Um primeiro aspecto relevante trata-se da inovação referente à tecnologia e ao mundo digital a qual é acompanhada por um projeto com objetivo de facilitar o cotidiano dos indivíduos por meio de seu dinamismo, versatilidade e utilidade, permitindo a publicação e promoção de diversas informações em computadores e gadgets (dispositivos eletrônicos portáteis) por meio de fotos, contatos, documentos, vídeos e dados bancários (WINCK et al. 2015).

No entanto, a conveniência dos ambientes virtuais, principalmente o anonimato, torna o instrumento em um meio para facilitar o comportamento criminoso, para que possa ser devidamente articulada quais são as implicações jurídicas do crime virtual e quais instrumentos jurídicos podem ser considerado em seu julgamento. Dessa forma, o cibercrime tornou-se comum devido à falta de compreensão do público, suas implicações jurídicas e sociais (RODRIGUES; LIMA; FREITAS, 2020).

A nomenclatura usada para identificar a localização de uma ação dos criminosos têm diferentes terminologias como mundo virtual, ciberespaço, espaço cibernético, sem padronização mundial, variando de acordo com Estado e sua lei. Na década de 1960 que surgiu a primeira aparição desses tipos de infratores, usando seu conhecimento em dispositivos tecnológicos, incluindo computadores e Internet para obter informações confidenciais dos usuários, empresas consideradas importantes, tais como de diferentes áreas de negócios bem como multinacionais (SOUZA; VOLPE, 2015).

Na década de 1970, o termo hacker, originário da América do Norte, era conhecido como termo usado para triagem de pessoas que encontram bugs em sistemas de computadores ligados á internet. Outra palavra muito empregada é “cookie”, além de um olhar mais detalhado sobre a falha do computador, quem roubou e excluiu informações importantes de outros utilizadores da internet (SOUZA; VOLPE, 2015). O progresso emprego da tecnologia

da informação permitiram a coleta e divulgação ampla das informações do cibercrime, termo de escolha neste estudo, eles cometeram crimes pela Internet, configurando-se como um novo tipo de delito com poucas soluções para o problema. Este problema está apenas se desenvolvendo, este novo crime atrelado as atividades ilegais mais organizadas tornam muito difícil encontrá-los, pois tais feitos são cruciais no rastreamento da origem da infração e de alguma forma conectá-lo às pessoas que o cometeram (SILVA, 2018).

Vale a pena salientar, no entanto que, mesmo que os criminosos se certifiquem de que não deixaram vestígios, os dados que ficaram para trás nos dispositivos têm maior amplitude do que no ambiente físico, pois, todas as operações realizadas na Internet criam rastros, como dados cadastrados na rede computador. Desta forma, os dados ficam acessíveis, possibilitando encontrar quem esteja praticando crime virtual, mesmo à primeira vista, sem pistas. Esses dados incluem o IP do computador ou Comunicações com acesso a redes utilizadas em condutas infratoras e evidencias deixadas em acesso a sites virtuais, programas e aplicativos (SOUZA; VOLPE, 2015).

Mattssuyama e Lima (2017) definem o cibercrime como "Conduta ilícita que ocorre através do uso de equipamentos de informática, para conectar ou não à World Wide Web", e a operação criminosa visa equipamentos técnicos, banco de dados ou sistemas de informação.

Abordaremos no próximo tópico como são classificados os cibercrimes perante a legislação brasileira.

2.2 CLASSIFICAÇÃO DOS DELITOS VIRTUAIS

Esses delitos podem se classificar como crimes contra reputação com foco na calúnia, injúria e difamação e busca de amparo no direito penal brasileiro em seus artigos 138, 139 e 140. O delito calúnia (artigo 138) e difamação (artigo 139), são infrações de cunho objetivo porque o delito está relacionado com o respeito social e a reputação da vítima, antes de tudo, são necessários a atribuição ilícita de alguém, sendo de fato, estabelecida como crime e, em segundo lugar, prejudicar a reputação da vítima com terceiros. No (art.140) o crime de injúria é uma ofensa percebida como subjetiva com vista a violar sua estima, dignidade e decoro próprio (Rodriguez; Lima; Freitas, 2020). A legislação inerente será mais detalhada depois.

2.3 O AVANÇO TECNOLÓGICO COMO BASE PARA O AUMENTO DO CIBERCRIME

A maioria das violações é punível pela lei penal existente de 1940. Desde então apareceram as primeiras legislações, cuja finalidade era proteger os usuários da Internet contra crimes cibernéticos.

A lei atualmente protege a propriedade intelectual de programa de computador, sendo a pirataria, a qual é um delito em que o criminoso falsifica programas de computador. No ano de 2012 nasceu a primeira lei do Brasil dedicada à tipificação de crimes cibernéticos. O advento da Lei nº 12.737/2012 intitulada Carolinas Dieckmann alterou o atual Código Penal adicionando o artigo 154 como resultado, inserindo os artigos 154-A e 154-B, os quais originou o termo invasão de dispositivo informático. Esse marco civil da internet, oficialmente conhecida como Lei n° 12.965/2014, é a lei que regulamenta o uso da Internet brasileira fornecendo garantias, princípios, direitos e obrigações para aqueles que usam a rede, tal como do estabelecimento de diretrizes para determinar a atuação do Estado.

Conforme expressa Tabosa et al. (2017) as infrações informáticas segmentam-se em duas categorias, sendo a Primeira classe a inserção de delitos para objetivos de coleta de informações pessoais, sendo esta prática de prejudicar a vítima chamada de phishing.

Por exemplo, a vítima sem querer instalou vírus, assim os infratores podem acessar aos seus dados com o intuito de lesá-la. Já na segunda Categoria abrange práticas de assédio e molestamento na Internet, violência, chantagem e ameaças contra crianças. Tomando por exemplo, os transgressores da lei participam de uma sala de bate-papo para interagir com a suposta vítima, construindo assim uma relação de confiança, pois, a conversa entre flui facilmente, destarte o infrator alcança uma boa relação afetiva, fortalecendo as relações de confiança, manipulando as vítimas por conduta que possa envolver automutilação.

Esses atos violentos e criminosos mencionados sempre existiram, os últimos anos, no entanto, as consequências devastadoras para a vida humana tornaram-se aparentes. Ao caluniar, injuriar difamar, cometer pedofilia e outros atos considerados ilegais, podem haver danos psicológicos, às vezes irreversíveis para a vítima. Tendo por exemplo, fotos íntimas e de vida privada exibidas, de forma grotesca e degradante, roubo de dados e informação (SOUZA; VOLPE, 2015).

Os crimes sexuais também aumentaram dramaticamente, tal como a pedofilia, com compartilhamento de imagens de crianças, perante uma legislação ineficaz e métodos incipientes de encontrar os pedófilos (SOUZA; VOLPE, 2015).

Além disso, aplicativos modernos que permitem gravação, armazenamento e a divulgação em tempo real do cotidiano faz parte da vida das pessoas, as quais precisam compartilhar suas atividades, a maioria das vezes expostas exageradamente em suas intimidades, o que de fato não amolda-se como alegação para o comportamento criminoso.

Ainda assim, especialmente para as mulheres, surge o crime o qual expõe à intimidade sexual, na pluralidade dos acontecimentos por alguém a qual há algum vínculo com a vítima, como parceiro, amante ou cônjuge. No tocante à privacidade das vítimas e ofensores, com ou sem consentimento, pode-se também haver a intimidade sexual, publicada por este último no fim da relação, a qual a exposição desonesta da intimidade das mulheres é contra a moralidade e condições psicológicas, segundo (SOUZA et al., 2020).

Conforme mencionado por Santos et al. (2017) mais um consequência do delito virtual no corpo social, pode tomar o cyberbullying como exemplo, o qual trata-se de uma prática voluntária que utiliza a tecnologia digital para desacreditar, ameaçar, ou prejudicar de forma outras pessoas. Assim, tal conduta age negativamente a sociedade, interferindo de forma prejudicial a vida em geral de suas vítimas, infringindo os direitos fundamentais dos indivíduos.

Ainda para o autor acima, um testemunho da influência da rede de computadores na sociedade hodierna, o cyberbullying não se restringi a certas regiões, mas sim, envolve fenômenos que afetam o globo, em diferentes culturas e ambientes. Os dispositivos mais utilizados pelos agressores são telefones celulares e computadores. A violência é uma das predominantes razões de desconforto no contexto educacional, sendo muitos de seus participantes, expondo-se a questões educacionais contemporâneas, exibindo consequências negativas de nascimento de novos atos ilícitos, além dos já tipificados pelo Sistema jurídico brasileiro (RAMOS, 2017).

Com o advento da internet surgiram inúmeras práticas criminosas, pois, as novas posturas estão presentes nos mais diversos interesses da sociedade, visto tais violações de interesses legítimos não se encontravam estavam abarcados anteriormente como delito. O efeito jurídico do crime virtual é o dano ao bem tutelado da vítima “honra”, sendo grande um desafio da Jurisdição e do Direito de produzirem métodos de evolução tecnológica, portanto, enfrentando criminosos anônimos, o que será analisado mais a frente neste estudo. A

responsabilidade de processar e julgar tais crimes são do Estado Réu, onde está o infrator (RODRIGUES; LIMA; FREITAS, 2020).

2.4 INVESTIGAÇÕES POLICIAIS AOS CIBERCRIMES

O uso crescente de novas tecnologias é uma peculiaridade que se encontra constantemente presente nomeio social, tornando fundamental que o Estado permita que os indivíduos usufruam da tecnologia com segurança, dificultando infração no meio virtual e possibilitando que utilizadores habituais sejam capazes de gozar da tecnologia para as mais diversas atividades. Parte da vida na sociedade atual ocorre virtualmente, desse modo é mister que o Estado seja responsável por extirpar o crime e salvaguardar a harmonia no ambiente digital (BRITO, 2020). O combate ao crime virtual é altamente complexo e, portanto, difícil de investigar, pois, há muitas dificuldades para encontrar suas evidências, tornando a punição muito complexa de ser feita. (SILVA; SILVA, 2019).

A percepção de impunidade gerada pelo sentimento de anonimato é um dos motivos que levam os criminosos a optarem pelos ambientes virtuais para espalharem insultas raciais, intimidações, ou para realizarem o chamado cyberbullying, entre outros (ABREU, 2014).

Dessa maneira, é fato que a investigação virtual no Brasil se depara com múltiplos obstáculos construídos pela tecnologia, seja pela criptografia, ou pela inexistência de eficientes tratados internacionais contra as infrações virtuais, pelo método empregado pelos criminosos em desfazer das informações celeremente na rede. É notório, posto que diante das provas virtuais, esta deve obedecer todos os requisitos das provas comuns, culminando na imposição de uma averiguação técnica-pericial (SILVA, 2017).

Nesta mesma tese, as Polícias Civil e Federal são as entidades de segurança pública apta para darem inicio a investigação criminal, particularmente, as seções encarregadas pela investigação dessa infração na esfera virtual carecem ser capacitados para enfrenar com proatividade e eficiência levando em consideração todos os tipos de crime dessa natureza e estabelecer um planejamento estratégico (WENDT; JORGE, 2013).

Sabendo que no processo penal a averiguação é uma etapa pré-processual importantíssima para as repercussões penais das quais decorrem incumprimento da lei penal,

faz-se essencial a transparente fixação de materialidade e autoria do crime para condenação criminal com base nos delitos digitais (BRITO, 2020).

Contudo, associado ao inquérito policial relacionado aos crimes cibernéticos ainda é inicial, visto que necessita de complementos que ajudem a polícia na investigação efetiva até descobrir o autor e na averiguação da autenticidade dos fatos (SILVA; MARQUES, 2019).

Além da inexistência de uma aplicação mais eficaz da lei, há necessidade de métodos mais específicos no tratamento das contingências deste crime, com ênfase para a inexistência de informações compartilhadas entre as organizações, acima de tudo para aquelas que trabalham particularmente com os sistemas de informação, o que afeta sobremaneira a ação rápida da polícia investigativa (SILVA; SILVA, 2019).

Outro ponto a ser ressaltado é a falta de registro de usuários que acessam o mundo virtual nos conhecidos cybercafés e lan houses, tal como o uso de documentos ilegais usados em cadastros, almejando conectar aos serviços de internet, tal como para outras práticas associadas com a infração averiguada (CAVALCANTE, 2014).

É importante ressaltar de acordo com Ramos (2017), no instante que o usuário acessa a rede mundial de computadores, lhe é gerado um número de IP – Internet Protocol, sendo que este permite que o usuário seja reconhecido, ou a investigação da ocorrência de determinado delito. O ponto principal é que tal número só é dado ao usuário no momento da conexão, isto é, ao desligar o modem, o endereço de IP será concedido a outra pessoa, na hipótese em que este não tenha decidido por um IP Fixo.

O IP quando requerido ao provedor de acesso à internet, deve conter o fuso horário do sistema e a data, momento da conexão, dado que tais dados são essenciais, apesar de que sem as mesmas, apresenta-se restrição na quebra de confidência das informações (RAMOS, 2017).

Segundo Doriggon e Soares (2018), os proxies tratam-se de servidores que agem intermediando as solicitações dos seus utilizadores, requisitando serviços ou recursos de outros servidores, isto é, se comportam como uma ligação entre o usuário e tudo que é acessado por este no ambiente virtual. Desta forma, constará o endereço IP do servidor Proxy de quem teve acesso ao conteúdo colocado na internet e não do usuário que de realmente acessou.

Os servidores proxies foram implementados com o objetivo de omitir o endereço IP do usuário para resguarda-lo de possíveis crimes na internet, bem como contra roubo de informações e fraudes. Entretanto, há aqueles com o intuito de ocultar a identificação dos usuários com propósito de impedir a identificação do autor de crimes, e a obter, consequentemente, a não resolução do crime praticado (DORIGON; SOARES, 2018).

São os chamados proxys anônimos, método empregado à prática de atividades na rede de modo a não deixar vestígios, com o objetivo de defender o usuário, tais como seus dados particulares ao esconder o endereço IP o qual foi conferido, garantindo a não disseminação dos dados de identificação do computador que deu origem a um dado evento na internet (DORIGON; SOARES, 2018).

Segundo Abreu (2014) um relevante elemento que torna árduo à repressão dos delitos digitais é a rapidez das informações associadas ao mundo virtual. Na maioria das ocasiões, no desenrolar do processo de averiguação penal, é fundamental que os órgãos competentes tenham acesso às informações pessoais de usuários com mais celeridade e precisão, diante a potencial facilidade de sumiço das provas virtuais, salientando que nem sempre isso seja possível.

Conforme o doutrinador, mesmo com os esforços feitos pelos operadores do Direito, periodicamente os provedores, na ameaça de ordens judiciais, por obstáculos no que diz respeito à área técnica, não são altas para inibir todos os elementos violadores em fluxo eficazmente ou mesmo levar ao conhecimento das autoridades com lisura dos dados pessoais de todos que cometem a prática criminosa. Além disso, nos cibercrimes definir o juízo competente é mais complicado, tendo em consideração que estes delitos são rotineiramente cometidos contra qualquer um, independentemente do lugar, e ocasionam danos muita das vezes irreparáveis e de tamanhos imponderáveis.

Dessa maneira, torna-se mister enfatizar a necessidade da implementação de inteligência e técnicas atualizadas para tornar mais eficaz as averiguações, reduzindo a impunidade sobre essas infrações (SILVA; MARQUES, 2019).

É notório esclarecer que para que esta política seja efetivada é necessário ter acesso às informações essenciais acerca da ocorrência desses crimes e de suas condições, perfil das vítimas, o horário mais utilizado na prática criminosa e o modus operandi do delito, de uma

política estruturada que direcione e coordene setores responsáveis, principalmente pela investigação dos crimes (SANTOS; MARTINS; TYBUCSH, 2017).

Elemento fundamental na garantia da efetividade da ação do investigador é, ao ter conhecimento da prática de um crime virtual, apresentar quais foram as ferramentas que os infratores utilizaram para cometerem o ato ilícito. A infração pode ter se compatibilizado com o emprego de programas maliciosos, websites, e-mails, programas que espelhem informações, redes sociais, grupos de debate, páginas de e-commerce, entre vários outros. Conforme o meio usado para cometer o delito, distintos serão os instrumentos para se solucionar a autoria (CAVALCANTE, 2014).

Cavalcante (2014) defende que com a sucessiva utilização de tablets, smartphones e computadores portáteis, um número cada vez maior de conexões sem fio ou redes wireless vão aparecendo, o que permite o acesso de forma gratuita à internet. Porém, estas conexões propiciam o acesso de pessoas não identificadas, expandindo as oportunidades para criminosos, uma vez que dificultam sua localização favorecendo a inserção com objetivo criminoso.

Nessa lógica, o combate ao cibercrime, igualmente, careceu moldar-se à atual realidade, dado que o avanço tecnológico promove o acesso absoluto dos infratores ao mundo virtual. Para obter resultado em conseguir a identidade de quem realizou a infração na internet, é mister requisitar aos provedores de aplicações de internet os dados de acesso do usuário que realizou determinada postagem (SILVA, 2017).

Ramos (2017, p.50) apresenta que “há uma carência de profissionais especializados para esse tipo de analise, uma vez que para a explanação desses tipos de delitos tornam-se indispensável a participação desses profissionais com tal peculiaridade técnica”, com o objetivo de evitar o aparecimento de indagações sobre a identidade da prova e a autenticidade de sua aquisição.

No tocante à investigação policial e lançamento do laudo pericial, a competência do perito ou investigador associa-se de forma direta ao resultado ou não das provas não encontradas. Tais profissionais necessitam estar para, por intermédio do emprego das mais atuais tecnologias, conseguir indícios que propiciem a obtenção de provas, a conservação das ferramentas, métodos e o local onde houve a conduta ilícita (RAMOS, 2017).

Por último, a lei para assegurar sua eficácia e aplicabilidade e gerar efeitos, inicia-se no instante em que o legislador aplica de forma transparente e conclui a tipificação dos delitos.

Sem isso, além dos obstáculos na identificação dos autores dos crimes, somente resta a adversidade em puni-los apropriadamente. Com isso, resulta o fato de que, habitualmente, processos e investigações sobre crimes cibernéticos no Brasil não findaram em resultados significativos e efetivos, tendo por justificativa a legislação primeiramente, relacionada à fragilidade das ferramentas digitais e tecnológicas as quais estão à disposição das polícias (MEDEIROS; UGALDE, 2020).

2.5 A LEI BRASILEIRA E OS CIBERCRIMES

Os crimes virtuais fazem referência a todos aqueles delitos que se concretizam no meio virtual, nas seguintes classificações. Na primeira classificação refere-se aos crimes conhecidos como puros, da qual seu designo é alcançar o sistema de um computador, seja na esfera física ou de informações, habitualmente pela atuação dos hackers; os delitos mistos, com o foco não sendo o computador, mas sim o que a vítima possui, por assim dizer, a internet é usada com o objetivo de praticar o crime, com realce para transferências ilegais de valores ou bens; os crimes comuns, que se valem da internet para concluir o crime, já tipificado na legislação, tomando, por exemplo a pornografia infantil, já destacado no Estatuto da Criança e do Adolescente.

A segunda categoria abrange os crimes próprios, cuja pratica ocorre unicamente por intermédio dos computadores e os crimes impróprios, os quais afligem o bem comum, do qual o meio virtual tão somente é uma das alternativas da prática do delito, podendo ser executado por outros métodos.

Conforme elucida Barreto (2017), os crimes perpetrados no meio digital estão crescendo gradualmente, desta forma os consumidores estão ficando desprotegidos e sujeitos a se tornarem vítimas. Além do mais, a lei brasileira é dispersa e não acompanha a pluralidade de tipos de delitos cibernéticos existentes, inexistindo um preceito específico que estabeleça uma conceituação jurídica pertinente.

No tocante aos crimes cibernéticos impróprios, a grande maioria das ações são penalizadas com fulcros no obsoleto Código Penal de 1940. Vale salientar nessa classe as infrações de fraude, de furto, crimes contra honra, de chantagem, de falsificação, falsa

identidade, apropriação indébita, etc. (BARRETO, 2017). Regularmente, é empregado o preceito da analogia como singular capaz de não deixar o cibercriminoso impune. Entretanto, este preceito não é utilizado no Direito Penal, por transgredir o princípio da taxatividade, sendo mister a produção de legislação mais específica.

Abaixo estão exemplos de normas aplicadas, com a utilização da similaridade, aos crimes virtuais: Calúnia (artigo 138 do Código Penal); Difamação (artigo 139 do Código Penal); Injúria (artigo 140 do Código Penal); Ameaça (artigo 147 do Código Penal); Furto (artigo 155 do Código Penal); Dano (artigo 163 do Código Penal); Apropriação indébita (artigo 168 do Código Penal); Estelionato (artigo 171 do Código Penal); Violação ao direito autoral (artigo 184 do Código Penal); Pedofilia (artigo 240 e 241 da Lei nº 8.069/1990 - Estatuto da Criança e do Adolescente); artigo 234 (Pornografia Infantil); Crime contra a Propriedade Industrial (artigo 183 e ss. da Lei nº 9.279/1996); Interceptação de Comunicações de Informática (artigo 10 da Lei nº 9.296/1996); Interceptação de e-mail Comercial ou Pessoal (artigo 10 da Lei nº 9.296/96); Crimes contra software - Pirataria (artigo 12 da Lei nº 9.609/1998).

Os doutrinadores Ugalde e Medeiros (2020) esboçam uma síntese a respeito dos crimes virtuais mais comuns. Os crimes contra a honra encontram-se listados nos artigos 138, 139 e 140 do Código Penal, com aplicação em delitos praticados tanto em ambiente virtual, quanto em real. Dispõe os seguintes artigos:

> Art. 138. 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. (BRASIL, 1940)
>
> Art.139. 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. (BRASIL, 1940)
>
> Artigo 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa. (BRASIL, 1940)

O artigo 234 do Código Penal dispõe a respeito da pornografia infantil:

> Art. 234. 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.
> Parágrafo único - 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. (BRASIL, 1940)

No ano 2014, a Central Nacional de Denúncias de Crimes Cibernéticos comprovou como o delito virtual mais praticado, a pornografia infantil. No ano de 2015, o próprio órgão reconheceu 43.182 denúncias anônimas de pornografia infantil com o envolvimento de 17.433 sites diferentes (cujo 5.142 foram deletados) resididas em 4.956 hosts distintos, com conexão à rede mundial de computadores através de 3.956 números IPs diferentes, impostos para 54 países espalhados nos cinco continentes (REIS, 2017).

Nos artigos 240 e 241, da Lei 8.069/1990, do ECA, localizam-se a tipificação infratora 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. (BRASIL, 1990)

> 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. (BRASIL, 1990)

No que se refere ao artigo 171, do CP:

> Art. 171. 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. (Brasil, 1940)

Encontra-se respaldo no artigo 184 do CP os crimes praticados contra a propriedade intelectual que lesam expressamente o direito autoral:

> Art. 184. Violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa. (BRASIL, 1940)

Barreto (2017) expõe que a Lei nº 7.232/1984 é uma das leis pioneiras, sendo voltada para os delitos virtuais, a qual estipulou diretrizes e princípios a respeito da Política Nacional de Informática (PNI) por intermédio da implantação do Conselho Nacional de Informática (CONIN).

Consequentemente, apareceram outras legislações com planos a defesa do bem jurídico na esfera virtual bem como suas relações no meio. A Lei nº 7.646/1987 teve revogação por meio da Lei nº 9.609/1998, e tratava sobre a comercialização de programas de computadores e apoio intelectual no Brasil, reconhecendo como crime suas transgressões (BARRETO, 2017):

> Art. 35. Violar direitos de autor de programas de computador: Pena – Detenção, de 6 (seis) meses a 2 (dois) anos e multa. (BRASIL, 1998)
>
> 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. (BRASIL, 1998)

No ano de 2001, na Hungria, criou-se por meio do Conselho da Europa, a Convenção de Budapeste, que trata sobre os crimes no âmbito virtual, globalmente, com prioridade a uma política de combate ao delito com propósito de resguardar o corpo social de crimes digitais, através legislação apropriada e do auxílio internacional, porém, o Brasil não atendeu a mencionada convenção.

Igualmente, um significativo progresso correlaciona-se à promulgação da Lei 12.735 de 30 de novembro do ano de 2012, que foi alterada com o objetivo de transformar os dispositivos legais já existentes, com o seguinte texto: Art. 1º: Esta Lei modifica 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, a qual tipifica condutas praticadas por meio do emprego de sistema digital, eletrônico ou semelhantes, as quais sejam cometidas em desfavor a sistemas de natureza informática e similares; e dá outras providências (BRASIL, 2012, s/p).

Neste mesmo sentido, a Lei Federal n° 12.737/2012 foi introduzida buscando a tipificação de crimes praticados no âmbito virtual, largamente renegados pelo corpo social entretanto, não eram adequadamente punidos frente a inexistência de cominação legal.

A dita lei versa a respeito da tipificação dos cibercrimes; altera o Decreto-Lei nº 2.848, do Código Penal sendo apelidada de "Lei Carolina Dieckmann", a qual faz referência ao fato de que no momento em que o Projeto de Lei prosseguia na Câmara de deputados a atriz foi vítima de delito virtual, na qual teve fotos íntimas expostas sem seu consentimento (RODRIGUES, 2020). Tal lei originou-se por meio do Projeto de Lei nº 2793/2011, que foi manifesto em 2011, pelo então Deputado Paulo Teixeira do partido do PT-SP, conforme Almeida et al. (2015), com prosseguimento urgente no Congresso Nacional, assemelhando aos outros projetos que abordavam acerca dos delitos informáticos e que foram analisados.

A lei modificou o Código Penal, acrescentando-lhe os arts. 154-A e 154-B, alterando os artigos 266 e 298 que já existiam:

> 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). (BRASIL, 1940, Art. 154-A)
>
> 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). (BRASIL, 1940, Art. 154-B)

Uma outra progressão obtida na esfera virtual no Brasil foi, segundo defende Matsuyama e Lima (2017), "O Marco Civil da Internet", por intermédio da promulgação da lei n.12.965/2014, que estabeleceu garantias, responsabilidades e princípios para a utilização da internet no Brasil.

Para os doutrinadores supramencionados, como garantias houve inovação no sentido de salvaguardar a liberdade de expressão e a privacidade de seus usuários, com ênfase para a equidade de rede, isto é, tratamento de acesso à rede de internet de forma igualitária, sem limitação, discriminação, ou bloqueio ou cobrança de modo diferenciado dos serviços existentes na rede. Nessa perspectiva, vale apresentar 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. (BRASIL, 2014)

De acordo com a lei, os sistemas provedores de internet tinham por incumbência preservar o registro de suas atividades e de seus usuários, na ocasião da navegação em seus serviços e plataformas, para segundo Ribeiro (2020) assegurar a segurança aos indivíduos sejam eles físicos ou jurídicos, que usavam o ambiente virtual, colocando fim ao expressão de "terra sem lei".

Nessa nova circunstância, é importante ressaltar, o evento que ocorreu no ano 2015, o qual teve o WhatsApp como protagonista, que por mediante sua conduta protetiva com os dados de seus usuários, ficou sob vigilância judicial que deliberaram a exposição da comunicação destes para sustentarem as investigações criminais.

A justiça estabeleceu que em todo o território nacional fosse suspenso o serviço, diante da não permissão em conceder tais informações pela empresa responsável pelo aplicativo, (RIBEIRO, 2020).

Há pouco tempo, a Lei 14.155/2021 passou a vigorar, trazendo maior rigidez às penas dos delitos de estelionato e furto cometidos no meio digital, incluindo smartphones, tablets e computadores. Modifica a lei n° 2.828 do Código Penal, enrijecendo as punições, por exemplo, furto qualificado, invasão de dispositivo e estelionato praticados nesse ambiente, conectado ou não à internet (GANEM, 2017).

Para o delito de furto, veio a pena de reclusão de quatro a oito anos. Já a pena do delito de invasão de aparelhos informáticos abrangido no artigo 154-A do Código Penal, passando de três meses a um ano de detenção, para, de um quatro anos de detenção, acrescentando-se um a dois terços se da invasão for gerado prejuízo econômico.

No que se refere ao crime de estelionato, este está estabelecido detenção de quatro a oito anos e multa quando a vítima for enganada e fornecer suas informações por meio das redes sociais. No uso de servidor que se ache fora do país, delito praticado contra vulnerável ou idoso, a penalidade para estelionato também aumenta. Por último, as legislações aqui descritas e detalhadas surgiram com o intuito de ajustar bem como atualizar as leis que embaraçam a tipificação de tais delitos no ambiente virtual, desejando cumprir os preceitos que amparam o Direito Penal, tendo como exemplo da proibição da analogia e da legalidade com enfoque na proteção do usuário.

Mesmo assim, as mesmas são insuficientes, levando em conta a impunidade e a lacuna na legislação no enfrentamento aos crimes virtuais, carecendo urgentemente de mecanismos legais mais específicos e eficientes.

3 CONSIDERAÇÕES FINAIS

O estudo mostrou que hodiernamente os crimes virtuais vêm ganhando grande relevância no Brasil e no mundo, impactando consideravelmente a sociedade, infringindo os direitos fundamentais das pessoas, tendo em vista a simplicidade que os infratores encontram ao entrar nesse ambiente e a dificuldade em localizar os contraventores diante do anonimato e a celeridade na eliminação de provas.

A comprovação dos delitos virtuais é dificultosa e de complicada investigação, principalmente pela falta de legislações específicas e pela situação de anonimato dos infratores. Há necessidade de métodos mais específicos no procedimento das contingências desta infração; carência de qualificação e de capacitação profissionais; falta de registro de utilizadores que conectam no mundo virtual nos famigerados cybercafés e lan houses, a agilidade das informações relacionadas ao mundo virtual dificulta o acesso aos cibercriminosos, além do mais, estes delitos são constantemente praticados contra qualquer um, independente do local.

Todos esses motivos consequentemente colaboram para que os crimes fiquem impunes. A literatura indicou que a lei brasileira contra os crimes cibernéticos é dispersa, se tornando um imenso desafio no tocante a materialidade e tipificação desses delitos, tal como a condenação eficiente aos seus autores. Destaca-se dentre os crimes contra a honra e os de fraude, de estelionato, furto, chantagem, a apropriação indébita, a falsificação, falsa

identidade, de pornografia infantil, de pedofilia, etc., dispostos no Código Penal de 1940, sendo a pornografia infantil apontada como sendo um dos crimes mais cometidos.

Um progresso importante foi a posto pela Lei Federal n° 12.737/2012, "Lei Carolina Dieckmann", o "Marco Civil da Internet", por intermédio da promulgação da lei n.12.965/2014 e recentemente, a Lei 14.155/2021, a qual traz um maior rigor as penas dos crimes de estelionato e furto.

Por último, vale destacar os propósitos desse estudo, que mesmo diante a inserção e inovação nos dispositivos legais, ao descrevê-los, tornou-se possível demonstrar a carência de uma maior eficácia e resolutividade quanto a suas aplicabilidades, como também nos instrumentos de investigação delituosa, desta maneira atentando para a frequência que esses delitos vêm sendo praticados, visto que em decorrência da recente pandemia do corona vírus vivenciada pelo mundo decorrente, medidas restritivas de isolamento social, deixaram os pessoas mais dependentes dos dispositivos digitais e por consequência mais vulneráveis a esses crimes. Torna-se essência preencher as lacunas legislativas, reduzindo a impunidade, desta forma garantindo um ambiente de segurança aos usuários.

CYBERCRIMES: The Use of the Internet as a Tool for the Practice of Crimes and the Evolution of Brazilian Criminal Legislation in Combating Virtual Crimes

ABSTRACT:

What turns into a practical format for the practical environment, especially what is a strong feature of this practical format for the virtual environment, which is considered to be a practical environment for a practical environment and which is considered as practical consequences for the practical processes that are considered as practical consequences for the virtual media and that are considered as consequences legal tools can be considered in the judgment of such crimes. Thus, this study aimed to investigate the application of Brazilian legislation in the fight against cyber crimes. A bibliographic review methodology was used, a bibliographic review was carried out through virtual data BDTD, google0 search, based on articles, dissertations, between the years 10 to 222. greater study of legal instruments, in view of the regularity with these crimes that do not come as types, especially in the time that there was a current health crisis in the global character of the Coronavirus pandemic, as due to the determinations of social isolation, people became more dependent on virtual devices and this way more defined to these crimes. The study showed that regulatory gaps must be guaranteed and guaranteed to reduce impunity for users on the world wide web.

Keywords: Cyber Crimes. Brazilian Penal Code. Legislation.

REFERÊNCIAS

ABREU, Eduardo Franco. **Os entraves à repressão aos crimes cibernéticos**, 2014. Disponível em: <https://edufranco91.jusbrasil.com.br/artigos/142294529/os-entravesa-repressao-aos-crimes-ciberneticos>. Acesso em: 15.abr. 2022.

AJEJE, Gisele Ajeje de Carvalho. A **Persecução penal** nos Crime Cibernéticos e a Aplicabilidade da Dorma Penal. 2018. nº. t.folhas, 55. TCC, 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: 20. maio. 2022.

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-soba-egide-da-lei-12-737-2012>. Acesso em: 10. jun. 2022.

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: 25.mai.2022.

BRASIL. **Decreto-Lei 2.848, de 07 de dezembro de 1940.** Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL. **Lei nº 12.737, de 02 de dezembro de 2012.** (Lei Carolina Dieckmann).

BRASIL. **Lei 12.964, de 23 de abril de 2014.** (Marco Civil da Internet).

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-fekenews-e-a-falsa-sensacao-de-anonimato>. Acesso em: 15. jul. 2022.

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: 15. Jul. 2022.

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. **Revista Jus** Naviggandi, IISSN 1518-4862, Teresina, ano 23, nº. 5342, 15 fev. 2018. Disponível em: <https://jus.com.br/artigos/63549>. Acesso em: 12. jul. 2022.

MATSUYAMA, Keniche Guimarães; LIMA, JAA. Crimes cibernéticos: atipicidade dos delitos. 2017. Disponível em: <http://www.joaoademar.qlix.com.br/3cbpj.pdf>. Acesso em: 20.ago.2022.

MEDEIROS, Gutembergue Silva; UGALDE, Júlio César Rodrigues. **Crimes Cibernéticos: consideração** 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: 18. jun. 2022.

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

RAMOS, Eduardo Dulcetti. **Crimes Cibernéticos:** análise evolutiva e a Legislação Penal Brasileira. 2017. 64f. TCC Graduação em Curso de Direito, pela Universidade Federal do Rio de Jane iro, 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 delitos contra a honra. ANAIS CONGREGA MICISBN: **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: Violências Virtuais com Consequências Reais. In: **Congresso Internacional de Enfermagem**. 2017. Disponível em: <https://docplayer.com.br/68155614-Cyberbullying-violencia-virtual-com-consequencias-reais.html> . Acesso em: 04. set. 2022.

SANTOS, Izabella O.'Hara Alves dos; CARVALHO, Grasielle Borges Vieira de. Atuação da polícia civil de Sergipe nos crimes contra a honra cometidos 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: análise da **legislação vigente no cenário brasileiro contemporâneo**. 2017.Disponível em: <http://coral.ufsm.br/congressodireito/anais/2017/7-7.pdf >. Acesso em: 15. ago. 2022

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, 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: 15. ago. 2022.

SILVA, Kaique Rodrigues da; SILVA, Rubens Alves da. crimes cibernéticos: necessidade de atuais ferramentas de **investigações** 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 lei específica para os delitos 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. A psicopatia em sua dimensão virtual: um olhar acerca do fenômeno baleia azul. 2016. Disponível em: <https://vivianehenriques2602.jusbrasil.com.br/artigos/460463001/a-psicopatia-em-sua-dimensao-virtual> . Acesso em: 20 ago. 2022.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos (2a. edição): Ameaças e procedimentos de investigação**. Disponível em: https://books.google.com.br/books?id=iGY-AgAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false >. Acesso em: 20.jun.2022.

WINCK, D.; YUKUDA, F. Y. C.; SAVARIS, A.; HACK, E. A LEGISLAÇÃO E OS CYBERCRIMES. **Seminário de Iniciação Científica e Seminário Integrado de Ensino, Pesquisa e Extensão**, [S.l.], 2017. Disponível em: <https://periodicos.unoesc.edu.br/siepe/article/view/14188>. Acesso em: 10.set. 2022.