FACULDADE EVANGÉLICA DE RUBIATABA
CURSO DE DIREITO
KELLITA DE OLIVEIRA FRAGA

LIMITAÇÕES NO COMBATE AOS CRIMES CIBERNÉTICOS

RUBIATABA/GO
2020

KELLITA DE OLIVEIRA FRAGA

LIMITAÇÕES NO COMBATE AOS CRIMES CIBERNÉTICOS

Projeto de monografia apresentado como requisito parcial para a obtenção do título de Bacharel em Direito pela Faculdade Evangélica de Rubiataba, sob orientação do professor Edilson Rodrigues, Mestre em Ciências Ambientais.

RUBIATABA/GO
2020

KELLITA DE OLIVEIRA FRAGA

LIMITAÇÕES NO COMBATE AOS CRIMES CIBERNÉTICOS

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Faculdade Evangélica de Rubiataba, sob orientação do professor Edilson Rodrigues Mestre em Ciências Ambientais.

MONOGRAFIA APROVADA PELA BANCA EXAMINADORA EM __ / ___ / __

Mestre em Ciências Ambientais Edilson Rodrigues
Orientador
Professor da Faculdade Evangélica de Rubiataba

Mestre em Ciências Ambientais Rogério Gonçalves Lima
Examinador
Professor da Faculdade Evangélica de Rubiataba

Especialista em Processo Civil Lincoln Deivid Martins
Examinador
Professor da Faculdade Evangélica de Rubiataba

Dedico este trabalho a Deus. Sem ele nada seria possível. Dedico ainda este projeto a todos os professores que me influenciaram nesta trajetória. Em especial para o meu orientador Mestre Edilson, com quem compartilhei minhas dúvidas e angústias a respeito do tema e ao coordenador da Faculdade Cláudio Kobayashi, pelo grande amparo.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer a Deus, porque sem sua direção e proteção eu nada seria. Aos meus pais Hermógenes e Maria de Fatima, que sempre estiveram ao meu lado me apoiando ao longo de toda a minha trajetória e por acreditarem que eu seria capaz de superar os obstáculos que a vida me apresentou, obrigada pelas inúmeras vezes que tiveram que abdicar de suas vontades para realizar o meu sonho. Agradeço a minha irmã Kefita, que sempre esteve ao meu lado sendo minha companheira e minha incentivadora, que presenciou as inconstâncias de emoções que enfrentei durante esses últimos cinco anos.

Do mesmo modo, gostaria de agradecer as pessoas que de alguma forma direta ou indiretamente contribuíram para a realização desse sonho, a minha tia, Tereza, que abriu a porta de sua casa e do seu coração, sei que sem suas orações teria sido impossível persistir nessa jornada. Não poderia deixar de mencionar o meu professor do ensino médio, Rui Bandeira, que acreditou na minha capacidade e não mediu esforços para me incentivar, ao meu tio do coração, Antônio, que sempre esteve disposto a ajudar.

Quero agradecer uma pessoa muito importante na minha vida, minha vó, Angelina Viana, que pelos desígnios de Deus não mais está entre nós, contudo, seus incentivos e preocupações me fortaleceram. Aos meus companheiros de curso, quero agradecer por me permitirem crescer ao lado deles, como pessoa e como profissional, sem vocês, essa caminhada não teria tantas recordações. Aos meus mais estimáveis amigos de transporte que alegraram o percurso até Rubiataba, obrigada por fazerem parte da minha vida.

Dentre tantas pessoas que se tornaram meus amigos durante essa jornada, os quais sou eternamente grata, quero agradecer especialmente a minha amiga, Vanessa Lourenço, que desde o primeiro momento que a encontrei nos corredores da faculdade tornou-se um anjo de luz na minha vida, obrigada por ser quem você é. Não poderia deixar de agradecer a minha amiga e companheira Hélida e sua família, que com seu modo afável de ser, acolheu-me em sua casa com tanto amor, não tenho palavras para agradecer.

Por fim, também gostaria de estender meus agradecimentos ao meu orientador Mestre Edilson, por aceitar conduzir o meu trabalho de pesquisa. Ao coordenador Cláudio Kobayashi pelas orientações e a todos os professores pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso. Sei que essas singelas palavras não são suficientes para agradecê-los. Obrigada.

EPÍGRAFE

O que segue a justiça e a bondade achará a vida, a justiça e a honra.

Provérbios 21:21

RESUMO

O objetivo desta monografia é apresentar as limitações no combate aos crimes cibernéticos. Para atingimento deste objetivo a autora desenvolveu o estudo por meio de pesquisas valendo-se do método dedutivo, por intermédio de pesquisas em livros, doutrinas, produções cientificas, artigos e materiais diversos por meio eletrônico (legislação, documentos jurídicos e etc.). A partir das inúmeras incidências de condutas fraudulentas praticadas por meio do uso da internet verificou-se a necessidade da produção deste trabalho. Ao final deste estudo pode-se observar que os números de crimes virtuais estão tendo uma crescente exponencial, e assim vem causando um grande impacto na vida da sociedade. Ante o estudo efetuado observou-se que com o passar dos anos o Estado assumiu para si a responsabilidade de rechaçar condutas criminosas para a defesa dos direitos da sociedade, da mesma feita, chegou-se a conclusão que inúmeras façanhas criminosas podem ser configuradas como crime, pois preenche todos os requisitos para tal, contudo, pela ação negligente do Estado essas façanhas criminosas não estão sendo reprimidas, não por falta de estrutura, mas sim por falta de legislação específica para os crimes cibernéticos, causando assim, uma sensação social de impunidade. Deste modo, nota-se que a criação de leis próprias é crucial para diminuição de tais crimes cibernéticos.

Palavras-chave: Estado. Leis. Cibercrimes.

ABSTRACT

The objective of this monograph is to present the limitations in the fight against cyber crimes. To achieve this goal, the author developed the study through research using the deductive method, through research in books, doctrines, scientific productions, articles and various materials by electronic means (legislation, legal documents, etc.). From the countless incidences of fraudulent conduct practiced through the use of the internet, the need to produce this work was verified. At the end of this study, it can be seen that the number of cyber crimes is increasing exponentially, and thus has had a major impact on the life of society. Before the study carried out it was observed that with the passing of the years the State assumed for itself the responsibility to reject criminal conduct for the defense of the rights of the society, likewise, it was concluded that innumerable criminal exploits can be configured as a crime because it fulfills all the requirements for this, however, by the negligent action of the State these criminal exploits are not being repressed, not for lack of structure, but for lack of specific legislation for cyber crimes, thus causing a social feeling of impunity. Thus, it is noted that the creation of own laws is crucial to reduce such cyber crimes.

Keywords: State. Laws. Cyber crimes.

LISTA DE ABREVIATURAS E SIGLAS

ART	Artigo
CRFB	Constituição da República Federativa do Brasil de 1988
CPB	Código Penal Brasileiro
EUA	Estado Unidos da América
ECA	Estatuto da Criança e Adolescente
Nº	Número
OECD	Organização para Cooperação Econômica de Desenvolvimento
ARPANET	Advanced Research Projects Agency Network
LGPD48	Lei Geral de Proteção de Dados Pessoais
IBGE	Instituto Brasileiro de Geografia e Estatística
PNSI	Política Nacional de Segurança de Informação

LISTA DE SÍMBOLOS

§ Parágrafo

SUMÁRIO

1	INTRODUÇÃO.....	13
2	CONCEITO DE ESTADO E SUA EVOLUÇÃO.....	17
2.1	Análise Estrutural do Crime.....	20
2.2	Evolução da Internet na Sociedade.....	23
3	CRIMES VIRTUAIS EM SUAS VARIADAS FORMAS.....	28
3.1	Responsabilidade do Estado.....	36
4	ANÁLISE DOS CRIMES CIBERNÉTICOS SOB A ÉGIDE DA LEI Nº 12.737/2012 E OUTRAS PREVISÕES LEGAIS.....	39
5	CONSIDERAÇÕES FINAIS.....	46
	REFERÊNCIAS.....	48

1. INTRODUÇÃO

O tema que se pretende investigar é sobre as limitações no combate aos crimes cibernéticos. Busca realizar esse estudo no contexto nacional. A pesquisa se limitará ao âmbito das decisões a partir da entrada em vigência da Lei nº 12.737/2012 que dispõe sobre a tipificação criminal dos delitos informáticos.

Pode-se conceituar os crimes cibernéticos, como sendo aqueles cometidos na internet, seja por meio de uma rede de utilização pública, privada ou doméstica. Eles podem atingir uma única pessoa ou várias pessoas ao mesmo tempo, e têm finalidades diversas. Convém salientar, inclusive, que um mesmo crime pode ser praticado em vários lugares ao mesmo tempo, por meio do uso de um ou de vários computadores diferentes.

Em relação ao combate aos crimes cibernéticos, nos dias de hoje, conta-se com a aplicação da Lei nº 12.737/2012, a qual foi introduzida para repelir crimes cibernéticos, tal qual a aplicação da legislação comum (Leis extravagantes e Código Penal) utilizada para cobrir lacunas na legislação material vigente.

Recentemente o Ministério Público Federal (2018, [s.p]) traçou um panorama sobre o combate aos crimes cibernéticos, o que tem sido um importante combatente, capacitando cada vez mais seus agentes para lograr a identificação dos transgressores. Pode-se extrair que o combate aos crimes cibernéticos se instaura em duas fases, inicialmente com a quebra do sigilo de dados telemáticos, onde busca identificar o usuário e a máquina de onde foi praticado o crime, isso é possível a partir do endereço de IP (número de protocolo exclusivo, pelo período de conexão), data e horário do acesso. Posteriormente, o combate aos crimes cibernéticos empreende a partir da comprovação da autoria e da materialidade, através de busca e apreensão do objeto utilizado, oitiva do assinante da conexão, fotos do local, do laudo pericial etc.

Dada as dificuldades encontradas diariamente no combate aos crimes no “mundo” cibernético, deu-se a necessidade de uma atuação mais efetiva do Estado, no entanto, de forma geral, essa atuação não tem acompanhado as evoluções constantes daqueles que a utiliza com finalidade de obter vantagem em face de outrem. Desse modo, o Estado não consegue oferecer uma segurança jurídica quanto aos crimes cibernéticos, haja vista que os níveis dos delitos na internet são elevados e rápidos, e através de ações ágeis os criminosos conseguem invadir redes e provocar uma série de condutas ilícitas.

Infelizmente, não existe uma gestão proativa e preventiva contra os cibercrimes tão eficientes quanto às próprias manipulações dos criminosos. A segurança virtual ainda está

há longos passos de acontecer em sua totalidade, isso porque o Estado não consegue no mesmo ritmo acompanhar as ações criminosas, e por isso, está sempre a um passo atrás dos bandidos.

Por isso, entende-se que ações mais severas por parte do Estado podem erradicar essa nova modalidade que chegou ao direito penal. Como se sabe, o Estado é conhecedor de suas autonomias, no mesmo sentido em que, detém todas as informações sobre os cidadãos, empresas, veículos, propriedades, assim como pode utilizar desses meios para conseguir impedir os crimes cibernéticos.

Assim sendo, o trabalho traz como problemática a seguinte questão: Há falta de estrutura do Estado para combater os crimes cibernéticos? O objetivo desse trabalho é investigar as limitações do Estado no combate aos crimes cibernéticos. E os objetivos específicos são: Analisar o conceito de Estado, crime, e a evolução tecnológica na sociedade; compreender os crimes virtuais e a responsabilidade do Estado; estudar sobre as legislações existentes sobre os crimes cibernéticos.

No que tange ao conteúdo, a pesquisa analisará apenas os fatores relacionados ao ordenamento jurídico brasileiro. Para chegar às respostas pretendidas neste trabalho, será empregado o método de pesquisa dedutivo, partindo de uma premissa generalizada, que consiste nas inúmeras condutas que são praticadas no âmbito virtual e entendendo como os inúmeros crimes cibernéticos estão sendo abordados e solucionados, e a partir de então, analisar as particularidades de tais legislações vigente aos crimes verificados. Para tanto, a análise será baseada por meio de pesquisas em livros, doutrinas, produções científicas, artigos e materiais diversos por meio eletrônico. Desta forma, após o referido estudo se terá condições de afirmar se existem limitações no combate aos crimes cibernéticos ou não.

Diante do crescimento desacelerado dos crimes provocados pelo mau uso da internet levantou-se o tema supracitado, haja vista a relevância do assunto nos dias atuais. Ante o exposto, urge a necessidade de que as autoridades policiais, assim como o poder judiciário e o ministério público tenham uma capacitação técnica eficiente a sanar os problemas que circulam no meio social. Espera-se que com o presente trabalho possa fomentar a criação de mecanismos para coibir as ações criminosas realizadas através da internet. Do mesmo modo, o trabalho tem a finalidade de incitar o poder público, representado pelo Estado e detentor de obrigações com a sociedade ao combate dos crimes virtuais.

O ambiente virtual usado para facilitar principalmente a comunicação revelou um lado negativo, já que os usuários e criminosas utilizam das tecnologias para cometer uma série de condutas que aos olhos da legislação é tipificado como crime. As acepções de

criminalidade envolvendo a tecnologia da computação alcançam diversas áreas da informática, justamente por ser um termo amplo, os crimes cibernéticos levam a condutas típicas de crimes a partir do Código Penal – Decreto Lei nº. 2.848/1940, vigente e da Lei específica 12.737/2012.

Para alcançar o pretendido resultado, este trabalho está dividido em três objetivos específicos, sendo que o primeiro abordará o conceito de Estado, crime e a evolução da internet na sociedade. Busca-se de início a compreensão do surgimento e evolução do Estado e sua formação, essa abordagem se dá em razão da necessária compreensão dos deveres e responsabilidades que o Estado adquiriu ao longo dos anos de acordo com o modo de governo, posteriormente, abordar-se-á sobre a teoria do crime, pois não há que se falar em punibilidade, e exigibilidade de ação do Estado se a conduta que alguém perpetra não for considerada crime, por fim, discorrer-se-á sobre a evolução da internet na sociedade, para se entender a dimensão e a importância que esta possui na vida de seus adeptos.

Os resultados obtidos nesse primeiro capítulo corroborarão no sentindo de que, após o Estado passar vários momentos, chegou-se a composição de Estado que se tem hoje e com isso é possível observar que, os detentores do poder têm legitimidade para legislar sobre questões que vão garantir os direitos do povo, nesse caso uma lei específica e eficaz para os crimes cibernéticos e que os crimes praticados com o uso da internet preenchem perfeitamente os requisitos para serem tipificados como crime, e ainda, que a internet tem uma grande influência na vida de muitos, e por tanto, precisa ter uma legislação específica.

No segundo capítulo, versar-se-á sobre os crimes virtuais e a responsabilidade do Estado. Desse modo, abordar-se-á sobre alguns crimes cibernéticos mais frequentes cometidos no meio virtual e suas várias modalidades e os vários modos de crimes cibernéticos, também explanará sobre a responsabilidade Estatal em rechaçar os crimes cibernéticos. Esse capítulo consolida a ideia apresentada na problemática deste trabalho, uma vez que os crimes virtuais cada dia mais vêm fazendo parte da realidade jurídica, e a compreensão da estrutura de um crime é de suma importância para que se possa entender que por mais que uma conduta ainda não esteja estabelecida materialmente como crime, nada impede que se possa amoldá-la como tal, para sofrer as consequências necessárias.

Em razão das inúmeras incidências dos crimes cibernéticos, surge também o questionamento sobre quem dotaria a responsabilidade para tolher tais práticas criminosas. Daí a necessidade de abordar a respeito da responsabilidade do Estado e suas atuações, a fim de poder estabelecer uma análise sólida sobre sua atuação. O resultado encontrado nesta seção corroborará para que o leitor possa compreender quais crimes são cometidos virtualmente,

quais são as modalidades de criminosos, e a partir de então enxergá-los como crimes. Também, o resultado encontrado na seção sobre a responsabilidade do Estado, ajudará a compreender que este é dotado de capacidade para adotar medidas que possam reprimir tais cibercrimes.

Por fim, mas não menos importante, far-se-á uma análise da Lei nº 12.737/2012, seus pontos fortes e a escassez de legislação em alguns pontos de suma relevância para tornar a internet uma "terra com leis", além disso, divagar-se-á sobre outras legislações e decretos que foram promulgados sobre os crimes cibernéticos e o "mundo" virtual.

Abordar esta temática contribuirá para a compreensão dos crimes que já estão materializados e abre espaço para discorrer sobre os crimes que necessitam ser tipificados, e ainda, por mais que a liberdade de expressão seja um direito constitucionalmente garantido, dissertar sobre a liberdade de expressão no "mundo" virtual ajudará a compreender que essa liberdade tem limites, e em muitos casos o que as pessoas entendem como liberdade de expressão no mundo virtual, é na realidade configuração de cibercrimes, necessitando então haver uma atuação legislativa maior para materialização penal destas condutas. Os resultados encontrados nesse capítulo contribuirão para o fechamento da ideia de que a legislação existente sobre os crimes cibernéticos é insuficiente, e também demonstrará a vaga tentativa do Estado de demonstrar que estão agindo em prol dos direitos do povo ao elaborar decretos e leis que estão muito aquém das condutas praticadas pelo criminosos.

2. CONCEITO DE ESTADO E SUA EVOLUÇÃO

Essa seção tem como objetivo abordar o conceito e a evolução do Estado, análise da estrutura de crime e evolução da Internet. A conceituação desses temas serve como ponto de partida da observação, posto que estabelece aquilo que em um primeiro instante não é diretamente perceptível e vai gradualmente sendo explicado à medida que se tratará de cada tema para compor a resposta para a problemática apresentada.

Essa discussão será de suma importância, pois, para se obter uma resposta à problemática, necessita-se compreender a organização do Estado e sua evolução, para que se possa atribuir a este a responsabilidade das inúmeras ocorrências de crimes cibernéticos pela ausência de legislação, considerando que este dota o dever de garantir os direitos e garantias individuais e coletivas, e englobando esses direitos está o direito de segurança. Em função disso precisa-se de um conceito inicial.

O intuito de abordar o conceito de crime e a evolução histórica da internet é para ajudar numa percepção de uma realidade cada vez mais recorrente, e não há como abordar questões dessa realidade sem entender quais são os elementos de um crime e como a internet tem sido um "palco" propagador de crimes cibernéticos. Ainda, a evolução histórica da internet propiciara no entendimento do quão importante se tornou esse meio tecnológico na vida de muitos e com isso vem causando constantes transformações, principalmente no âmbito criminal.

Deste modo, para explanar sobre o assunto recorreu-se a obras de alguns escritores, os quais estão presentes nas citações nesse capítulo, como a obra de Dalmo de Abreu Dallari, intitulada como elementos de teoria geral do Estado (2016); Acquaviva – Teoria Geral do Estado (2010); Guilherme de Souza Nucci- manual de direito penal (2019); Gustavo Junqueira – Manual de direito penal (2013), para formação do entendimento recorreu-se a alguns artigos científicos, para uma divisão correta desta seção, explorar-se-á o material disponibilizado pelo coordenador da Faculdade Evangélica de Rubiataba Cláudio Kobayashi.

De início, cumpre discorrer sobre a transformação contínua da sociedade, ora evoluindo, ora retrocedendo. Nessa esteira, se respeitar a ideia exposta por Aquaviva (2010, p. 47), "a sociedade humana, propriamente dita, mostra-se dinâmica e mutável, sempre em perpétuo movimento. Fruto da cultura e da experiência acumulada pelo homem". Entende-se, que essas transformações são consequências de tudo que se dispõe a vivenciar.

O Estado como entidade de poder soberano trouxe para si responsabilidades, e com isso, tem o dever de garantir o necessário para aqueles que estão sob sua guarda, conforme demonstra o preâmbulo da Constituição da República Federativa do Brasil, vejamos:

> Nós, representantes do povo brasileiro, reunidos em Assembléia Nacional Constituinte para instituir um **Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fraterna,** pluralista e sem preconceitos, fundada na harmonia social e comprometida, na ordem interna e internacional, com a solução pacífica das controvérsias, promulgamos, sob a proteção de Deus, a seguinte CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL. (BRASIL, 1998, grifo nosso).

Nessa senda, observa-se que na promulgação da nossa Constituição de 1998, esta assumiu a responsabilidade de assegurar a segurança individual bem como os direitos sociais. Posto isto, imprescindível faz-se entender as transformações pelas quais o Estado enfrentou para se chegar ao status atual.

Desta feita, compreende-se da conceituação exposta na obra de Dallari (2016, p. 62), as inúmeras formas que poderão originar um Estado e a formação de uma sociedade, dentre essas teorias está a de que "o Estado teve sua formação de forma natural e espontânea, não havendo entre elas uma coincidência quanto à causa, obedecendo ao curso natural das coisas, não por um ato puramente voluntário". Em continuidade, outra teoria a ser mencionada do mesmo autor é a "formação do Estado a partir da vontade de alguns homens, ou então a de todos os homens, gerando a denominação de formação contratual".

Assim sendo, percebe-se que não há um conceito uníssono sobre o surgimento do Estado, fazendo com que esse conceito possa ser formado a partir da visão e opinião de cada qual, gerando em torno do assunto, abrangentes teorias, como as expostas acima, todavia, de forma a corroborar com o presente trabalho, conclui-se que, a partir do instante em que o Estado assume uma obrigação, surge o dever de garantir e zelar pelos direitos daqueles que lhes conferiram essa atribuição.

Noutro giro, considera-se a vinculação do direito penal e o direito de punir do Estado, Bittencourt (2015, p.78), assim disserta:

> Defendemos que a exegese do Direito Penal está estritamente vinculada à dedução racional daqueles bens essenciais para a coexistência livre e pacífica em sociedade**. O que significa, em última instância, que a noção de bem jurídico-penal, é fruto do consenso democrático em um Estado de Direito. A proteção de bem jurídico, como fundamento de um Direito**

> **Penal liberal, oferece, portanto, um critério material extremamente importante e seguro na construção dos tipos penais,** porque, assim, "será possível distinguir o delito das simples atitudes interiores, de um lado, e, de outro, dos fatos materiais não lesivos de bem algum". **O bem jurídico deve ser utilizado, nesse sentido, como princípio interpretativo do Direito Penal num Estado Democrático de Direito e, em consequência, como ponto de partida da estrutura do delito** (grifo acrescido).

Destarte, quando um indivíduo comete um ilícito penal, surge para o Estado o *jus puniendi*, ou seja, o direito de o Estado punir o infrator. À vista disso, o bem jurídico deve de todo modo ser tutelado e amparado, e para tanto abrange o direito de segurança direito à vida e à privacidade dentre outros.

Constata-se ainda que o Estado não é improgressivo, passando desde sua formação por inúmeras fases, e cada uma traz consigo uma peculiaridade e uma atribuição para o que se é hoje, sendo que cada etapa é formada por períodos cronológicos. Com a percepção das suas várias fases vivenciadas pelo Estado, de acordo com Dallari (2016, p. 59) surgiram as seguintes Cognominações "Estado Antigo, Estado Grego, Estado Romano, Estado Medieval e Estado Moderno".

Fazendo uma abordagem sobre o Estado moderno, vale mencionar que, diante tantas desigualdades despertou na população a busca pela igualdade, gerando assim um novo Estado, conforme preceitua Dallari (2010, P. 77), repare:

> Marcas fundamentais, desenvolvidas espontaneamente, foram-se tornando mais nítidas com o passar do tempo e à medida que, claramente apontadas pelos teóricos, tiveram sua definição e preservação controvertidas em objetivos do próprio Estado.

Com tal apontamento, em linhas gerais, pode se afirmar a existência de várias posições, no que se refere aos elementos de composição do Estado Moderno. Posto isso, delimitar-se-á aos três elementos materiais mais sedimentados na concepção de Marcus Cláudio Acquaviva, quais sejam, (1) povo; (2) nação; (3) território.

"O povo, compreende como sendo uma totalidade de pessoas que se encontram num dado momento, em um determinado Estado" (ACQUAVIVA, 2016, p. 63). Nesse contexto, engloba o todo da população não se distinguindo pela nacionalidade, idade, ou qualquer outra distinção existente, o que vale para quantificar é o total de pessoas dentro do Estado.

O segundo elemento material é a nação, e quanto a esta, convém indicar as sábias palavras de Acquaviva (2010 p. 31) "Quanto à nacionalidade, consiste no vínculo jurídico que

liga o indivíduo ao Estado, em razão do local de nascimento, da ascendência paterna ou da manifestação de vontade do interessado".

O conceito material de território desdobra-se no seguinte vértice, Acquaviva (2010 p. 31) "o território pode ser uma parcela do solo, na qual o Estado exerce seu poder soberano, com uma ficção jurídica, isto é, um dado abstrato, ideal". Destarte, os elementos materiais são de suma importância para compreensão do Estado em um todo, pois através dessa conceituação, surge a responsabilidade de cada Estado zelar pelos componentes e pelo seu espaço.

Com o reconhecimento da existência de um Estado, conclui-se que encontram alguns elementos dentro de sua formação, como foi supramencionado, um dos componentes é a constatação de que o povo é componente material do Estado. Consequentemente, traz para o Estado a responsabilidade de fornecer tudo quanto for necessário para assegurar os direitos destes. Importante destacar uma relevante passagem no livro de Acquaviva (2010, p. 71), que diz:

> Sem o mínimo de ordem, a vida não seria possível nem por um instante. A insegurança, a incerteza e os abusos destruiriam a sociedade quase na rapidez de um terremoto. Por isso, dentre os atributos essenciais do Estado, refulgem o poder amparado na força, e o direito que modela o exercício desta.

Por conseguinte, quando um determinado ser humano se depara com uma situação onde seus direitos estão sendo de forma arbitrária restringidos ou cerceados, quer pela ação ou pela omissão do próprio Estado, cabe a este rever seus atos para que tal situação não persista, estabelecendo um Estado de direito.

Por fim, ante o exposto, conclui-se que em todas as mudanças enfrentadas pelo Estado, sempre se teve a presença de alguém que detinha o poder e ditava as "regras" para aqueles que estavam em seu território, com isso, reportando para o tema em questão, qual seja, limitações no combate aos crimes cibernéticos, este tópico contribui para a compreensão no sentido de que, os detentores do poder tem legitimidade para legislar sobre questões que vão garantir os direitos do povo, nesse caso uma lei específica e eficaz para os crimes cibernéticos. Na sequência, para contribuir o presente trabalho, far-se-á uma abordagem pormenorizada da análise estrutural do crime.

2.1 ANÁLISE ESTRUTURAL DO CRIME

Esta seção será dedicada ao estudo sobre a análise estrutural do crime, suas características, bem como os elementos que o compõe, também serão abordadas sua finalidade e posteriormente apresentação de resultados. Tópico de suma importância para percepção da problemática proposta.

A presente abordagem tem como finalidade conceituar e definir a estrutura de crime, quais são seus requisitos para que se possa entender o que é e quando pode ser caracterizado como conduta criminosa e que no término possa concluir se as condutas que são praticadas cotidianamente virtuais podem ou não ser consideradas como crime.

Para enriquecimento dos argumentos sobre o assunto, recorreu-se a pesquisas bibliográficas de alguns escritores como Bitencourt, Nucci, Junqueira e a Constituição da República Federativa do Brasil de 1988. A abordagem do tema trará a importância de se criar novas leis, mais eficazes a respeito dos crimes cibernéticos, tendo em vista que, para legislar sobre determinado assunto faz-se necessário o enquadramento do fato como crime, o que será mostrado adiante.

Ao utilizar a culpabilidade como critério da pena, automaticamente significará um juízo de valor, que assente atribuir responsabilidade pela prática de um fato típico e antijurídico a uma pessoa precisa, para a decorrente aplicação da pena. Assim sendo, deverá analisar fartos requisitos, para que não ocorra falha no momento que necessitar efetivar o direito ao caso concreto, Bitencourt (2012, p.62), em sua obra escreve sobre dois principais requisitos que terá que observar, é a capacidade de culpabilidade e a consciência da ilicitude da conduta.

Porém, para entrar em uma discussão mais precisa sobre a culpabilidade daqueles que cometem uma determinada ação criminosa, principalmente nos delitos cibernéticos, o assunto em ênfase, faz-se necessário discorrer sobre a teoria geral do crime. Para a definição utilizada pelo conceituado escritor Nucci (2019, p 147) o crime é classificado da seguinte forma: fato típico, antijurídico e culpável.

Fato típico é a descrição abstrata de uma ação, ou seja, aplicando em sua íntegra o princípio da legalidade. Junqueira (2013, p 150), em sua obra conceituou, como sendo:

> A tipicidade é característica da ação que consiste em adequar-se a determinado tipo. O tipo é um substantivo que descreve uma realidade jurídica. A tipicidade é um adjetivo que implica em afirmar que uma ação concreta amolda-se a determinado tipo. A conduta, portanto, tem como atributo ser ou típica.

Por conseguinte, de imediato remete ao descrito na CRFB/88, em seu artigo 5º inciso XXXIX “não há crime sem lei anterior que o defina, nem pena sem prévia cominação

legal". Então considera conduta lesiva aquela que viola tal preceito. Nos crimes cibernéticos observa-se que a conduta daqueles que se utilizam das redes de internet na tentativa de se camuflar, tem a legislação que a tipifica prevista na lei nº 12.737/2012.

Outra classificação é a antijuridicidade ou também denominada ilicitude, e esta segundo Nucci (2019, p. 211), "é a contrariedade de uma conduta com o direito, causando efetiva lesão a um bem jurídico protegido. Trata-se de um prisma que leva em consideração o aspecto formal da antijuridicidade". Com isso há algumas condutas que são consideradas como condutas de ação atípica como, por exemplo, as excludentes de ilicitude, não existindo, nesses casos, qualquer ação advinda do ser humano com intendo de agir com dolo e também não tendo nenhuma norma incriminadora.

Ao analisar os crimes perpetrados por meios virtuais, entende-se que em inúmeras situações o criminoso age de modo intencional, violando um ou vários bens da pessoa humana, bens estes que estão sob a guarda daquele que zela pelo bem de todos, o Estado, como a intimidade à vida, causando grandes consequências para as vítimas. Não podendo alegar nesse caso, que as condutas destes criminosos são passiveis de serem isentas pela grande dificuldade de identificação ou pelo embaraço que encontram em provar a ilicitude cometida por aqueles, pela escassez de legislação, merecendo uma atenção e uma atuação maior por parte do Estado.

A última classificação do crime é a culpabilidade, e nesse ponto, Nucci (2019, p. 257), diz que "a culpabilidade trata-se de um juízo de reprovação social, incidente sobre o fato e seu autor, devendo o agente ser imputável, atuar com consciência potencial de ilicitude, bem como ter a possibilidade e a exigibilidade de atuar de outro modo". É indene de dúvida que aquele que se utiliza dos meios virtuais para causar alguma consequência prejudicial para outrem, age de forma consciente tendo sim a opção moral de nada fazer e de abster de tal ação, contudo, nesses casos, a ação é contrária.

À face do exposto, pode-se chegar à conclusão que aqueles que cometem qualquer conduta com intuito de prejudicar outrem se utilizando dos meios que a internet propicia têm que ser responsabilizados, com isso os resultados obtidos nessa seção contribuiu no sentido de que, restou comprovado que as condutas praticados com o uso da internet preenchem perfeitamente os requisitos para ser tipificados como crime. Ao reverso, se todas as práticas criminosas praticadas no âmbito da internet não configurassem um delito, não seria possível exigir uma solução, vez que não seria da competência do Estado tutelar tais ações.

Contudo, ficou evidente que as condutas, afrontam sim inúmeros direitos respaldados pela Constituição da República Federativa do Brasil, para tanto, exige-se uma

atuação mais eficaz do Estado na aplicação das leis vigentes e também elaborar novas leis adequando-as a nossa atualidade, necessitando tão somente de uma atuação legislativa para consolidar em lei tais práticas. Sequencialmente, na seção vindoura será versado sobre a evolução da internet na sociedade e sua importância.

2.2 EVOLUÇÃO DA INTERNET NA SOCIEDADE

Na última seção, discorrer-se-á sobre o meio pelo qual os crimes cibernéticos são praticados, a internet, para um maior discernimento do leitor, para isso, falar-se-á sobre os vários momentos em que a internet percorreu para conseguir chegar à dimensão atual. Essa abordagem tem como finalidade levar o conhecimento do surgimento da internet, sua evolução, contexto histórico e sua relevância.

Para engrandecer esse trabalho, foi realizada a utilização de pesquisas bibliográficas em obras de escritores como Piaget em sua obra - Para onde vai a educação (2002); Moran – Integração das tecnologias na educação (2005); Barata – Criminologia crítica e crítica do direito penal introdução à sociologia do direito penal (2002); Xavier – O hipertexto na sociedade da informação: a constituição do modo de enunciação digital (2015); Ávila – uma anamnese da história da escrita (2008), as quais poderão ser evidenciadas pelas citações. Em que pese à internet ser o vetor principal, pelo qual os criminosos se utilizam para cometer os crimes cibernéticos, a discussão desse tema se torna imprescindível para responder a problemática apontada.

A informática nos últimos anos passou a fazer parte do cotidiano de quase toda população mundial e no Brasil da mesma forma. É impressionante a velocidade da tecnologia criada, são inúmeros benefícios que a tecnologia promoveu considerando as fronteiras, assim foi possível que as informações e notícias circulassem o mundo num piscar de olhos. Desse modo, não se pode afirmar que a tecnologia trouxe apenas benefícios aos seus usurários. Todo esse avanço tecnológico infelizmente resultou nos crimes cibernéticos.

Sabe-se que a internet é utilizada para várias finalidades, dentre elas, a transmissão de dados e informações são as principais, com isso, verifica-se a facilidade do crime para as pessoas que aproveitam de tais informações para tirar proveito pelo anonimato das redes, causando danos às vítimas, e ficando impunes pelos crimes cibernéticos pela dificuldade em encontrar a localização do criminoso.

As tecnologias de comunicação e da informação evoluem sem parar e com bastante celeridade. Tornou-se um grande desafio para a sociedade à democratização do

acesso à tecnologia disponível, juntamente com a consequente possibilidade de usar tais recursos para alcançar as informações, considerando o contexto econômico, social, e educacional do país. No entanto, nem sempre foi assim, as tecnologias são frutos de avanços progressivos, conforme discorre Piaget (2002, p.443):

> Por volta de 1860 surge um aparelho de comunicação de grande importância também para os dias atuais, o telefone, que foi inventado pelo italiano Antonio Meucci, este o inventou com o objetivo de comunicar-se com sua esposa doente que ficava no andar superior da casa em uma cama, no mesmo ano o italiano tornou pública sua invenção. No Brasil o telefone foi instalado no ano de 1883 no Rio de Janeiro. Após o surgimento do jornal e do telefone o homem conseguiu evoluir ainda mais com a invenção do rádio, a primeira transmissão é datada de 1900, a partir deste momento marca se o início de uma forma de transmitir informações numa velocidade maior, pois as ondas do rádio tinham um alcance às pessoas muito superior ao do jornal, essa evolução marca o momento em que as informações passam a cruzar grandes distâncias geográficas, culturais e até mesmo cronológicas

O homem desde os primeiros momentos em que passou a conviver em grupo teve à necessidade de comunicação com os demais, como forma de expressar seus desejos, culturas, sentimentos, e utilizavam a comunicação muitas vezes para alertarem sobre algum perigo que tivesse próximo ao seu grupo. Por isso, a comunicação sempre foi um instrumento bastante importante para a vida em sociedade, já que através dela as pessoas podem se expressar.

Sobre as mudanças das tecnologias, Ávila (2008, p. 15), vem explicar que:

> Os avanços tecnológicos estão sendo utilizados praticamente por todos os ramos do conhecimento. As descobertas são extremamente rápidas e estão a nossa disposição com uma velocidade nunca antes imaginada. A internet, os canais de televisão a cabo e aberta, os recursos de multimídia estão presentes e disponíveis na sociedade. Em contrapartida, a realidade mundial faz com que nossos alunos estejam cada vez mais informados, atualizados, e participantes deste mundo globalizado.

O homem evoluiu com o decorrer dos anos, e sempre buscou desenvolver meios que pudesse facilitar sua vida em sociedade, e a comunicação foi um dos aspectos essenciais para a melhoria da vida em sociedade, já que por meio dela tornaram-se sujeitos ativos e capazes, além de facilitar a comunicação social das pessoas de uma determinada sociedade.

O processo de evolução foi se desenvolvendo até chegar à era da comunicação permitida pela tecnologia, no entanto, todo esse processo de evolução sofreu alterações

significativas na história passando por várias fases e invenções até que chegasse a tecnologia que a sociedade atual conhece.

"As chamadas 'tecnologias da inteligência', construções internalizadas nos espaços da memória das pessoas e que foram criadas pelos homens para avançar no conhecimento e aprender mais, vem ressaltando a linguagem oral, a escrita e a linguagem digital". Assim, os computadores podem ser citados como exemplos desse tipo de tecnologia. (XAVIER, 2015, p.35).

Entretanto, as evoluções tecnológicas ao mesmo tempo em que trouxeram mudanças importantes a sociedade também provocou algumas variações quanto ao uso, já que a sociedade utiliza os recursos tecnológicos sem pensar nas consequências ou prejuízos.

A dificuldade em punir os criminosos está principalmente adstrita com a falta de legislação adequada, haja vista que, o ordenamento jurídico brasileiro não possui um acervo de legislações aplicadas ao caso, apenas um ali outra acolá que possa facilitar a identificação e na punição dos criminosos cibernéticos.

Basicamente, existe hoje no Brasil apenas duas leis que tratam dos crimes virtuais, uma é a Lei 12.735/2012 e a 12.737/2012. No entanto, elas não são suficientes para regulamentar as infrações cometidas no mundo da web. Posto isto, é importante realizar um estudo mais aprofundado sobre o tema em comento, com a finalidade de obter informações relevantes acerca das limitações no combate aos crimes cibernéticos.

Barata (2012, p. 28) traz alguns apontamentos que sugere o início da internet no mundo, veja:

> Sabe-se que a Internet teve início em plena guerra fria, e foi utilizada como uma arma norte-americana de informação militar. E possuía como principal função interligar todas as centrais de computadores dos postos de comando estratégicos, fazendo com que os americanos, se prevenissem de uma suposta ofensiva russa. Porém se ocorresse algum imprevisto em um desses pontos estratégicos e os americanos fossem atacados, os demais pontos continuariam funcionando de forma autônoma, auxiliando e fornecendo informações a outros centros militares.

O contexto histórico da internet está ligado a 1946 quando surgiu o primeiro computador digital. Anos mais tarde, em 1950 iniciou-se a comercialização do computador no mundo. Jonh Kennedy prometeu que criaria um satélite para impulsionar o desenvolvimento tecnológico, e assim foi criado através da Agência de Investigação de Projetos Avançados. Essa agência foi à idealizadora e criadora da internet que surgiu em 1969. A finalidade

principal da arpanet (Rede da Agência de Pesquisas em Projetos Avançados) era estabelecer a comunicação entre os militares em suas bases nos EUA. (BARATA, 2012, p. 80).

O autor prossegue, explicando sobre os avanços tecnológicos da internet:

> Ao mesmo passo dos avanços tecnológicos, surgiram as ameaças virtuais. Elas se iniciaram com um grupo de programadores que elaboraram um jogo nomeado "Core Wars", apto este a se autorreproduzir a cada execução, causando um sobrepeso à memória do computador. Os mesmos criadores também desenvolveram o primeiro antivírus, chamado de "Repper", com a finalidade de aniquilar as cópias criadas pelo "Core Wars". Após este intento, diversas ameaças nasceram com o uso de computadores. Outro exemplo foi Richard Skrenta, que, aos quinze anos, desenvolveu o "ElkCloner", considerado por diversos estudiosos como o primeiro vírus com o objetivo de contaminar computadores. (BARATA, 2012, p. 28).

"A internet é entre tantos, mais um rico recurso para uma metodologia dinâmica de ensino, quando bem explorada nos proporciona uma vasta quantidade de ferramentas que podem enriquecer o processo de ensino aprendizagem, entre tantos artifícios" (MORAN, 2015, p. 12).

O uso da internet possibilitou aos usuários maior facilidade na comunicação, contribuindo para que ocorresse mesmo diante da distância, assim, as pessoas não têm mais problemas quanto às limitações visuais e auditivas, mesmo que essas conversas venham ocorrer por plataformas digitais, do mesmo modo foi facilitado o envio de dados e informações.

O autor José Manuel Moran segue afirmando que sobre a internet "ao selecionamos os seguintes recursos: o alto poder de divulgação, pesquisa, comunicação, exploração, informação, educativos" (MORAN, 2015, p. 12-13). Muitos crimes na atualidade, não são restritos ao âmbito computacional, isto é, provocam danos não somente aos computadores, mas também, em vários casos, a privacidade e a vida íntima da pessoa usuária da internet, como por exemplo, na invasão ao ICloud dos famosos que tiveram suas fotos e demais conteúdos pessoais expostos.

Em conclusão, os resultados obtidos nessa seção demonstraram que a internet é sim algo que está fazendo parte da vida de muitas pessoas, por isso, consideram a grande influência e importância que ela está obtendo, é mais que necessário que haja uma tutela jurídica que respalde o direito dos seus usuários para que não fiquem vulneráveis as ações criminosas.

Aliás, levando em conta a problemática apresentada, o resultado encontrado demonstrou que a internet também é um bem jurídico que merece proteção e assim o Estado

necessita com urgência aplicar as leis já existentes com eficácia, bem como elaborar outras mais abrangentes, tendo em vista que, atualmente os casos de crimes cibernéticos têm uma crescente vertiginosa e a cada dia aqueles que a utilizam se capacitam, com isso, ao tratar desse tema é clarividente que a internet, assim como o Estado vem sofrendo inúmeras mudanças ao longo dos anos, ao passo que muitos têm manuseado a internet e seus meios para prejudicar vidas alheias, por isso o entendimento da evolução da internet foi de suma importância para se chegar a esse resultado, em síntese. Sequencialmente far-se-á uma abordagem sobre os crimes virtuais e a responsabilidade do Estado e suas nuances.

3. CRIMES VIRTUAIS EM SUAS VARIADAS FORMAS

Essa seção tem como objetivo discorrer sobre os crimes que podem ser praticados virtualmente, tendo como meio o uso de computadores ou da internet. Para explanar com mais clareza as abordagens sobre a temática desta pesquisa, utilizar-se-á da ajuda de obras literárias de escritores como, por exemplo, Chaves, Viana, Roque Molina, Rosa dentre outros, e essas colaborações poderão ser observadas através das citações inframencionadas de forma que estas corroborarão de forma ímpar com este trabalho de conclusão de curso.

Tal abordagem corroborará para a explicação de que a internet tem sido um palco de incontáveis crimes, e que esse tem sido um problema enfrentado por muitas vítimas, por essa razão trazer a baila os inúmeros delitos que podem ser identificados virtualmente é relevante para entender a dimensão do problema apresentado e perceber a necessidade de uma atuação jurídica.

Ressalta-se que esta seção ajuda no esclarecimento da discussão abordada no presente trabalho, diante do fato de que, com a internet estando disponível e acessível com mais facilidade pelas pessoas, propiciou também o crescente aumento desse tipo de crime e assim, fez com que novas tipificações de crimes fossem reconhecidas e, consequentemente surgindo a necessidade do aprimoramento na legislação penal vigente.

Inicialmente, cabe salientar que a informática favoreceu de forma quase que indiscutível para a comunicação entre as pessoas por se tratar de uma tecnologia que permite de forma bastante simples essa interação entre as pessoas em toda parte do mundo. Contudo, como já mencionado antes, também houve o uso desta tecnologia de maneira prejudicial e por isso o Estado teve que intervir e reprimir os crimes praticados de forma virtual, pois em que pese olhar sob a ótica de ser em “mundo” virtual que é diferente do “real”, tais crimes afetam diretamente a vida daqueles que são vítimas com este tipo de conduta criminosa.

Como a legislação material penal não permite o uso da analogia ao caso concreto, isso dificultou grandemente a punição daqueles que cometem os cibercrimes, tendo em vista que muitas condutas não estão tipificadas. A partir do manual de cooperação jurídica internacional e recuperação de ativos, extrai-se o conceito de crimes virtuais:

> Crime virtual ou crime digital pode ser definido como sendo termos utilizados para se referir a toda à atividade onde um computador ou uma rede de computadores são utilizados como uma ferramenta, uma base de ataque ou como meio de crime. Infelizmente, esta prática tem crescido muito já que esses criminosos virtuais têm a errada impressão que o anonimato é possível na Web e que a Internet é um mundo sem lei. (BRASIL, online, 2008).

Bem, como se vê acima, toda atividade onde um computador ou que seja uma rede de computadores são utilizados como meio para se praticar um crime, este crime será caracterizado como sendo um crime virtual, porém, esses crimes ultrapassam o alcance virtual e, por conseguinte, trazem danos efetivamente reais tanto para as pessoas físicas quanto para as pessoas jurídicas, logo, precisam ser coibidos.

Há uma dissemelhança entre os delitos de computação e crimes cibernéticos, assim o doutrinador aponta que "crimes de informática são todas as ações típicas, que são praticadas no intuito de expor alguém para o mundo virtual com a utilização de computadores e/ou de outros recursos da informática". (BARATA, 2012, p. 28-29).

No que tange os crimes cibernéticos, Molina (2011, p.67) assim conceitua "pode-se conceituar como sendo aqueles cometidos utilizando a Internet, sendo então derivado do crime de informática, pois, necessita utilizar os computadores para acessar a Internet".

A palavra cibernética é a "ciência geral dos sistemas informantes e, em particular, dos sistemas de informação. Sendo a ciência da comunicação e dos sistemas de informação, parece o termo mais amplo, e apropriado, a denominação dos delitos tratados nesse trabalho de crimes cibernéticos" (CHAVES, 2017, p. 19). Desse modo, compreende um conceito mais amplo sobre os crimes cibernéticos.

Pelas lições de Rosa (2012, p. 52), compreende-se que:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o 'Crime de Informática' pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão.

Nota-se que, diante o posicionamento do autor acima mencionado que os crimes de informáticas podem ter mais de um modo operacional, contudo, essas condutas podem configurar crime por ser uma ação típica, antijurídica e culpável. Ainda, o alcance desses crimes pode ser para inúmeras pessoas e atingir patrimônios.

A OECD (Organização para a Cooperação Econômica e de desenvolvimento), “propôs uma definição ampla, conceituando esse tipo de crime como sendo qualquer conduta ilegal não ética, ou não autorizada que envolva processamento de dados e/ou transmissão de dados”. (ROSA, 2012, p 52). Percebe-se que, tem inúmeras condutas e definições, contudo, todas ofendem direitos garantidos pela Constituição.

Já nas palavras de Roque (2007, p. 13), os crimes cibernéticos são: “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”. Por sua vez, Castro (2003, p. 88), a partir da Convenção sobre o Cibercrime de Budapeste explica o seguinte “os crimes de informática são aqueles perpetrados através dos computadores, contra os mesmos, ou através dele. A maioria dos crimes é praticada através da internet, e o meio usualmente utilizado é o computador”.

Junto à globalização, às novas tecnologias à internet, começaram também a surgir crimes virtuais que crescem em uma proporção alarmante e que causam muita preocupação entre os usuários da internet. São vários os crimes praticados pelo uso da internet, entre eles, a invasão de sistemas, a pirataria, a pedofilia, transmissão de vírus, danificação de arquivos, roubo, extorsão, sequestro de dados, compartilhamento de vídeos, fotos e áudios, dentre outros.

Acerca dos crimes cibernéticos, existe no mundo virtual, a figura principal dos criminosos, que é o sujeito ativo que utiliza dos conhecimentos da informática e da internet para praticar o crime causando prejuízo à vítima, podendo atentar contra sua vida, liberdade, honra e privacidade. Já o sujeito passivo “é o titular do bem jurídico lesado ou ameaçado pela conduta criminosa. Nos crimes de informática, o sujeito passivo é aquele que venha sofrer qualquer tipo de prejuízo proveniente de sistemas informatizados, podendo ser física ou jurídica”. (BRASIL, 2008, p. 125).

Sobre o perfil dos criminosos, é importante ressaltar que:

> O perfil dos criminosos digitais normalmente é: jovens, entre 15 e 32 anos, do sexo masculino, com inteligência acima da média, educados, audaciosos e aventureiros, sempre alegam o desconhecimento da ilegalidade cometida movida pelo anonimato oferecido pela Internet, têm preferência por ficção científica, música, xadrez, jogos de guerra e não gostam de esportes de impacto. Como o criminoso virtual é aquele que não se apresenta fisicamente e pode agir de qualquer parte do planeta, levam os criminosos a acreditarem que estão imunes às leis (WENDTH; JORGE, 2012, p.29).

Assim, depreende que o perfil do criminoso é consideravelmente ímpar, necessitando ter uma inteligência em demasia, todavia infelizmente é utilizada para a prática inadequada. Outro ponto importante é a sensação dos criminosos de serem inatingíveis por acreditarem que não estão agindo de forma ilegal, o quê de certa forma está correta, vez que muitas condutas que eles praticam não estão estatuídas em lei, ou seja, não estão agindo em desconformidade com o ordenamento jurídico para serem punidos.

Em outro trecho da citação acima, restou evidente que os criminosos como já mencionado neste trabalho, vivenciam a total tranquilidade de não serem identificados, visto que estão escondidos atrás de um computador ou um celular ou por outro meio que lhes cause essa noção, e o fato de se sentirem assim é um fator que deixa o usuário criminoso sentindo-se seguro para a prática dos delitos cibernéticos.

Para uma melhor compreensão dos termos utilizados para definir esses criminosos segue uma explanação. Deste modo, os Preaker são definidos como “aqueles que fraudam os meios de comunicação telefônica, para proveito próprio sem o pagamento devido, instalando escutas a fim de facilitar o acesso externo, visando o ataque a sistemas” (WENDTH; JORGE,2012, p. 29-30).

No caso dos Lammers esses são definidos como “aqueles que possuem algum conhecimento querem se tornar um hacker, e dessa maneira ficam invadindo e perturbando os sites, em outras podem ser denominados de iniciantes” (WENDTH; JORGE, 2012, p. 30).

As vítimas dos crimes cibernéticos são pessoas que são atingidas de forma direta ou indiretamente pelo uso da tecnologia, haja vista que, os bandidos se apoderam de dados, imagens, áudios, senhas, entre outros recursos pessoais para prejudicar o usuário sem qualquer tipo de medo às infrações que podem se caracterizar.

Molina (2011, p.54) sobre as vítimas dos crimes cibernéticos explica que:

> Podemos citar ainda, as vítimas de pedofilia, de pirataria de software, de dano, contra a honra, entre muitas outras vítimas de crimes praticados pela Internet. A agilidade que a Internet proporciona ao seu usuário para realização de diversas tarefas, como entretenimento, trabalho, pagamentos de despesas, entre outras, facilita também a ação de pessoas inescrupulosas que se aproveitam do anonimato e da falta de segurança existente na rede para conseguir informações sobre os usuários, principalmente senhas que são digitadas durante essas transações. Os atos ilícitos praticados via Internet, a cada dia que passa, aumentam a sua prática e sua diversificação. Temos crimes antigos, que agora são praticados pela rede mundial, assim como, temos novas modalidades. No entanto, alguns desses crimes já estão tipificados no nosso ordenamento jurídico, por exemplo: o furto, estelionato, etc.

Existe um leque abrangente de crimes que podem ser praticados pela internet. O código penal brasileiro tipificou em seu art. 313- A o crime de inserção de dados falsos em sistemas de informações, o qual também está tipificado no capítulo os crimes contra a administração geral. Não obstante, o art. 313-B do CPB reforçou a tipificação anterior referente aos dados falsos inseridos em sistemas que condicionem informações e dados.

Prosseguindo sobre os crimes praticados pela internet, a pornografia infantil também é um dos tipos dos crimes cibernéticos. O Estatuto da Criança e do Adolescente (ECA) já previa em seu art. 241 a tipificação inicial sobre a conduta de fotografar ou publicar cenas de sexo que envolvesse crianças e adolescentes, no entanto, após a promulgação da Lei 10.764/2003 o tipo penal foi alterado, determinando como crime expressamente a prática criminosa pela rede mundial de computadores.

Cassanti (2014, p. 14), explica sobre a pornografia infantil que é através das "home pages" e por correio eletrônico. As home pages são definidas segundo Ian (2010, online) como sendo "a página inicial de um site, ou seja, é página de entrada quando o usuário digita o endereço eletrônico de um site", já os correios eletrônicos são definidos por Editorial (2017, online) como sendo um "serviço digital que permite aos usuários de computadores o envio e a recepção de mensagens com conteúdo de texto. Ao se utilizar da chamada "home pages", os gerenciadores das páginas recebem uma quantia dos usuários (através de depósito ou cartão de crédito) que dispõe de um acervo de fotos e vídeos. "Já ao se utilizar de correio eletrônico, o material é distribuído de um usuário a outro, diretamente".

Não obstante, ainda sobre o crime de pedofilia pela internet, a Lei Federal 11.829/2008 trouxe nova redação para o tipo penal, tornando mais claro a interpretação acerca do combate a produção, a comercialização, e a distribuição da pornografia envolvendo menores de idade (crianças e adolescentes), assim como é claro ao afirmar que é crime a compra e o compartilhamento de pornografia infantil, o qual configura pedofilia na internet.

Existem ainda outros crimes praticados pelo uso da internet. A falsificação, que com o advento das novas impressoras de alta resolução facilitou a falsificação de documentos oficiais, papel-moeda, entretanto o crime ainda é de falsificação de papéis e documentos públicos (arts. 293 e 297, CPB) e falsificação de moeda (art. 289, CPB) (VIANA, 2003, p. 13).

"Outro tipo de crime bastante comum no mundo virtual é a utilização dos Cavalos de Tróia e Sniffers que são bastante utilizados para se conseguir as senhas dos cartões de crédito e os números das contas, para que logo após sejam sacados todo o dinheiro e realizado compras com os cartões alterados" (BARATA, 2002, p. 42).

Assim, a conduta é entendida pela matéria penal como o crime de estelionato previsto no art. 171 do Código de Processo Penal, doutro lado, doutrinadores afirmam que se trata de furto conforme art. 155 do Código Penal Brasileiro.

> O crime de dano que é previsto no artigo 163 do Código Penal, que ocorre quando um cracker invade uma página da "Internet" danificando-a, destrói banco de dados, arquivos e demais informações constantes no disco rígido. O crime de estelionato (art. 171, CPB), também pode ser aplicado a outras formas de condutas criminosas, como fraudar vendas com a utilização de sites e dados falsos, onde a vítima adquire uma mercadoria e paga com cartão de crédito e essa mercadoria nunca chega, nem a pessoa consegue mais contatar com o estelionatário, uma vez que seus dados não são verídicos (PEDRA, 2015, p.34,).

Importante destacar que o tráfico de drogas também pode ser considerando um crime cibernético, tendo em conta que os traficantes diariamente utilizam os correios eletrônicos como local de negociar a comercialização de entorpecentes de acordo com o art. 33 da Lei nº. 11.343/2006. Além disso, existe o incentivo ao consumo da droga por meio da internet.

Há várias outras formas de crimes estabelecidas pela internet. Molina (2011, p. 87), aponta como exemplos, os crimes de ameaça prevista no art. 147, do código penal, a injúria (art. 140), calúnia (art. 138, CPB), difamação (art. 139, CPB), racismo (art. 20, da Lei 7.716/89), apologia ao crime (art. 287, CPB), incitação ao crime (art. 286, CPB), lavagem de dinheiro (Lei 9.613/98), e quadrilha ou bando (art. 288, CPB).

O ordenamento brasileiro tem até o presente momento lei de crimes digitais (Lei nº. 12.737/2012) e algumas alterações no Código Penal, o que representa a fragilidade da segurança nos crimes cibernéticos. Além disso, a atuação da polícia judiciária e do Ministério Público como órgãos normativos para a aplicação da referida legislação.

Sobre o trabalho da polícia e do MP, Porto (2009, p. 150), assevera que:

> É um sistema que se dedica à aplicação de faculdades de observação e de conhecimento científico que nos levem a descobrir, defender, e interpretar os indícios de um delito, de molde a sermos conduzidos à descoberta do criminoso, possibilitando à Justiça a aplicação da justa pena.

Como se denota, para que se proceda a uma identificação sobre o verdadeiro criminoso, exige uma investigação minuciosa, exigindo assim empenho e agentes capacitados

para tal, pois a investigação se desdobra de modo diferenciado se compararmos com outros delitos que não exigem tanto para se obter respostas.

No mesmo seguimento, de acordo com Rossini (2011, p. 23) "Nos crimes cibernéticos, o trabalho pericial é de suma importância para demonstrar materialidade e autoria do crime. Via de regra, a perícia é realizada na fase policial, até porque muitas delas necessitam ser feitas imediatamente ou logo após a prática do crime".

Nesse sentido, Nogueira (2014, p. 91), dispõe que:

> É imprescindível que o Direito Penal preste mais dedicação a esses casos, observando a partir do crescimento e das mudanças propostas pelo desenvolvimento das tecnologias e da globalização apresentando uma solução possível para sanar os problemas envolvendo a tecnologia da internet que atinge todas as classes sociais, considerando que a consumação de um crime praticado através da Internet ocorre em todos os lugares em que a rede tem acesso disponibilizado.

Considerando a falta de uma lei específica para os crimes cibernéticos, assim como, a insuficiência das disposições legais previstas na Lei nº 12.737/2012, somado ao crescimento de casos de infiltrações clandestinas através dos computadores, percebe-se a dificuldade a cada dia, no que tange a garantia constitucional do direito à privacidade da pessoa.

Cabe pontuar ainda o grau elevado de acesso à intimidade e na vida privada do indivíduo por meio da internet, assim como o risco consequente de abuso. Em razão disso, percebe-se a relevância do ordenamento jurídico pátrio "confeccionar uma legislação que possa apontar claramente os requisitos para a caracterização dos crimes cibernéticos, os procedimentos e cautelas a serem observados em seu deferimento" (MENDES, 2015, p. 46).

Os estímulos maiores dos criminosos que invadem sistemas operacionais, dados, e celulares é acreditarem que não vão ser descobertos e que suas ações estão escondidas através de uma tela de computador. Assim, eles se mostram mais ousados com suas condutas ilegais por pensar que não serão inibidas.

Logo, as práticas dos crimes virtuais se aperfeiçoam com o tempo, assim como qualquer outro crime e contam com o avanço da tecnologia para facilitar suas práticas criminosas. Assim, nota-se as complexidades em acompanhar todos os mecanismos que a internet disponibiliza para seus usuários, logo com a demanda de acesso na web às pessoas ficam mais vulneráveis as ações criminosas, considerando todo desenfreado avanço do mundo cibernético.

> Essas inúmeras informações estão disponíveis na conta do usuário sem que haja a necessidade de invadir a conta do usuário, ou até mesmo realizar procedimentos de quebra de mecanismos de segurança valendo-se de eventuais vulnerabilidades, tornando-se dessa forma uma investigação invasiva, pois nesse tipo de investigação se faz necessário o que seria invasivo, pois haveria a necessidade de ludibriar os sistemas de bloqueio, e assim praticar a violação da privacidade do sujeito (OLIVEIRA, 2012, p. 98).

Percebe-se na atualidade, que as decisões judiciais acerca da internet e as redes sociais como forma de provas para a persecução penal, ocorrem a partir do empirismo, isto é, da análise do caso concreto, facilitando para que decisões antagônicas possam surgir e contribuir com a aplicação da norma.

O Whatsapp, por exemplo, é um dos instrumentos de comunicação e rede social mais utilizado na atualidade, e não existe para ele uma normatização sobre a forma de seu uso. Nota-se que as decisões judiciais voltadas para essa área apenas bloqueiam de forma temporária o aplicativo, causando prejuízo a todos os usuários do país.

Existem classificações doutrinárias sobre os crimes. Alguns doutrinadores como Jesus (2016, p. 52), que defendem que existem quatro categorias de crimes cibernéticos, os próprios, os impróprios, os mistos e os mediatos, em que sua caracterização vai depender do delito praticado.

O maior problema pertinente aos crimes digitais é que a maioria não tem rastros de provas que levem ao autor da conduta delituosa, seria como a ausência da arma no local do crime. Através de uma invasão gloriosa aos sistemas disponíveis na internet não é possível encontrar vestígio para a incriminação do autor, ou seja, não é possível encontrar arquivos que seriam alterados ou copiados, por exemplo, dessa forma nenhum dano seria identificado. Um crime perfeito, sem traços, e, portanto, sem evidências.

Exatamente por essa condição da maestria como invadem as redes, há a dificuldade em pressupor o razoável número desses delitos. Logo, nota-se a importância da persecução dos transgressores da norma, no entanto, “utiliza-se todas as ferramentas para que não seja necessária a ilegalidade da violação dos direitos fundamentais do acusando, considerando sempre que o direto penal é a última razão na busca do equilíbrio social”. (OLIVEIRA, 2013, p.65).

Com as proposições abordados nesta sessão, claro se mostra a necessidade mais que urgente de medidas eficientes no combate aos crimes cibernéticos, tendo em vista que são crimes que a cada dia se mostram inovados por aqueles que objetivam causar o mal para outros. Isto posto, como inúmeras outras condutas criminosas que sofreram alteração na

legislação dada as diversas nuances que alguns delitos vieram criando, do mesmo modo, é imprescindível a elaboração de novas legislações concernentes ao tema.

Destarte, mais uma vez averigua que uma das decisões primordiais a serem tomadas é uma atuação legislativa quanto aos crimes cibernéticos. Ulteriormente, dissertar-se-á a respeito da responsabilidade do Estado quanto sua competência e inercia na tomada de decisões sobre a criação de nova legislação sobre os crimes virtuais.

3.1 RESPONSABILIDADE DO ESTADO

Nessa seção se explanará sobre a responsabilidade do Estado quanto à tutela protetiva dos direitos individuais e coletivos e quais posicionamentos o Estado está tendo para coibir os crimes virtuais. A corrente seção tem por finalidade abordar qual é a capacitação jurídica do Estado para atuar no combate aos crimes cibernéticos, sua responsabilidade e sua atuação.

Para corroborar para a composição do que será exposto a seguir, recorreu-se a pesquisas em livros, pesquisas bibliográficas, pesquisas em artigos científicos e se procedeu à leitura da Constituição da República Federativa do Brasil de 1998, e Código Penal.

A priori, a capacitação jurídica voltada para os crimes cibernéticos é de suma relevância, principalmente para a aplicação do direito e justiça, considerando que a tecnologia nos envolve a cada dia, possibilitando um contato maior com o mundo. Assim, o conhecimento da legislação deve ser associado ao conhecimento do mundo virtual para que os profissionais sejam capazes de resolver os impasses relacionados aos crimes praticados na internet.

Sabe-se que os mecanismos eletrônicos, resguardam vários bens jurídicos, como por exemplo, a intimidade, liberdade, saúde e etc. Corroborando com essa perspectiva vale mencionar que:

> “Aparecem os crimes virtuais e, com eles, novos bens jurídicos, aos quais a ordem constitucional precisa proteger. Há um impacto da sociedade da informação na ordem constitucional, o que gera consequências na esfera penal” (MONTEIRO NETO, 2008, p. 6; OLIVEIRA, 2013, p. 11)

À vista disso, com as novidades no mundo informacional gerou-se a inevitabilidade do reconhecimento de uma revolução informacional. No pensamento de Beneyto (1997, p. 15), “para considerar-se plenamente cidadão, o homem contemporâneo

precisa dispor de fontes informacionais que lhe permitam conhecer o que se passa e, em seguida, formar juízos sobre os acontecimentos".

Por ser um direito fundamental regido pela Constituição da República Federativa do Brasil de 1998, o direito à informação, como vários outros direitos, precisa ser resguardado nas diversas áreas jurídicas, uma vez que tal direito está vinculado à democracia atual, ainda mais se observar as inúmeras avalanches de notícias e *fakes News* que circulam a cada segundo. Se considerar a atual situação na qual se está vivendo, uma pandemia, que afetou de modo repentino o cotidiano de todos, resta somente recorrer às inovações tecnológicas para a realização do essencial.

Mister é a necessidade de intervenção do Estado na utilização dos meios tecnológicos de produção e difusão da informação, contudo, tal ingerência não pode ser desregrado, pois, mesmo que haja essa necessidade de intervenção, não se pode esquecer um princípio constitucional norteador para balizar a interferência quando necessária, qual seja, o princípio da intervenção mínima. Assim sendo, tais intermédios devem ser pontuais nas inibições de práticas nocivas causadas pelo uso inconsequente da tecnologia.

Muitas condutas delituosas, as quais são praticadas com o suporte da internet ou por meio de um computador, em sua grande maioria, carece de uma tipificação específica, o que como outrora mencionado, dificultam demasiadamente uma medida punitiva de tais pessoas.

Em conformidade com o mencionado, os escritores infracitados discorrem sobre alguns dos princípios norteadores do direito penal, vide:

> "A Carta de 1988 destaca o princípio da dignidade da pessoa humana como norteador do Estado Democrático de Direito. Nesse ínterim, partindo da premissa de que o Direito Penal amolda-se ao perfil traçado pela Constituição, destacam-se princípios constitucionais-penais, como os princípios da legalidade ou da reserva legal, da anterioridade, da taxatividade e da territorialidade". (MONTEIRO NETO, 2008, p. 85; SOUZA NETO, 2009, p. 58)

Não resta qualquer dúvida de que, para reprimir delitos cibernéticos, o reconhecimento legal de tais condutas é imprescindível, observando o princípio da legalidade e também o princípio da taxatividade, o qual compele que a norma penal incriminadora seja exata, e caso não observe tal determinação, corre o risco de perder a eficácia.

> Vale ressaltar que o Direito Penal não vem acompanhando as mudanças ditadas pela explosão tecnológica, operada desde a última metade do Século XX. Tais mudanças já estão preconizadas na Constituição da República do

> Brasil, de forma que se buscou proteger os interesses envolvidos contra os avanços da utilização dos meios informáticos em práticas que ferem a dignidade da pessoa humana, assimilando as nuances da nova realidade social. Assim, a tutela penal de tais interesses faz-se extremamente necessária, vez que a falta de regulamentação que reprima atos que vão de encontro à nova ordem social torna instável a sustentação desse novo modelo (SOUZA NETO, p. 134-135).

Destarte, ante todo exposto, o Estado detém todos os meios para que os crimes cibernéticos possam ser drasticamente reduzidos. Logo, a inércia do Estado em adotar novas mudanças no ordenamento jurídico penal só aumenta ainda mais a impunidade e a "segurança" dos criminosos.

Por fim, restou claro que o Estado é parte legítima para atuar em defesa dos direitos dos cidadãos, revendo leis e tipificações obsoletas e, ainda reconhecendo e materializando penalmente novas condutas que são diariamente praticadas, não podendo o Estado ficar a parte dos casos recorrentes existentes.

Com o que foi esclarecido, os resultados encontrados contribuem para a apresentação da resposta para a problemática exposta inicialmente, uma vez que, a partir do instante em que se concluí que o Estado é parte legítima para atuar em defesa dos direitos dos cidadãos, este tem o dever de zelar e garantir esses direitos, não importando o quão empenho exigirá dos representantes da nação, tendo em vista que por estar em um Estado democrático de direito dois de seus fundamentos de respalda em garantir dignidade da pessoa humana e salvaguardar valores sociais que forem afrontados. Sucessivamente, elucidar-se-á sobre uma análise pormenorizada das legislações existentes que versam sobre cibercrimes.

4. ANÁLISE DOS CRIMES CIBERNÉTICOS SOB A ÉGIDE DA LEI 12.737/2012 E OUTRAS PREVISÕES LEGAIS.

Este capítulo será dedicado ao estudo e análise das legislações e decretos concatenados com os cibercrimes, seus respaldos jurídicos; época de criação; eficácia; vigência e quais elementos foram considerados pelo legislador para elaboração destas Leis e decretos, quais condutas foram ponderadas para tipificar o núcleo do tipo para se considerar crime virtual.

Tem como finalidade analisar os artigos que possuem uma abrangência eficaz na atualidade, tal qual as lacunas que tais leis possuem, para que se possa entender quais são as leis aplicadas ao caso concreto. Para uma maior elucidação do tema buscou-se fazer a leitura das leis, as quais serão mencionadas abaixo, buscou-se pesquisar em artigos científicos, bem como as pesquisas bibliográficas, por fim, perscrutou-se jurisprudências sobre os crimes cibernéticos, onde se teve êxito de encontrar dois acórdãos proferidos no Supremo Tribunal Federal dos Ministros Marco Aurélio e Gilmar Mendes.

Em face do exposto nas seções anteriores deste trabalho, pode-se observar que a legislação vigente sobre os crimes cibernéticos é a Lei nº 12.737/2012 intitulada como "Carolina Dieckmann", e diante disso, observa-se que essa legislação é escassa e insuficiente, pois inúmeros delitos que são praticados através do uso da internet não estão tipificados.

Apesar disso, vale ressaltar que, antes da previsão legal da lei supramencionada, não havia dispositivo legal específico que regulamentasse condutas criminosas no âmbito cibernético, havendo somente leis esparsas que eram aplicadas a certos casos. À vista disso, convém ressaltar o grande passo que foi dado com a elaboração e aprovação dessa lei, pois com ela abriu-se a possibilidade de que fossem rechaçadas essas condutas.

Outrossim, por ter sido criada anos atrás, verifica-se que grande parte dos crimes tipificados estão em desuso, em razão das rápidas inovações dos criminosos. A Lei nº 12.737/2012, é bem limitada em suas tipificações, sendo que possui apenas 04 (quatro) artigos. Tal lei foi criada com objetivo de alterar o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, devida as recorrências de crimes cibernéticos há época. Dessa forma depreende-se que, pela insuficiência de legislação, caso ocorra um ataque de crimes cibernéticos poderá afetar drasticamente as vidas de inúmeras pessoas, levando em consideração que grande parte da população tem acesso à internet, e ainda, esses criminosos teriam grandes chances de saírem imunes juridicamente, ou ainda, sofrer sanções insignificantes perto do caos que esses crimes podem causar.

Ao fazer breve leitura da legislação acima mencionada, nota-se que há poucas tipificações sobre a conduta que o indivíduo precisa cometer para se considerar um crime cibernético e sofrer a devida sanção, consequentemente, o legislador deixou margem para uma vasta interpretação, no entanto, como no direito penal não é admissível que se faça interpretação e analogia *in malam partem* como já especificado no capítulo anterior, acaba culminando pela impunidade dos infratores.

Nesse sentido, como já demonstrado outrora, as condutas que um indivíduo pode cometer com o uso de um computador ou de outros objetos digitais móveis são inúmeros, não se restringindo aos que estão previstos.

O artigo 154-A, *caput*, da Lei nº 12.737/2012, prevê que:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 2012, [s.p]).

Nessa senda, denota-se que o dispositivo legal que foi inserido no Código Penal está sendo constantemente alvo de discussão, em razão das inúmeras lacunas interpretativa que se pode obter deste dispositivo. Observando que o legislador não deu a clareza que se exige para se caracterizar estes crimes.

Cumpre salientar que, existem outras leis que abordam temas a respeito do mundo cibernético, todavia as questões abordadas estão muito aquém do imaginável. A Lei nº 12.735/2012 que trata sobre a instalação de delegacias especializadas, onde em seu artigo 4º de um total de 06 (seis) artigos, prevê:

> Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado (BRASIL, on-line, 2012).

Na teoria, há uma legislação onde os crimes cibernéticos deveriam ser investigados de forma distinta e em delegacias especializadas. Contudo, na prática, tais criações de delegacias fogem a realidade.

Concernente a Lei nº 12.965/2014 esta prevê sobre o marco civil da internet, pois trata dos princípios, garantias, direitos e deveres para o uso da Internet no Brasil, da mesma forma, não trouxe nenhuma novidade quanto à tipificação de novas condutas criminosas.

Todavia, acarretou em novas diretrizes para a atuação do Estado, estabelecendo normas para proteger os dados pessoais e a privacidade dos usuários no ambiente online. Em seu artigo 3º dispõe que:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - **preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas**; VI - **responsabilização dos agentes de acordo com suas atividades, nos termos da lei** (BRASIL, 2014, grifo nosso).

Como se denota, a preservação da estabilidade, segurança e funcionalidade da rede está como um dos princípios previsto nessa lei, todavia, diante os dados estatísticos que será posteriormente apresentado, pode-se verificar que os casos existentes são exorbitantes, concluindo que essa segurança só está no plano teórico.

Além do mais, na mesma Lei nº 12.965/2014, está previsto a responsabilização dos agentes de acordo com suas atividades, nos termos da lei, entretanto, observa-se o contrário, tendo em vista que a legislação vigente quanto aos cibercrimes está obsoleta, não havendo uma eficácia em sua aplicação.

Quanto à Lei nº 13.709/2018, esta trata da Lei Geral de Proteção de Dados Pessoais - LGPD48, entretanto, o nível de articulação e de normatização das instituições brasileiras nos temas relacionados à segurança cibernética ainda é muito insuficiente.

> Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; III - sugerir ações a serem realizadas pela ANPD; IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e V - **disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população** (BRASIL, 2018, grifo nosso).

Conforme previsto na Lei Geral de Proteção de Dados Pessoais, um dos objetivos é propagar o conhecimento sobre a proteção de dados pessoais e da privacidade à população. Todavia, observa-se que muitos têm acesso à internet, porém, poucos têm o real

conhecimento de como proteger seus dados pessoais. Segundo matéria divulgada no jornal G1, onde demonstrou uma estatística divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE) em 2018[1], na qual ficou evidente que a maioria das pessoas que não utilizavam a internet alegou não saber como navegar, e deste desconhecimento fortuitamente tem gerado grandes transtornos na vida dos usuários da internet.

Vale mencionar o Decreto 9.637/2018, o qual versa sobre a Política Nacional de Segurança da Informação (PNSI), e em seu artigo 2º, ficou definido quais informações da segurança esse decreto abrangeria, sendo:

> I - a segurança cibernética; II - a defesa cibernética; III - a segurança física e a proteção de dados organizacionais; e IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação (BRASIL, 2018 [s. p]).

Partindo do pressuposto que a normatização das condutas ilícitas praticadas ciberneticamente é o primeiro passo para o combate de tais crimes, nesse quesito, o ordenamento jurídico brasileiro tem se mostrado de forma omissa, posto que, por mais que nos últimos anos têm se promulgado inúmeros decretos e leis, nenhum deles tratou de forma objetiva quais condutas seriam reprimidas deixando margem para ampla interpretação.

Ainda, no artigo 4º do mesmo decreto estabeleceu-se os objetivos da PNSI, sendo eles:

> I – contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação das ações de segurança da informação, observados os direitos e as garantias fundamentais; II – fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança da informação; III – **aprimorar continuamente o arcabouço legal e normativo relacionado à segurança da informação** (BRASIL, 2018, grifo acrescido).

Nota-se que, existe uma previsão somente para aprimorar o arcabouço legal e normativo da segurança da informação. Com isso, percebe-se que atualmente somente com informações sobre a segurança cibernética não está sendo suficiente para reduzir os cibercrimes, necessitando uma atuação normativa mais específica e que trate de outros inúmeros crimes que podem ser definidos como tal.

---

[1] SIQUEIRA, Daniel. Em 2018, quase 46 milhões de brasileiros ainda não tinham acesso à internet, aponta IBGE. G1, Rio de Janeiro, 29/04/2020. Disponível em <https://g1.globo.com/economia/tecnologia/noticia/2020/04/29/em-2018-quase-46-milhoes-de-brasileiros-ainda-nao-tinham-acesso-a-internet-aponta-ibge.ghtml>. Acesso em: 26 maio. 2020.

Em continuidade, recentemente, o atual Presidente da República, Jair Messias Bolsonaro promulgou o decreto nº 10.222/2020, onde foi aprovada a Estratégia Nacional de Segurança Cibernética. Entretanto, tal decreto terá validade até 2023, um prazo extremamente transitório para se colocar em prática o que restou previsto em tal decreto. Na parte introdutória restou previsto que "[...] promover um ambiente participativo, colaborativo e seguro, entre as organizações públicas, as instituições privadas, a academia e a sociedade, por meio do acompanhamento contínuo e proativo das ameaças e dos ataques cibernéticos [...]" (BRASIL, 2020).

Desta feita, verifica-se que todos os decretos que foram promulgados até o presente momento ficaram restringidos somente em questões de distribuição de competências e algumas "promessas" para aprimorar o arcabouço legal sobre os cibercrimes, contudo, verifica-se que essas "promessas" permanecem ano após ano no plano especulativo.

Partindo para uma análise de estatísticas, segundo informações apresentadas no próprio Decreto nº 10.222/2020, em 2018:

> "89% dos executivos foram vítimas de fraudes cibernéticas; - As questões de segurança desestimulam o comércio eletrônico; - Em 2017, os crimes cibernéticos resultaram em US$ 22.500.000.000,00 (vinte e dois bilhões e quinhentos milhões de dólares) de prejuízo; e o Brasil é o 2º com maior prejuízo com ataques cibernéticos" (BRASIL, 2020).

Destarte, o cenário de constantes ocorrências de crimes cibernéticos está causando prejuízos exponenciais, conforme os números acima expostos. Dessa forma, inúmeros executivos sofreram alguma fraude cibernética afetando drasticamente a economia do nosso país. Dito isso, com a devida vênia, é um despautério um país onde 98% da população[2] possui acesso às redes móveis de internet, liderar o 2º lugar com maior prejuízo com ataques cibernéticos e não tendo uma legislação mais efetiva.

Aurélio (2019, on-line), em sede de Recurso Extraordinário, deixou manifesto a importância do estudo aprimorado dos crimes cibernéticos, dada a especificidade de tais delitos, deixando claro que não há que se tratar dos crimes cibernéticos com o mesmo procedimento que são tomados no cometimento de crimes ocorridos no ambiente físico em virtude das peculiaridades que os delitos cibernéticos exigem. Mais uma vez, ficou evidente que os crimes virtuais são facilmente cometidos de modo desmedido.

[2] Dados obtidos no Decreto nº 10.222/2020.

Ainda, corroborando com a mesma ideia, em sede de acórdão Mendes (2018, on-line), este evidenciou que sem dúvida alguma as consequências que os crimes cibernéticos podem causar nas vidas das vítimas são imensuráveis, manchando a honra e o decoro destas.

De acordo com o Ministro Luís Barroso (2014, p.56) "A honra é um direito da personalidade previsto constitucionalmente, sendo necessária a proteção da dignidade pessoal do indivíduo e sua reputação". Desta feita, compreende-se que um dos campos mais afetados é o psicológico das vítimas, para que esses crimes cibernéticos não ocasionem outras tantas vítimas, como tem ocorrido diariamente é necessário um posicionamento do poder legislativo.

Em suma, mais uma vez, observa-se que existem algumas Leis que trataram das condutas que são praticadas virtualmente, todavia, ficou claro que nenhuma das leis possui uma tipificação contundente com as constantes práticas de crimes cibernéticos. Também restou comprovada que a internet é um meio bastante difícil de monitorar, porém não é impossível, bastando que o Estado use de suas estruturas para amenizar as ações dos delituosos.

Com a míngua de leis que existem sobre os crimes virtuais, fez com que o Brasil fosse um dos países que sofreram maior número de ataques on-line na América Latina, mais precisamente, 54[3] % dos ataques ocorreram dentro do nosso país, é de se considerar tais dados alarmantes, e isso se dá pela legislação mal elaborada.

Por fim, durante a elaboração deste trabalho e considerando tudo que foi estudado, foi possível selecionar as principais dificuldades para se combater os crimes cibernéticos, além dos expostos acima, são eles: falta de inclusão de inúmeras condutas criminosas no Código Penal, ou em uma elaboração específica de lei sobre cibercrimes; não há um incentivo a especialização em segurança cibernética para as empresas, quanto para a população em geral, pois em muitos casos o desconhecimento de manuseio da internet facilita a ação do criminoso; falta de investimento na especialização de agentes para que atuem na linha de frente nas delegacias especializadas para solução mais célere dos casos.

Com os resultados obtidos verifica-se que não é pequena a incidência de crimes cibernéticos ocorridos no país, e esse número se dá pela ineficácia das leis já existentes, tal qual a falta de legislação que aborde novos conteúdos do mundo virtual. Verifica-se também a vaga tentativa do legislador em tentar tapar sua omissão ao criar decretos e leis que pouco contribui para uma atuação eficiente para penalizar os infratores.

[3] Dados obtidos no Decreto nº 10.222/2020.

Averigua-se também que, a grande questão existente quando se refere aos crimes cibernéticos não é a falta de estrutura do Estado, mas sim o descaso manifestadamente do Estado, representado pelas autoridades competentes, bem como a falta de compromisso destes para colocar em ação o poder que lhes foi atribuído para coibir esses crimes. Ulteriormente, proceder-se-á para as considerações finais deste trabalho, onde se fará uma reflexão sobre os problemas e resultados encontrados.

5 CONSIDERAÇÕES FINAIS

Após o estudo acerca do tema proposto, ficou manifesto o atingimento dos objetivos apresentados, uma vez que restou confirmado que com a evolução veio a estabelecer um Estado democrático de direito, bem como ficou caracterizado que as condutas delitivas cometidas pelos infratores podem sim ser considerada como crime, posto que os requisitos foram preenchidos. Do mesmo modo, constatou que a internet tem transformado a vida de grande maioria da população do nosso país, dada a sua grande acessibilidade que esta proporciona, e assim, como tem sido palco de crimes mais que rapidamente precisa da atenção do Estado.

Ainda, constatou que, desde o surgimento da internet surgiram inúmeros crimes das mais variadas formas, porém muitas dessas condutas não estão previstas em nenhuma legislação. Ato contínuo, restou incontestadamente esclarecido que o Estado tem a responsabilidade de zelar pelos direitos daqueles que estão em seu território, pois lhes foi conferido tal poder pela organização Estatal que se tem. Além do mais, com o estudo das legislações pertinentes sobre o tema mundo virtual e crimes virtuais, verificou-se que o país ainda tem que tomar consideráveis iniciativas para reprimir e tipificar os crimes cibernéticos.

Salienta-se que, um dos problemas para o desenvolvimento deste trabalho se recostou ao final da elaboração deste trabalho, considerando impossibilidade de buscar material didático para pesquisas na biblioteca da Faculdade, considerando o momento atípico em que se está enfrentando, uma pandemia, com isso, foi preciso buscar alternativas que corroborassem para o resultado esperado.

Destarte, dada às pesquisas que foram anteriormente realizadas para a elaboração dos objetivos gerais e específicos, pode-se afirmar que os resultados alcançados foram esperados, visto que, conseguiu-se chegar a resposta da problemática apresentada, pois, pela grande incidência de casos dessa natureza, já esperava que fosse possível existir uma lacuna em algum lugar do ordenamento jurídico que justificasse tantas vítimas e tantas impunidades.

Todavia, como sendo acadêmica de direito, é enfático dizer que o resultado encontrado infelizmente não foi exultante como esperado, pois, como uma futura militante pelos direitos que nos são garantidos pela Constituição da República Federativa do Brasil de 1988, sofre-se um desapontamento ao perceber que existe uma falta de comprometimento do Estado. Quando se diz Estado, refere-se aos seus representantes, mais precisamente dos três poderes (legislativo, executivo e judiciário), pois estes têm o poder-dever de atuação e não tem cumprido com suas atribuições satisfatoriamente, deixando a mercê os direitos de muitas

vítimas que sofreram ações delituosas no âmbito cibernético, ao não criar novas Leis sobre cibercrimes, ao deixar de administrar assuntos de interesse do povo, e ao agir com vistas grossas com os casos que surgem.

Através dos estudos realizados, seria de grande contribuição se os leitores a partir da presente obra se desafiassem a elaborar novos estudos, podendo se enveredar em pesquisar sobre vastos temas existentes sobre o mundo cibernético sobre o modo de investigação dos agentes e também como as provas são obtidas para a comprovação da materialidade e da autoria de um crime cibernético dentre outros.

Por fim, os resultados alcançados corroboram no âmbito jurídico, no sentido de que, para ajudar na prevenção desses crimes, o profissional do direito, com seu vasto conhecimento sobre a lei, pode ajudar a sociedade em geral trazendo à tona alertas que ajudarão a população a se desvencilhar das artimanhas dos criminosos, como por exemplo, fazer com que a população tenha um discernimento maior do que pode ser garantido por lei e o que são ofertas enganosas por não ter respaldo jurídico.

REFERÊNCIAS

ACQUAVIVA, Marcus Cláudio. **Teoria geral do Estado**: 3. Ed.- Barueri, SP: Manole, 2010.

ÁVILA, Maribel Chagas de Internetês. **uma anamnese da história da escrita**. Dissertação de mestrado UFMT, 2008.

Atuação_do_MP_no_combate_aos_crimes_cibernéticosinfancia_e_juventude. Disponível:em:https://www.cnmp.mp.br/portal/images/Palestras/Atua%C3%A7%C3%A3o_do_**MP_nocombate_aos_crimes_cibernéticos**infancia_e_juventude.pdf. Acesso em: 12 mar.2020.

BARATTA, Alessandro. **Criminologia crítica e crítica do direito penal introdução à sociologia do direito penal**: 3. ed. Rio de Janeiro: Revan, 2002.

BARROSO, Luís Roberto. **Estado, Sociedade e Direito: Diagnósticos E Propostas para o Brasil**. In: XXII Conferência Nacional dos Advogados. Rio de Janeiro, 2014.

BENEYTO, J. **Informação e sociedade: os mecanismos sociais da atividade informática**. Petrópolis: Vozes, 1997.

BITENCOURT, Cezar Roberto. **Tratado de direito penal**: parte geral, 1. – 18 ed. Ver. Ampl. e atual.- São Paulo: saraiva, 2012.

_____, Cezar Roberto. **Tratado de direito penal: parte geral:** 1. 21 ed. São Paulo: Saraiva, 2015.

BRASIL, Lei nº. 10.764 de 12 de novembro de 2003. Altera a Lei nº 8.069, de 13 de julho de 1990, **que dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/L10.764.htm. Acesso em: 03 set. 19.

_____, Lei nº. 8.069/1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**.Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 30 ago. 19.

_____, Supremo Tribunal Federal. **Recurso Extraordinário com Agravo nº 1245982 / DF**. Recorrente: Danielle Patrícia Costa De Souza. Recorrido: Ministério Público Federal. Brasília, DF, 20 de novembro de 2019. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/despacho933929/false. Acesso em 02 jun. 2020.

_____, Supremo Tribunal Federal. **Recurso Extraordinário com Agravo nº 1066401 / DF.** Relator Ministro Gilmar Mendes. Recorrente: Elinay Almeida Ferreira De Melo Adv.(A/S): Mario Antonio Lobato De Paiva. Recorrido: Maria Zuila Lima Dutra. Brasília, DF, 30 de novembro de 2018. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/despacho933929/false. Acesso em 02 jun. 2020.

_____,BRASIL. **Decreto-Lei nº 3.689**, de 3 de outubro de 1941. Código de Processo Penal. Planalto. Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em 20 fev. 2020.

_____, BRASIL. **Decreto-Lei nº 10.222, de 05 de fevereiro de 2020**. Estratégia nacional de segurança cibernética. Diário Oficial da União. Brasília, DF. Publicado em 06/02/2020.órgão: atos do poder judiciário. Ed. 26. Pg. 06. Seção 1. Disponível em: http://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 05 maio 2020.

_____, BRASIL. Lei nº 12.737, de 30 novembro de 2012. **Tipificação criminal de delitos informáticos**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12 mar.2020.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**: 1. ed. Rio de Janeiro: Brasport, 2014.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais.** 2. Ed. Rio de Janeiro: Lumen Juris, 2003.

CASTRO, Ian. **O que é Home page e Landing page?** Disponível em: https://www.intermidias.com.br/seo-otimizacao-de-sites/o-que-e-home-page-landing-pages/. Acesso em: 12 mar.2020.

CHAVES, Antônio apud SILVA, Rita de Cássia Lopes. **Direito Penal e Sistema Informático**, 2017.

Correio Eletrônico. Site: https://conceitos.com Autor: Editorial Conceitos. Publicado: 24/11/2017. Disponível em: https://conceitos.com/**correio-eletronico**/ São Paulo, Brasil. Acesso em: 12 mar.2020.

DALLARI, Dalmo de Abreu. **Elementos de Teoria Geral do Estado**. – 33. Ed. – São Paulo: saraiva, 2016.

JESUS, Damásio de; MILAGRE, José Antonio. **MANUAL DE CRIMES INFORMÁTICOS.** São Paulo: Saraiva, 2016.

JUNQUEIRA, Gustavo. **Manual de direito penal.** Gustavo Junqueira, Patrícia Vanzolini. – São Paulo: saraiva, 2013.

MONTEIRO NETO, J. A. **Aspectos Constitucionais e Legais do Crime Eletrônico**. Fortaleza, 2008.

MORAN, José M.; ALMEIDA, Maria E. B. (2005). **Integração das Tecnologias na Educação. Salto para o futuro. Secretaria de Educação à Distância**. Brasília: MEC, SEED.

NOGUEIRA, Sandro D'Amato**. Vitimologia: lineamentos à luz do art. 59, caput, do Código Penal brasileiro**. Jus Navigandi. Teresina, a. 8, n. 275, 8 abr. 2014. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=5061. Acesso em: 30 ago. 2019.

NUCCI, Guilherme de Souza. **Manual de direito penal**. 15 ed. – Rio Janeiro: Forense, 2019.
Lei 10.764
OLIVEIRA, J. C. **O cibercrime e as leis 12.735 e 12.737/2012. Monografia** (Conclusão de curso). Departamento de Direito da Universidade Federal de Sergipe. Universidade Federal de Sergipe. São Cristóvão. 2013. Disponível em: <https://www.conteudojuridico.com.br/pdf/cj045489.pdf>. Acesso em: 03 set. 2019.

PEDRA Jorge, Alline. **Em busca da satisfação dos interesses da vítima penal**. Rio de Janeiro: Lúmen Júris, 2015.

PIAGET, Jean. **Para Onde Vai a Educação**. 16 ed. Rio de Janeiro. José Olympio, 2002.

POLEGATTI, B. C.; KAZMIERCZAK, L. F. **Crimes Cibernéticos: O Desafio do Direito Penal na Era Digital**. Ourinhos, 2012.

PORTO, Gilberto apud OPILHAR, Maria Carolina Milani. **Criminalística e Investigação Criminal.** 2009.

ROQUE, Sérgio Marcos. **Criminalidade informática: crimes e criminosos do computador.** São Paulo: ADPESP Cultural, 2007.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2012.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2011.

SOUZA, Neto, P. A. de. **Crimes de Informática**. Itajaí, 2009.

VIANA, Marco Túlio apud CARNEIRO, Adeneele Garcia. **Fundamentos de direito penal informático. Do acesso não autorizado a sistemas computacionais**. Rio de Janeiro: Forense, 2003.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira**. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação.** 2. ed. Rio de Janeiro: Brasport, 2012.

XAVIER, Antônio C. S. **O Hipertexto na Sociedade da Informação: a constituição do modo de enunciação digital**. Tese de doutorado Unicamp, 2015.