Revista JRG de Estudos Acadêmicos, Ano 6, Vol. VI, n.12, jan.-jul., 2023.

(CC BY 4.0) | ISSN 2595-1661

DOI: 10.5281/zenodo.7760710

ARK: https://n2t.net/ark:/57118/JRG.v6i12.520

A evolução do direito penal brasileiro relacionado aos crimescibernéticos[1]

The evolution of Brazilian criminal law related to cyber crimes

Recebido: 23/12/2022 | Aceito: 18/03/2023 | Publicado: 22/03/2023

Camila Cristina Gonzaga de Freitas[2]
https://orcid.org/0000-0003-2202-3695
http://lattes.cnpq.br/8179035153258645
Centro Universitário UniProcessus, DF, Brasil
E-mail: camilacristinafreitas@hotmail.com

Jonas Rodrigo Gonçalves[3]
https://orcid.org/0000-0003-4106-8071
http://lattes.cnpq.br/6904924103696696
Universidade Católica de Brasília – DF, Brasil
E-mail: professorjonas@gmail.com

Mateus Guimarães Torres[4]
https://orcid.org/0000-0002-4959-2858
http://lattes.cnpq.br/5886682363154988
Centro Universitário UniProcessus, DF, Brasil
E-mail: mateusgtorres@gmail.com

Resumo

O tema deste artigo é a evolução do Direito Penal brasileiro relacionado aos crimes cibernéticos. Investigou o seguinte problema: “Com o advento tecnológico digital, a sociedade possui segurança jurídica?”. Cogitou a seguinte hipótese: “as questões debatidas no tocante a seguridade jurídica, demonstram que a legislação evoluiu, oferecendo eficiência regulatória”. O objetivo geral é “explorar os avanços dos crimes cibernéticos no Direito Penal”. Os objetivos específicos são: “a importância do ordenamento jurídico Brasileiro contra os crimes cibernéticos”; “as lacunas relacionadas a Era digital”; “o estímulo de políticas preventivas”. Este trabalho é importante para um operador do Direito por demonstrar a aplicação do tipo penal no caso concreto; para a ciência, é relevante pela concretização da busca pelo conhecimento; e agrega à sociedade por transparecer a credibilidade do sistema jurídico. Trata-se de uma pesquisa qualitativa teórica com duração de seis meses.

Palavras-chave: Sociedade. Crimes cibernéticos. Evolução. Internet. Prevenção.

[1] Este artigo foi corrigido linguisticamente por Roberta dos Anjos Matos Resende.
[2] Graduanda em Direito pelo Centro Universitário Processus – UniProcessus – DF (Brasil).
[3] Doutor em Psicologia; Mestre em Direitos Humanos (Ciência Política e Políticas Públicas); Licenciado em Filosofia, em Sociologia e em Letras (Português e Inglês); Especialista em Direito Constitucional e Processo Constitucional, em Direito Administrativo, em Direito do Trabalho e Processo Trabalhista, entre outras especializações em Educação e Letras.
[4] Graduado em Direito; Especialista em Direito Tributário.

Abstract
The subject of this article is the evolution of Brazilian criminal law related to cyber crimes. The following problem was investigated: "With the advent of digital technology, does society have legal certainty?". The following hypothesis was considered: "the issues discussed regarding legal certainty demonstrate that the legislation has evolved, offering regulatory efficiency". The overall objective is to "explore advances in cybercrime in criminal law". The specific objectives are: "the importance of the Brazilian legal system against cyber crimes; "the gaps related to the digital age"; "the stimulus of preventive policies". This work is important for a law operator to demonstrate an application of the criminal type in the concrete case; for science, it is relevant for the search for knowledge; to society by showing the credibility of the aggregate legal system. This is a theoretical research lasting six months.

Keywords: *Society. Cyber crimes. Evolution. Internet. Prevention*

Introdução

O presente trabalho tem o intuito de analisar os crimes cibernéticos e sua punibilidade na legislação Brasileira, bem como o avanço legislativo, que surgiu com o advento do combate a esse novo tipo de crime. No qual busca objetivar e expor a importância do alcance punitivo que a nova legislação em vigor trouxe ao ordenamento jurídico pátrio.

Nossa sociedade atual não é a mesma de anos atrás, mesmo em nosso país de fronteiras continentais, a desigualdade impera de maneira avassaladora. Com o advento da tecnologia da informação, formada por computadores e principalmente pelo advento da *internet*, as fronteiras físicas se tornaram obsoletas, sendo necessário uma nova legislação para fazer frente aos novos crimes surgidos com a evolução da sociedade moderna (CRESPO, 2011, p. 23).

Este artigo se propõe a responder o seguinte problema: com o advento dos crimes tecnológicos digitais, a sociedade possui segurança jurídica? Com a chegada dos crimes da Era digital, a sociedade possui segurança jurídica, o ordenamento jurídico brasileiro como base reguladora de condutas, necessita de modificação conforme a sociedade evolui, trazendo segurança jurídica, portanto, o Direito consequentemente se molda conforme as necessidades surgem.

A racionalidade dos crimes no contexto tecnológico gera um aumento dos crimes tipificados como honra, ameaça, etc. No tocante aos crimes oriundos do sistema financeiros, como os crimes de estelionato, furto, extorsão e falsificação de documentos e também os crimes de natureza sexual, como o registro e divulgação de imagens pornograficas e o estupro. Portanto, tais condições agregam a importância de se observar detalhadamente o caso concreto, almejando a conjunturado tipo penal ao caso em questão (WENDT; JORGE, 2021, p. 41).

A hipótese levantada sobre a importância do problema foi em relação a omissão da segurança jurídica diante da Era digital. As questões omissivas debatidas, de seguridade normativa tecnológica, demonstram, em caráter significativo, que a legislação penal (BRASIL, 1940) evoluiu concomitante com a sociedade, oferecendo total eficiência regulatória.

É notório dizer que a nossa lei penal (BRASIL, 1940) está habilitada a punir condutas concretizadas dentro do campo tecnológico. No tocante aos crimes digitais onde pode surgir novas condutas a todo momento através dos meios tecnológicos, o Código Penal (BRASIL, 1940) possui expressa capacidade de punição em relação aos crimes oriundos do meio virtual, como: os crimes contra a honra, crimes

patrimoniais, crimes contra a pessoa, crimes econômicos, entre muitos outros (CRESPO, 2011, p. 169).

O objetivo geral desse trabalho é explorar, no âmbito penal, os respectivos avanços em decorrência aos crimes cibernéticos oriundos da Era digital. A nossa legislação, como norteadora da segurança jurídica brasileira, conseguiu após crescentes avanços suprir omissões procedentes dos crimes da esfera digital no Brasil.

A habilidade adaptativa da lei estabelece exclusiva proteção da estrutura jurídica, seguindo a lógica do equilíbrio jurídico onde atua frente a capacidade de produzir sanções altamente eficazes, a referida segurança é demasiadamente importante para a comunidade, no qual buscam a criação de leis que ajustem todas as matérias virtuais, especialmente a rede mundial de computadores (PINHEIRO, 2021, p. 19).

Os objetivos específicos deste trabalho se traduzem em enfatizar a importância do ordenamento jurídico Brasileiro, destarte, a rigorosa legislação penal (BRASIL, 1940) que evidentemente busca combater lacunas oriundas dos problemas evolutivos da sociedade. Neste diapasão, surge também como objetivo a necessidade de encaixar o tipo penal incriminador nas condutas oriundas da Era digital.

Consequentemente, as principais áreas do Direito, sendo ela publica ou privada, necessita urgentemente de recapitulação para que se encaixe nos novos padrões que compõe a sociedade, portanto, diante da referida situação, devemos nos atentar para que não somente a lei seja transformada, mas também todas as profissões do judiciário, visando efeitos que norteiam todo o ordenamento jurídico (ZANIOLO, 2007, p. 27).

Esta pesquisa contribui significativamente para a sociedade e para a compreensão do bem comum, serve para aqueles que possuem contato rotineiro com o ordenamento jurídico, como também aqueles que pretendem entender como o bem jurídico tutelado é resguardado pela lei. Nesta mesma linha de pensamento, entender como o Direito Penal alcança todos os que estão em risco na obscuridade da Era digital é de altíssima relevância, o tema em questão é sem duvidas a evidência de que as garantias jurisdicionais refletem no seio social.

A ciência sempre esteve presente desde os primórdios da humanidade, é por meio dela que a busca pelo conhecimento se concretiza, quando novas ferramentas surgem, o indivíduo produz maior capacidade de desenvolver novas sabedorias. Participar desse ciclo de conhecimento cria de maneira importante um grau de percepção para a sociedade, concretizando então uma progressão sobre a área abordada.

Acreditar no sistema que rege a segurança de todos funciona de modo a tranquilizar todos aqueles que precisam da sua proteção, é fundamental para confiar que o ordenamento jurídico brasileiro possui credibilidade. Garantir que a sociedade tome conhecimento sobre a sua segurança por meio de informações prestadas, sem dúvidas é ter a absoluta certeza de que as informações estão sendo prestadas de forma segura e eficiente.

O presente artigo trata de uma pesquisa teórica, bibliográfica, utilizando como base para fundamentação a utilização de livros de renomados autores, que demonstraram total domínio pela temática abordada. Para o reforço das ideias exploradas no presente artigo, foram utilizadas leis, mais precisamente as que se encontram no texto do Código Penal (BRASIL, 1940), no qual se encontravam expressamente designadas dentro das obras utilizadas.

Foram selecionados por mim para ser utilizado como fundamentação desse

artigo, 5 livros, utilizei a ferramenta conhecida como Google Acadêmico, através da referida ferramenta, fiz a busca de livros com ênfase no tema deste trabalho, utilizei algumas palavras chaves para obter resultado satisfatório em relação a pesquisa, foram utilizadas as seguintes palavras chaves através da plataforma Google Acadêmico: “cibernéticos, legislação, *internet*, crimes, sociedade”.

Como critério de exclusão das obras, foram escolhidos por mim obras de autores renomados na área de pesquisa, além de priorizar livros com ISBN. Está pesquisa de revisão de literatura possui prazo previsto de 6 meses. No primeiro mês foi realizado o levantamento de literatura e o referencial teórico, no segundo mês houve a elaboração do problema e hipótese, no terceiro mês foi efetuada a elaboração dos objetivos gerais e específicos, no quarto mês foram realizadas as elaborações justificativas e metodológicas, no quinto mês foi confeccionado o capitulo introdutivo, e no sexto mês foram terminados todos os detalhes finais.

Trata-se de uma pesquisa qualitativa teórica, no qual os autores buscaram embasamento por meio de aspectos subjetivos levantados através de históricos sociais. Buscou-se compreender os fenômenos sociais após observar as práticas adotadas pela sociedade durante anos, buscando compreender os fenômenos dentro do seu contexto natural.

A abordagem da pesquisa qualitativa teórica possui a função de buscar e observar como a sociedade se constrói e seus aspectos sobre suas vidas e rotina, busca refletir sobre os pontos fundamentais mais relevantes, todas as situações vividas e documentadas compondo um importante fato histórico para o estudo social, no qual esses fatos buscam debater e discutir as questões de maior relevância para o estudo do comportamento humano. Destarte, os métodos qualitativos são utilizados pelos pesquisadores para o exame das teorias e tipologias, por meio desses exames é encontrado ou é possível chegar próximo as respostas necessitadas (GIBBS, 2009, p.8).

A evolução do Direito Penal brasileiro relacionado aos crimes cibernéticos

A Era da informação ficou conhecida após o período da Era Industrial, posteriormente em 1980, embora o conhecimento tecnológico ter ganhado atenção no inicio do século XX, observando a década de 1970 fica concreto sobre quando surgiram as invenções do microprocessador, as redes computacionais e a fibra ótica do computador individual (CRESPO, 2011, p. 26).

Assim, como ocorre em processos evolutivos, com o advento da Era da Informação conhecida também como Terceira Onda, o inicio dos indícios surgiram ainda mesmo na Segunda Onda, trazendo grandes mecanismos, como o telefone, o cinema, o rádio e a televisão, no qual surgiu aproximadamente entre o final do século XIX e início do século XX. Esses meios de comunicação, como citado anteriormente, são atributos centrais da Terceira Onda, o seu crescimento ficou conhecido e centralizado ainda mesmo na Era industrial (PINHEIRO, 2021, p. 18)

Com o passar do tempo, milhares de pessoas optaram por utilizar os variados recursos tecnológicos, esses recursos passaram a fazer parte do cotidiano da sociedade, sendo um mecanismo facilitador na vida de muitos, onde as pessoas utilizavam e utilizam presentemente para buscar novos conhecimentos, fazer novas amizades, utilizam como ferramenta de relações comerciais, investimentos financeiros e para manter relacionamentos pessoais (WENDT; JORGE, 2021, p. 20).

Como citado anteriormente, surgiu de um grande período, que foi a chegada dos mecanismos evolutivos que tiveram início na fase da Era tecnológica. Antes do surgimento desse mecanismo facilitador, outros mecanismos evolutivos já haviam

surgido, facilitando cotidianamente a vida de muitas pessoas, a sociedade sempre visando a busca pela evolução tecnológica, procura se adaptar as novas mudanças que surgem a cada dia, com a chegada da nova Era tecnológica, problemas relacionados ao campo digital começaram a surgir, e foi nesse momento que as mudanças e adaptações precisaram se encaixar na nova realidade, foi preciso que as novas mudanças acompanhassem a velocidade digital trazendo segurança e proteção aos milhares de usuários, de modo que a sociedade pode se tornar vítima fácil para os criminosos cibernéticos.

Geralmente, muitos acreditam que pelo fato de estarem atrás de um computador possuem livre arbítrio, criando uma certa coragem para praticar condutas inadmissíveis, a maioria dessas pessoas criam perfis falsos, acreditando que jamais serão identificadas, tirando proveito da situação, usam a *internet* para praticar ações negativas, mesmo sabendo que a *internet* deveria ser utilizada como uma ferramenta em prol do bem comum, porém os criminosos utilizam as redes para benefício próprio causando prejuízos para muitos (BARRETO; BRASIL, 2016, p. 29).

Mesmo com a chegada positiva da Era digital, precisamos mencionar os impactos negativos que acompanharam essa nova realidade, sendo uma situação completamente nova, a sociedade ainda não estava preparada em para a proteção virtual, o que gera muitos prejuízos e transtornos para a sociedade, a prática de crimes virtuais se tornou cada vez mais frequente, surgiram então os crimes cibernéticos, que se caracteriza pela prática de delitos cometidos dentro do ambiente virtual, afirma-se atualmente que a prática desses delitos crescem a cada dia, devido ao aumento de usuários e pela facilidade que as inovações tecnológicas trouxeram para a sociedade, que gerou fácil acesso para todos (WENDT, JORGE, 2021, p. 20).

A nova Era trouxe, sem sombra de dúvida, muitos benefícios para a sociedade, porém observando o outro lado, também trouxe diversos malefícios, surgiu também a Era da desinformação, no qual se define por um fenômeno onde todos podem expressar o que pensam, sem respeitar as opiniões alheias, criando um atrito social imenso. Virou muito comuns assuntos relacionados a algumas doenças psicológicas devido aovício em redes virtuais, como o resultado esses usuários precisaram de intervenção terapêutica e médica, essas pessoas ficavam expostas mais de 35 horas em frente aos computadores sem interrupções (CRESPO, 2011, p. 27).

Não restam dúvidas de que a nova Era trouxe, além de muitos benefícios, vários malefícios. O anonimato é um problema resultante dos inúmeros malefícios da Era digital, não podemos ignorar o fato de que todos aqueles que cometem crimes no ambiente digital estão em anonimato, atingindo a todos nós, ou seja, em frente a um computador há uma pessoa que está realizando atividades incapazes de identificação, isso quando realmente é uma pessoa física, atualmente com a inovação tecnológica existem programas que realizam essas atividades criminosas.

Oriunda do desenvolvimento tecnológico, a *internet* é o principal meio responsável pelas transformações que surgiram nos últimos tempos, os mecanismos tecnológicos como o telefone, radio, computador e afins, preparou o centro que ligou as redes uma na outra, criando a base para integrar o alcance mundial entre rede e pessoas, independente de onde estiver, pessoas estão conectadas massivamente (ZANIOLO, 2007, p. 27).

Os avanços ocorreram de forma tão espantosa, a ponto de impressionar toda a sociedade, impressionado até mesmo estudiosos em questão, esses avanços trouxeram uma enorme expansão tecnológica, atualmente com o advento da *internet*, as pessoas estão mais próximas pelo fato de estarem conectadas por telas, porém, esses avanços trouxeram o aumento de crimes através das redes digitais, conforme

esses crimes avançam, o ordenamento jurídico enfrenta novos desafios, esses desafios incluem muitas vezes situações jamais vistas. Neste diapasão, é preciso se valer da interpretação doutrinaria e jurisprudencial para resolução da lide (BARRETO; BRASIL, 2016, p. 10).

Atualmente, sentimos o impacto que a realidade da tecnologia digital trouxe, os desafios interpostos incluem cada vez mais maneiras de definir os limites perante aos usuários da *internet*, tudo isso deve acontecer na mesma velocidade em que os indivíduos esperam receber respostas, a Era digital trouxe uma infinidade de sociedades virtuais, que unificou vários interesses, sejam pessoais, empresariais e institucionais em muitos lugares do mundo (PINHEIRO, 2021, p. 18).

Ante o exposto, vimos que a legislação precisa a todo momento estar se modificando conforme o surgimento de novas demandas, essa importância ocorre pelo fato de que a sociedade precisa sentir o escopo da segurança jurídica, essa proteção precisa estar no cotidiano da sociedade para poder agir diante da ação de pessoas mal intencionadas, ou seja, agir contra criminosos que utilizam o meio digital para tirar proveito. O fato exposto chama a atenção para questões preventivas de controle, onde deveria haver investimento em políticas informativas para a população que ainda enfrenta uma grande desinformação a respeito da proteção digital.

A sociedade precisa refletir que a lei penal (BRASIL,1940) não consegue alcançar e agir preventivamente elucidando todos os casos existes. É preciso que sejam operadas formas de proteção para que os usuários se conscientizem dos perigos que a *internet* proporciona, pois atualmente a rede mundial de computadores oferece informações gratuitas e das mais variadas (CRESPO, 2011, p.163).

Dentro do contexto virtual, todos possuem o livro arbítrio de se relacionar umas com as outras, usar a *internet* como ferramenta de trabalho ou como diversão, porém infelizmente a sociedade esta a mercê de criminosos em ambientes digitais, onde os criminosos estão cada vez mais especializado em condutas ilícitas. Portanto, é importante enfatizar as informações relacionadas com a segurança tecnológica, criando uma base eficiente para os usuários utilizarem as redes com prevenção, tornando a *internet* uma opção segura e eficaz para a utilização de todos, atualmente a *internet* dispõe de ferramentas acessíveis e complexas para prevenção de fraudes, furtos de identidade e invasões financeiras (BARRETO; BRASIL, 2016, p.18).

Em outras palavras, a capacitação de profissionais adequados gera um grande significado em termos de prevenção sobre os relacionados crimes cibernéticos, essa qualificação é extremamente importante pelo fato de existir atualmente um déficit gigantesco em relação a educação tecnológica da sociedade diante da *internet* (WENDT; JORGE, 2021, p. 305).

O Estado busca acompanhar os passos evolutivos da Era digital e todas as ligações judiciárias que compõe esse contexto social. O Estado atua de forma significativa na informação e na prevenção dos usuários, evitando o número crescente de vítimas (BARRETO; BRASIL, 2016, p. 219).

Atualmente, as informações são facilmente acessíveis, não restam dúvidas de que a *internet* trouxe uma infinidade de ferramentas informativas para atuar como fonte de prevenção para a sociedade, além do mais, as agências bancarias disponibilizam a todo momento vários meios de informação para enfrentar e combater a criminalidade nas plataformas financeiras, devido ao fato dos criminosos estarem cada vez mais preparados, utilizando táticas para enganar principalmente o público mais idoso. Diante disto, as leis precisam estar preparadas a todo instante para incriminar essas condutas, as práticas ilícitas, denominadas crimes cibernéticos, são de grande complexidade dentro do campo tecnológico. A justiça busca a todo instante

identificar e punir os responsáveis pelas ações criminosas. Destarte, serão analisadas posteriormente as peculiaridades denominadas como crime cibernético.

Com o advento do crescimento tecnológico da informática, ocorreu uma grande evolução da comunicação voltada para as relações sociais, devido a esse crescimento surgiram novos conceitos sobre bens jurídicos, criando ideias conceituais sobre os crimes cibernéticos (CRESPO, 2011, p. 57).

Os crimes cibernéticos estão dentro do escopo tecnológico, crimes que são cometidos através de computadores, *internet* e caixas eletrônicos. São uma espécie de crime meio, o que impressiona é a capacidade e a maneira como os crimes cibernéticos se tornam cada vez mais inovadores, de forma que os criminosos estão sempre modificando a forma como praticam o ato ilícito, apesar de acontecerem na *internet*, os crimes cibernéticos alcançam resultados fora do mundo virtual (BARRETO; BRASIL, 2016, p. 36).

No Brasil, os crimes cibernéticos são de extrema preocupação, levando em consideração que as atividades criminosas dentro da realidade virtual possuem lucros gigantescos, a nossa legislação atual tenta a toda instante combater as lacunas que se desenvolvem com as novas ameaças, tendo em vista que as quadrilhas estão cada vez mais preparadas para lidar com esse tipo de situação, criando maneiras de driblar as barreiras de segurança criadas para a proteção dos cidadãos (BARRETO; BRASIL, 2016, p. 36).

As ações incriminadores realizadas através de computadores ou dispositivos móveis podem ser classificadas como crimes cibernéticos ou ações prejudiciais atípicas. Os crimes cibernéticos possuem duas espécies: os crimes cibernéticos abertos que consistem em crimes praticados e não praticados por meio informático, e os crimes exclusivamente cibernéticos que são os crimes que dependem do meio informático para serem definidos como crime (WENDT; JORGE, 2021,p. 39).

Com a facilidade tecnológica, muitas pessoas utilizam a *internet* para favorecimento próprio, a grande maioria possui uma rotina extremamente corrida, qualquer mecanismo de agilidade no cotidiano é muito favorável, porém os criminosos estão a todo momento encontrando formas de driblar a sociedade, utilizando táticas de proveito sobre cidadãos inocentes e completamente despretensiosos. Consumando assim vários delitos através da rede mundial decomputadores.

A sociedade acredita que os crimes cibernéticos são delitos que ocorrem facilmente na *internet*, ou seja, que no ambiente digital pode ser feito o que quiser como quiser, há lugares em que a obscuridade é imperiosa. Realmente, essas crenças só são estimuladas pelo fato de a sociedade sentir que os agentes criminosos não são barrados. A norma penal (BRASIL,1940) é extremamente relevante para tipificar condutas dentro do contexto virtual, caso isso não ocorra, os crimes aumentarão e a sociedade que utiliza a *internet* como forma de sustento digno e honesto encontrará dificuldades para seguir adiante (PINHEIRO, 2021, p. 134).

Desse modo, o Direito Penal encontrou novas realidades em seu caminho, essa nova realidade se resume em novas práticas delitivas, essas ações merecem total atenção, pelo fato de serem condutas extremamente danosas (CRESPO, 2011, p.48). Os criminosos utilizam várias técnicas para enganar vítima, oferecendo recursos e fazendo as vítimas acreditarem em suas farsas, os criminosos agem de maneira tãopropulsora, ludibriando as vítimas para que ofereçam informações pessoais, concretizando a vontade dos criminosos (WENDT; JORGE, 2021, p. 41).

Atualmente, o que antes só era retratado em filmes passou a fazer parte do contexto real, pela facilidade que a *internet* oferece, qualquer cidadão pode ter acesso aos mais diversos materiais criminosos, essas ferramentas se tornaram tão fáceis que

a própria rede mundial de computadores ensina técnicas criminosas, que consistem em desmantelamento de senhas e identidades, fraudes em sistemas, acesso a muitas drogas, armas, contato com assassinos de aluguel, pornografia infantil, dentre muitas outras (BARRETO; BRASIL,2016, p. 43).

Na *internet* há distinção entre os chamados *hackers* e *crackers*, o primeiro possui elevado entendimento sobre computadores e suas redes, buscando utilizar seus conhecimentos como forma de apoio para outras pessoas, já o segundo, seria totalmente o oposto, utiliza todo o conhecimento para práticas criminosas e desrespeitosas (BARRETO; BRASIL, 2016, p. 44).

Não restam dúvidas de que os criminosos estão cada vez mais preparados para a prática de crimes na *internet*. São facilmente fornecidas formas para a associação de esquemas criminosos. Atualmente, a maior preocupação se baseia em maneiras de combater os crimes praticados no contexto virtual, a facilidade que os criminosos possuem para falsificar as suas identificações tem gerado uma emblemática desvantagem para a polícia identificar esses delinquentes, o fato de esses infratores estarem o tempo todo mudando de localidade é um fator que atrapalha as investigações. São necessários policiais habilitados e preparados para lidar com essas situações, bem como ferramentas táticas para identificar os cibercriminosos que atuam de diversas formas prejudicando a sociedade.

No período de investigação dos crimes cibernéticos é possível observar alguns requisitos que ajudam na identificação dos criminosos, essas análises buscam localizar o dispositivo utilizado nos crimes para identificar o delinquente, a busca consiste na verificação de informações e detalhes repassados pelas vítimas, ligando os pontos fáticos ocorridos no contexto virtual. São repassadas algumas instruções para que a vítima preserve todas as provas que comprovam o crime, os meios de prova coletados são de extrema importância para as evidências do crime, os materiais e provas fornecidos pela vítima serão direcionados para policia. A próxima fase consiste na formalidade do ato em relatório expedido pelas autoridades policiais, com todas as provas reunidas. Após o último ato é solicitado aos fornecedores de conexão um requerimento de dados que favoreça a investigação, depois de repassados os dados, é solicitada ao Poder Judiciário a autorização judicial para a quebra de sigilo de dados e o acesso de informações(WENDT; JORGE, 2021, p. 74).

Os chamados crimes modernos não se restringem somente a um meio de utilização, como os computadores ou a *internet*, pois atualmente há várias formas de passagem para consumar os delitos cibernéticos, como os crimes contra a fraude bancária que são cometidos através de caixas eletrônicos, essas formas devem ser cuidadosamente analisadas e discutidas (ZANIOLO, 2007, p. 33).

Nas conexões pagas, a identificação do endereço eletrônico dos usuários é mais fácil, após identificados, ocorre uma restrição de todos os dados em decorrência das práticas delitivas, essa facilidade ocorre pelo pagamento dos clientes que contratam o serviço de *internet*, que fazem o pagamento mensal para utilizar essa conexão, muitas vezes debitam as parcelas com cartões de crédito ou débito, ou seja, a maioria dessas informações constadas no banco de dados das operadoras de crédito são seguras e auxiliam na investigação (PINHEIRO, 2021, p. 134).

A investigação dos crimes cibernéticos é feita com indícios que permitem verificar a autoria e materialidade do delito, observamos acima que não é uma tarefa simplificada, mas árdua e perspicaz, o combate aos crimes dentro do contexto tecnológico ocorre a todo o momento, as autoridades policiais correm contra o tempo para elucidar os delitos virtuais, uma das ferramentas de apoio para ajudar a combater os crimes cibernéticos é a criação do inquérito policial eletrônico, ágil no auxilio de

coleta de provas e de altíssima importância para elucidar esses crimes. Diariamente as delegacias policiais recebem inúmeras denúncias, o aumenta o número de inquéritos relacionados aos crimes digitais, resultando em um acúmulo de tarefas para os agentes de segurança pública. Destarte, a criação de delegacias de crimes virtuais atua fortemente na apuração dos delitos de autoria cibercriminosa. Além do mais, a infinidade de crimes cometidos dentro do contexto tecnológico é infelizmente uma realidade longe de terminar, tendo em vista que além dos crimes cometidos dentro da rede mundial de computadores, há algumas zonas de navegação nas quais a polícia encontra extrema dificuldade para elucidar crimes, pela dificuldade de identificação dos motores de rede.

Devido ao favorecimento da evolução da rede mundial de computadores, o número de usuários tende a crescer mais. Portanto, com o crescente acesso, o número de crimes relacionados ao campo de digital tem acompanhado em ritmo crescente as estatísticas. É possível observar o crescimento de novas ameaças, um exemplo disso foi a pandemia do Coronavírus, a sociedade mudou completamente sua rotina, demonstrando que a *internet* se tornou parte do cotidiano de muitas pessoas. Porém, ao mesmo tempo os criminosos passaram a utilizar cada vez mais as redes para concretizar suas ações (WENDT; JORGE, 2021, p. 297).

A engenharia social era conhecida há muitos anos atrás como fraude ou falsificação fraudulenta no Direito Penal. Atualmente, a engenharia social é compreendida como uma ferramenta que age enganando os usuários das redes com falsas pretensões para que repassem informações pessoais concretizando a vontade dos criminosos. Esse mecanismo, chamado engenharia social, é uma ponte entre criminosos e usuários. Essa ponte não é necessariamente um meio tecnológico, mas qualquer ferramenta de comunicação (CRESPO, 2011, p. 85).

Com base em levantamento de dados, no Brasil os crimes mais tradicionais são os crimes de estelionato e pornografia infantil. Uma forma de expandir rapidamente vírus e outros materiais ilegais são os *e-mails*, um mecanismo facilitador para acabar com a expansão de *e-mails* não identificados seria a obrigação dos usuários em identificar suas contas usando imagens reais que comprovem a propriedade do e-mail. Basicamente, seria a mesma forma de identificação que as agencias bancárias utilizam com os seus clientes, isso facilitaria demasiadamente a questão da segurança (PINHEIRO, 2021, p. 134).

A principal polêmica é que a rede mundial de computadores avança de forma surreal, a sociedade, em termos evolutivos, busca evoluir, mas grande parte das pessoas desconhece o poder que os criminosos possuem para enganar suas vítimas. Atualmente, um dos maiores empecilhos que a segurança pública enfrenta para incriminar condutas de cibercrimes é a produção de provas de condutas dentro do contexto virtual.

Um dos maiores empecilhos encontrados no caminho da investigação é a produção de provas, pelo fato de ser um instrumento comprobatório de altíssima importância para a condenação dos ciber-criminosos (ZANIOLO, 2007, p. 34). Tratando de termos evolutivos, alguns crimes estão sendo elucidados por meio de análises feitas pelos computadores dos criminosos, provas mais simples evidenciam a ligação de criminosos com os crimes de pedofilia, fraudes bancárias e crime organizado. Isso é um marco revolucionário, pelo fato de conseguir apurar de forma significativa a tipicidade desses delitos, colhendo evidências de maneira ágil e eficaz. No presente, o documento eletrônico é um importante meio para constituir prova (ZANIOLO, 2007, p. 37).

Os meios de provas de natureza moral e legal, que sejam eficazes na

investigação dos crimes cibernéticos, podem ser empregados para ajudar na busca real dos fatos (ZANIOLO, 2007, p.35).

Fatos probatórios são relevantes para punir os criminosos virtuais, muitos agentes de segurança pública encontram dificuldades na resolução dos cibercrimes, isso acontece pelo fato de o governo não investir em treinamento qualificado na preparação desses profissionais, ou seja, há alguns empecilhos voltados para a questão da preparação profissional dos agentes de segurança pública. Os criminosos acreditam que a *internet* oferece uma infinidade de vantagens, acreditam que por aplicarem golpes em suas vítimas a distância, a punição jamais chegará até eles, a segurança pública com o dever de perseguição desses criminosos, enfrenta diariamente a missão de garantir segurança para a sociedade.

As autoridades de segurança possuem o dever de vigilância, porém a dificuldade aumenta em crimes virtuais pelo fato de ainda existir uma grande dificuldade para demonstrar a culpabilidade do agente que praticou aconduta, na fase de perseguição do infrator, a questão probatória se revela ao fato de provar se o usuário do endereço eletrônico é o da conduta, partindo do pressuposto de que muitas vezes o endereço eletrônico utilizado não está vinculado apenas a uma pessoa, prevalecendo em muitos casos o princípio do *in dúbio pro réu* (PINHEIRO, 2021, p. 25).

A realidade da segurança pública em relação aos crimes praticados dentro do contexto virtual tem demonstrado que ao diminuir a exibição dos suspeitos ocorre a abertura de vias para continuar a prática dos delitos. Possivelmente, devido ao crime ocorrer em situações em que a vitima e o criminoso estão em locais distintos, que de certa forma instiga reincidentes criminosos que praticavam assaltos pessoalmente, hoje passarem a praticar crimes virtuais (BARRETO;BRASIL, 2016, p. 22).

Sobre a criação de delegacias que atuam contra os crimes cibernéticos, somente contam com instalações em capitais, porém constituem um importante auxílio para a justiça, mesmo com o avanço, as delegacias operam de forma inferior ao que se espera (ZANIOLO, 2007, p. 46).

Ainda há um óbice muito grande nas investigações dos cibercrimes, como mencionado, os criminosos encontram brechas ao seu favor, os crimes que ocorrem dentro do contexto virtual inovamcriando uma tarefa árdua para as autoridades de segurança pública. A legislação corre contra o tempo para garantir que os crimes dentro do contexto virtual tenham punição, porém o combate aos crimes digitais depende exclusivamente de condutas eficientes dos órgãos de segurança pública.

Diante de todos os problemas que têm surgido, a infinidade de maneiras que os criminosos praticam os delitos chama a atenção para as autoridades judiciárias que procuram formas para enfrentar esses desafios. O sistema jurídico Brasileiro atua n esses problemas, tratando as lacunas que surgem a todo momento, um dos maiores problemas é em relação ao departamento policial de investigação cibercriminosa, tendo em vista que a preparação e o treinamento dos agentes ainda são tratados de forma omissa em nosso país (WENDT; JORGE, 2021, p. 297).

Os ilícitos ocorridos dentro do ambiente virtual devem ser conceituados de maneira distinta de crimes virtuais, pelo fato de não constituirem somente um ilícito da informática, mas verdadeiros riscos para a sociedade, pois atuam no contexto real (CRESPO, 2011, p. 166).

Ficou evidente que os cibercriminosos encontram maneiras de inovar na prática de seus crimes. Prever qual será a próxima artimanha utilizada pelos criminosos é algo que chama a atenção das autoridades de segurança, pois é preciso adotar técnicas de inovação nos setores de controle e prevenção. Tais técnicas precisam ser

voltadas para a melhoria dos sistemas informáticos que são utilizados como ferramentas pelos agentes de segurança e prevenção. É preciso encontrar formas de qualificar mais os servidores que atuam no combate dos cibercrimes.

Pensando na forma de melhorar e qualificar mais os profissionais dos órgãos jurisdicionais, o governo precisa ter formas de capacitar os servidores para que sejam aprimoradas técnicas eficazes para o enfrentamento dos cibercriminosos. Entretanto, além da capacitação e do aprimoramento que devem ser aplicados nos cargos, os órgãos devem investir em políticas de prevenção e informação (WENDT;JORGE, 2021, p. 316).

Segundo Arnaud (1999, p.3), a globalização atua diretamente no Direito, e atualmente, com as mudanças sociais, o Poder Judiciário enfrenta vários problemas de omissão. Destarte, por meio da globalização, os juristas se baseiam na interpretação doutrinária para alcançar o suprimento de lacunas, conforme a evolução social cresce, crises relacionadas ao Direito acompanham esse crescimento (ZANIOLO, 2007, p. 26).

Não restam dúvidas de que as leis precisam ser adaptadas conforme a realidade tecnológica, em especial a *internet*. Sabemos que é considerada um grande marco social, pelo fato de ter trazido inúmeros benefícios para a sociedade. A rapidez disseminada em informações trouxe alguns problemas, que podemos classificar como atividades ilícitas. A lei precisa alcançar essas tipologias (ZANIOLO, 2007, p. 33).

As políticas públicas voltadas ao combate e prevenção dos crimes cibernéticos são de extrema importância, o enfrentamento desse caótico problema está longe de ter fim, porem é necessário que todos os mecanismos para combater os cibercrimes sejam usados em conjunto. Destarte, a lei penal (BRASIL, 1940) é de extrema relevância para punir os agentes criminosos.

A lei penal (BRASIL, 1940), como *última ratio*, busca penalizar os ilícitos sociais mais importantes, conforme a mutação social ocorre, o Direito Penal busca se transformar junto com a sociedade. Portanto, como ocorre genericamente, a lei penal (BRASIL, 1940) deve tipificar os delitos que surgem da rede mundial de computadores (BARRETO; BRASIL, 2016, p. 11).

Assim, como acontece em vários países, no Brasil não seria diferente, o sistema jurídico está em crescente evolução, isso ocorre devido aos avanços da sociedade. Portanto, surgem situações e comportamentos novos, obrigabdo a sociedade a se adaptar conformes novas mudanças surgem na sociedade e em todo o ordenamento jurídico. Diante disso, observamos o surgimento de novas leis para a *internet*, houve alteração na Lei penal (BRASIL, 1940) para crimes contra a Administração Pública, teve alteração no Código de Processo Civil(BRASIL, 2015) nas assinaturas digitais e uma das alterações mais importantes foi a mudança no Estatuto da Criança e do Adolescente (BRASIL, 1990) acerca do crime de pedofilia, e a criação de previsões legais para *cyber* cafés e *lan houses* (PINHEIRO, 2021, p. 137).

Há crimes que estão disciplinadas no texto penal (BRASIL, 1940), que agem diretamente contra os bens jurídicos, porém existem outros crimes que agem diretamente contra as informações das ferramentas de rede, estes afetam dados de programas e outros. São tipicamente detalhados e a legislação ainda definiu uma punição para eles (CRESPO, 2011, p. 169).

A lei, como a principal fonte de controle social, busca alcançar a segurança social, e tratando dos crimes cibernéticos não seria diferente, conforme as evoluções sociais surgem, o ordenamento jurídico corre contra o tempo para garantir a proteção de todos. Nos casos de omissão, o juíz deverá se valer da interpretação para a resolução concreta da lide.

Com a chegada da nova realidade tecnológica, surge a necessidade de estabelecer novos princípios jurídicos. Diante dessa necessidade, deve-se repensar os valores que os princípios do Direito e as leis trouxeram, portanto,é preciso objetivar a interpretação da norma jurídica em relação as novas condutas sociais (PINHEIRO, 2021, p. 143).

Atualmente, quando não existentes tipificação penal para determinado ato ilícito, deve se valer da interpretação para suprimir as lacunas existentes, caso ela se aplique aos casos já dispostos no ordenamento jurídico (ZANIOLO, 2007, p. 37).

A atualização legislativa é extremamente importante para encaixar o tipo penal na lei, segundo Klaus Tiedemann, “os ilícitos informáticos devem ser analisados conjuntamente com exemplos de outros países para que se siga as praticas observadas, caso isso não ocorra, a nossa legislação correrá sérios riscos”. Destarte, observando a elaboração das nossas leis e para poder criar uma base fortalecida, é de suma importância observar a forma como outros países e órgãos influentes tratam a questão dos crimes cibernéticos pelo mundo (CRESPO, 2011, p. 25).

Entretanto, nosso país conseguiu conquistar uma evolução imensa na legislação penal (BRASIL, 1940) aplicada aos crimes do contexto digital, foi achegada da Lei 12.737/2012 (BRASIL, 2012) que ficou conhecida pelo projeto Carolina Dieckmann, e também com a chegada do Marco Civil da *Internet* (PINHEIRO,2021, p. 135).

Como citado, ocorreu a evolução de um grande marco no enfrentamento aos crimes cibernéticos, foi a chegada da lei que tipificou os crimes de invasão de natureza cibernética. No ano de 2021, foi sancionada a Lei 14.155/2021 (BRASIL, 2021) que possui penas mais severas contra crimes cibernéticos, como fraude, furto e o tão temido estelionato, todos praticados com o uso de celulares ou computadores, a nova lei alterou o antigo texto, agravando as penas de furto qualificado, invasão de dispositivo informático e crimes de estelionato digital. A nova lei demonstrou que os crimes ocorridos dentro do contexto virtual são levados a sério no Brasil, a nova redação demonstra que as penas para quem invade um dispositivo informático alheio serão de um a quatro anos e multa, a pena poderá aumentar de um a dois terços se for comprovado que a vitima sofreu um prejuízo econômico, para quem cometia esse crime anteriormente a pena era de três meses a um ano de detenção e multa. Já para o crime de furto qualificado, a pena será de quatro a oito anos de reclusão cumulado com multa, porém se a vitima for idosa ou vulnerável, a pena aumentará para um terço até o dobro. A grande conquista foi em relação ao crime de estelionato, a pena teve alteração de quatro a oito anos de reclusão e multa, a consumação do delito acontece quando o crime ocorrer dentro das redes sociais e a vitima tiver repassado informações por meio de seus perfis sociais, antes da nova lei o estelionatário só recebia a punição de um a cinco anos de reclusão e multa. Ambos os crimes, de estelionato e furto qualificado, se praticados com servidor informático fora do território nacional terão a pena aumentada, assim como no crime de furto qualificado, a pena do crime de estelionato também será aumentada contra aquele que praticar o crime em idosos ou pessoas vulneráveis. Com esse marco revolucionário, nosso país avança no caminho certo para combater crimes cibernéticos, tendo em vista que o Brasil possuía uma legislação pacata na punição dos crimes informáticos. A legislação acabava considerando os crimes cibernéticos como crimes menorores, nos quais as penas eram, na maioria dos casos, substituídas por outras mais brandas.

Segundo Begalli (2002, p.160), a justiça atual necessita diariamente de tecnologia, como sua fonte primária, a *internet* é um dos principais instrumentos no tocante a sua conservação (ZANIOLO, 2007, p. 27).

O Código Penal (BRASIL, 1940) altamente eficaz no sentido de que consegue alcançar a grande maioria dos tipos de crimes cibernéticos, principalmente os crimes que causam problemas para os usuários, mas existem alguns casos específicos que não estão previstos no texto legal, ou seja, o crime em questão não possui previsão expressa. Portanto, muitas vezes ocorre a discussão de que determinadas condutas dentro do contexto virtual não geram crime, para desmistificar essa situação foi criado o projeto de Lei n.° 84/1999. pelo deputado Luiz Piauhylino. Aprovado em 2003 pela Câmera Federal, o projeto só teve a aprovação do Senado em 2008, acabou retornando para a Câmara Federal e foi definitivamente aprovado em 2012. A aprovação do projeto teve um marco revolucionário no tocante aos crimes cibernéticos, visando a determinação de que os agentes de segurança pública podem agir estruturando profissionais capazes de combater diretamente práticas delituosas no contexto virtual, o outro artigo aprovado pelo projeto de lei prevê que em crimes de racismo, quando ocorridos na *internet*, o juíz pode determinar, após parecer do Ministério Público e também a pedido do mesmo se for o caso, o desmantelamento de informações dos dispositivos relacionados ao usuário que cometeu o crime. Devendo o criminoso interromper suas atividades dentro da *internet* (WENDT; JORGE, 2021, p. 310).

Atualmente, é preciso observar todas as informações relevantes na criação de lei para a rede mundial de computadores, consideravelmente a criação de leis para os crimes cibernéticos, não menos importante, a criação de leis civis que sejam ligadas a privacidade dos usuários. Carecemos que sejam quebrados paradigmas, existe um desafio gigantesco sobre a legislação voltada para a Era digital, existem questões para ser resolvidas, e a necessidade de resolver questões relevantes como o furto, disciplinado no Artigo 155 do Código Penal(BRASIL, 1940) ou seja, em termos de uso virtual, copiar e colar determinado texto estaria tipificado como furto, caso não seja exposto a referência. Assim, é notório que nenhuma legislação é dotada de perfeição, é preciso encontrar criminosos que enganam e se valem da boa fé da sociedade, é preciso aplicar-lhes a punição cabível, mas é preciso ainda considerar a identificação de um usuário inocente que não teve nenhuma intenção de repassar algum arquivo contaminado. O presente enseja desafios constantes, deve-se pensar diariamente sobre as formas de combater e alcançar os melhores resultados para que os nossos filhos e netos se sintam protegidos e estabilizados ao utilizar a rede mundial de computadores. O Poder Judiciário possui várias demandas diárias, encontrar formas de resolver os conflitos de maneira conciliatória e arbitrária resolveria muitos problemas. O maior óbice seria a proteção dos usuários, ou seja, estamos expostos a várias ameaças virtuais que no contexto relevante poderiam causar conflitos nacionais e internacionais, destarte, a sociedade não retrocede. Temos a função e o dever de garantir a proteção a todos, trabalhando diariamente (PINHEIRO, 2021, p. 137).

Portanto, como demonstrado, os aspectos jurídicos de informáticanão são mais contextos obscuros, já possuem respaldos há longos períodos, merecem que sejam enaltecidos cada vez mais (CRESPO, 2011, p. 42).

A sociedade acredita que o nosso país não está preparado juridicamente para lidar com os crimes que ocorrem no contexto virtual, podemos verificar que o óbice não se encontra diretamente nas leis, mas em relação ao combate e ao enfrentamento dos crimes cibernéticos, a nossa legislação é completamente eficaz, conforme a sociedade avança, a legislação busca se moldar diretamente aos crimes que ocorrem no escopo social. A sociedade não é a mesma de antigamente, a tecnologia passou a fazer parte do cotidiano das pessoas e será assim sucessivamente.

Considerações Finais

Buscou-se explorar os respectivos avanços no Direito Penal brasileiro em relação aos crimes cibernéticos. Foram abordados tópicos de caráter extremamente relevantes para o Direito Penal e toda a sociedade, a legislaçãopenal (BRASIL, 1940) conseguiu alcançar os problemas oriundos da Era digital, no qual se considerou um grande marco histórico para o Direito Penal brasileiro relacionado aos crimes cibernéticos.

A sociedade conseguiu conquistar segurança jurídica em relação a proteção dos crimes cibernéticos? Em termos evolutivos, a legislação penal (BRASIL 1940) conseguiu evoluir de maneira significativa, acompanhando a sociedade em termos evolutivos, para que nenhuma ameaça oriunda da Era digital passe impune.

O Direito Penal avançou com os processos evolutivos da sociedade, alcançou significativamente regulações para os denominados crimes digitais. Foi enfatizada a importância do Código Penal (BRASIL, 1940) brasileiro no tocante ao combate dos problemas que surgem com os processos evolutivos da humanidade.

Esta pesquisa demonstrou a importância do ordenamento jurídico, pois serviu de auxilio para todos compreenderem como o Direito Penal tratou de assegurar proteção para aqueles que estavam expostos a Era digital. Esta pesquisa, para a ciência, demonstrou que a sociedade buscou novos conhecimento a respeito das ferramentas virtuais, desenvolveu sabedorias e prevenção, o ordenamento jurídico garantiu eficiência proteção para todos os que buscaram acreditar na segurança que a lei penal (BRASIL, 1940) trouxe.

Chegou-se as seguintes conclusões: o ordenamento jurídico brasileiro, especificamente o Código Penal (BRASIL, 1940) como *última ratio* do Direito, conseguiu caminhar com todos os processos evolutivos que acompanharam a sociedade, punindo as condutas oriundas da Era digital. Os óbices que foram encontrados em relação ao tipo penal incriminador, foram suprimidos pelo entendimento de que nenhuma conduta considerada como ilícita ficou sem punição, pois, nos referidos casos, a jurisdição se valeu da interpretação para aplicação da lei ao caso concreto.

Conclui-se, portanto, que o maior empecilho não está dentro da legislação, pois o Direito Penal segue garantindo a regulação do poder estatal, onde busca a todo momento a garantia da proteção social gerando o dever de punir. Destarte, o maior óbice está na política de enfrentamento aos crimes da era digital, pois nos deparamos com profissionais desqualificados e despreparados para atuar no combate ao enfrentamento da nova guerra cibernética, esse despreparo é o resultado de um sistema totalmente fraco e omisso, a força deveria surgir de investimentos para progressão de questões relacionadas a melhoria e qualificação desses servidores.

Referências

ARNAUD, André Jean. **O direito entre modernidade e globalização**: lições de filosofia do direito e do estado. Rio de Janeiro: Renovar. 1993, p.3.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira; **Manual de investigação cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016.

BEGALLI, Paulo Antônio. Justiça e Modernidade. Cidadania e Justiça – **Revista da Associação dos Magistrados Brasileiros**. Rio de Janeiro: AMB, a.5, n. 11, p. 160, 2001.

BRASIL. **Lei n. 8.069**, de 13 de julho de 1990. Dispõe sobre o estatuto da criança e do adolescente e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 10 nov. 2022.

BRASIL. **Lei n. 14.155**, de 27 de maio de 2021. Altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940, que torna mais grave os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei n° 3.689, de 3 de outubro de 1941, que define a competência em modalidades de estelionato. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Acesso em: 01 nov. 2022.

BRASIL. **Lei n. 13.105**, de 16 de março de 2015. Institui o Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 março 2015. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em: 07 nov. 2022.

BRASIL. **Lei n. 12.737**, de 30 de novembro de 2012. Altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940, que dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 10 out. 2022.

BRASIL. **Decreto-Lei n. 2.848**, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 07 nov. 2022.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

GIBBS, Graham R. **Análise dos dados qualitativos**. São Paulo: Ártemis, 2009. p.8.

GONÇALVES, Jonas Rodrigo. Como elaborar uma resenha de um artigo acadêmico ou científico. **Revista JRG de Estudos Acadêmicos**. Vol. 3, n. 7, p. 95–107, 2020. DOI: 10.5281/zenodo.3969652. Disponível em: <http://revistajrg.com/index.php/jrg/article/view/41>. Acesso em: 13 out. 2022.

GONÇALVES, Jonas Rodrigo. Como escrever um artigo de revisão de literatura. **Revista JRG de Estudos Acadêmicos**. Vol. 2, n. 5, p. 29–55, 2019. DOI: 10.5281/zenodo.4319105. Disponível em: <http://revistajrg.com/index.php/jrg/article/view/122>. Acesso em: 13 out. 2022.

GONÇALVES, Jonas Rodrigo. Como fazer um projeto de pesquisa de um artigo de revisão de literatura. **Revista JRG de Estudos Acadêmicos**. Vol. 2, n. 5, p. 01–28, 2019. DOI: 10.5281/zenodo.4319102. Disponível em: <http://revistajrg.com/index.php/jrg/article/view/121>. Acesso em: 13 out. 2022.

GONÇALVES, Jonas Rodrigo. Escolha do tema de trabalho de curso na graduação em Direito. **Revista Coleta Científica**. Vol. 5, n. 9, p. 88–118, 2021. DOI: 10.5281/zenodo.5150811. Disponível em: <http://portalcoleta.com.br/index.php/rcc/article/view/58>. Acesso em: 13 out. 2022.

PINHEIRO, Patrícia Peck; **Direito digital**. 7 ed. São Paulo: Saraiva Educação,2021.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**. 3. Ed. Rio de Janeiro: Brasport, 2021.

ZANIOLO, Pedro Augusto; **Crimes modernos**: o impacto da tecnologia noDireito. Curitiba: Juruá, 2007.