FACULDADES DOCTUM DE CARATINGA

ANDRESSA CRISTINA MACHADO ALVES

OS CRIMES CIBERNÉTICOS E A (IN) EFICÁCIA DA LEI 12.737/12

BACHARELADO

EM

DIREITO

CARATINGA – MG

2019

ANDRESSA CRISTINA MACHADO ALVES

OS CRIMES CIBERNÉTICOS E A (IN) EFICÁCIA DA LEI 12.737/12

Monografia apresentada ao Curso de Direito das Faculdades Doctum de Caratinga, como exigência parcial à obtenção do grau de Bacharel em Direito.
Áreas de concentração: Direito Penal e Direito Constitucional.
Orientador: Prof. Luiz Eduardo Moura Gomes.

.

CARATINGA - MG

2019

rede de ensino DOCTUM	FACULDADES DOCTUM DE CARATINGA	FORMULÁRIO 9
	TRABALHO DE CONCLUSÃO DE CURSO	
TERMO DE APROVAÇÃO		

TERMO DE APROVAÇÃO

Trabalho de Conclusão de Curso **Os crimes cibernéticos e a (IN)eficácia da lei 12.737/12**, elaborado **Andressa Cristina Machado Alves** foi aprovado por todos os membros da Banca Examinadora e aceita pelo curso de DIREITO da FACULDADES DOCTUM DE CARATINGA, como requisito parcial da obtenção do título de

BACHAREL EM DIREITO.

Caratinga 09 de JULHO 2019

Prof. Luiz Eduardo Moura Gomes

Prof. Neuber Teixeira dos Reis Junior

Prof. Rafael Soares Firmino

RESUMO

O presente trabalho irá apresentar alguns conceitos sobre internet, computadores e pontos que abordam estes dois temas, como por exemplo, a grande expansão tecnológica da sociedade de informação. Ainda se tem como alvo apontar as falhas existentes na Lei 12.737/12, conhecida popularmente como “Lei Carolina Dieckmann”, criado com o intuito de combater crimes cibernéticos. Com a conquista cibernética, muitas barreiras vêm sendo quebradas, como por exemplo: a interação simultânea com pessoas a milhares de quilômetros, desenvolvendo, assim, o nível cultural. Contudo, abre espaço também para, romper com direitos e princípios conquistados há muito tempo, como a privacidade e a intimidade. O Brasil. Preocupado com essa crescente inovação, buscou criar leis que protegessem seus cidadãos, porém, ao analisar a Lei 12.737/12, ficou evidente que ainda não estamos preparados para tal, levantando, assim, a obrigação de estudarmos com mais afinco o assunto, objetivando aperfeiçoar nossa proteção. Ainda sim existem poucas leis que punem os crimes praticados através da internet, as duas principais são: a lei 12.737 de novembro de 2012 e a lei 12.965 de abril de 2014 conhecidas também por lei Carolina Dieckmann e Marco Digital, respectivamente.

Palavras-Chave: (In) eficácia; Crimes Virtuais; Tipificação; Internet.

A minha mãe, Maria de Fátima, que me mostrou que das qualidades de um ser humano as maiores são a dignidade e o respeito. E a toda minha família pelo integral apoio e compreensão.

AGRADECIMENTOS

Agradeço a Deus, por ter guiado meus passos até aqui, sobretudo naqueles momentos que mais precisei, sendo que, sob sua guarda segui até o presente momento e continuarei caminhando em sua graça. Agradeço ainda a minha mãe, Maria de Fátima, pois tudo que sou que conquistei e irei conquistar é devido ao seu incontável exemplo de vida. Agradeço também aos meus amigos, que sempre estiveram comigo nessa caminhada de conhecimento, tanto aqueles que colaboram no meu aprendizado junto ao meu estágio e durante todo o curso bem como aqueles que estiveram em vários momentos presentes na minha vida. Em especial as amigas que fiz nesses cinco anos de curso: Lídia, Joice, Nivea, Letícia, Jéssica, Dayane e Gisele. E também, não obstante, ao meu querido orientador, Professor Luiz Eduardo Moura Gomes, pela atenção, paciência e carinho com que me transmitiu suas orientações e conhecimentos.

“- A gente só conhece bem as coisas que cativou, disse a raposa. Os homens não tem tempo de conhecer coisa alguma. Compram tudo prontinho nas lojas. Mas como não existem lojas de amigos, os homens não têm mais amigos. Se tu queres uma amiga, cativa-me! Os homens esqueceram a verdade, disse a raposa:

- Mas tu não a deves esquecer.

- Tu te tornas eternamente responsável por aquilo que cativas"

(O Pequeno Príncipe - Antoine de Saint-Exupéry)

SUMÁRIO

INTRODUÇÃO

O presente projeto de pesquisa tem como tema ‘’os crimes cibernéticos e a (in) eficácia da lei 12.737/06‘’ tendo em vista que os crimes do meio virtual vêm crescendo de forma alarmante. Tratará em específico sobre a fragilidade da Lei 12.373/12, tendo como principal objetivo apontar a má elaboração do artigo 154-A, caput, que foi acrescentado ao Código Penal Brasileiro através da Lei 12.373/12, no que diz respeito à violação de medida de segurança de dispositivo informático, evidenciando a lacuna existente e o risco presente em relação à aplicação da referida Lei. Tal dispositivo legal não demonstra, bem como não deixa claro sobre a tipificação de delitos informáticos, e por haver essa lacuna, estaria prejudicando a condenação daquele que praticasse tal ato delituoso.

Nesse sentido, existem poucas leis que punem os crimes praticados através da internet, as duas principais são: a lei 12.737 de novembro de 2012 e a lei 12.965 de abril de 2014 conhecidas também por lei Carolina Dieckmann e Marco Digital, respectivamente, sendo esta última considerada um grande avanço no ordenamento jurídico. Em um primeiro momento, podemos acreditar que estamos protegidos por elas, mas infelizmente não é bem assim, pois se formos analisar constataremos que não só os crimes são tratados de maneira superficiais como as penas são ineficazes.

A lei nº 12.737 foi criada com o objetivo de penalizar os crimes praticados no meio virtual. A lei inseriu os arts. 154-A e 154-B no Código Penal, criando a “invasão de dispositivo informático” e regulamentando sua ação penal.

Porém fica evidentemente claro que a redação quanto a tipificação dos crimes virtuais foi infeliz e está é repleta de falhas, mais especificamente em seu artigo 154-A.

O Estado deve atuar de forma que não exista lacunas em relação à aplicação de suas Leis, em especial, as Leis que definem crimes devem ser precisas, deixando claro a conduta que objetivam punir. Em razão do princípio da legalidade não é admitido no Ordenamento Jurídico a existência de leis vagas e imprecisas, ou seja, Leis estas que não deixam perfeitamente delimitado o comportamento a ser incriminado e punido, podendo a ser a estes elencado o nome de “tipos penais abertos”.

No entanto, por mais que seja possível a investigação dos crimes cometidos no âmbito virtual, a incriminação de tais crimes seria quase que impossível pelo fato de

inexistir lei específica que os incrimine. E neste caso, não seria cabível o uso da analogia do Código Penal Brasileiro, tendo em vista que a analogia *in malan partem* é vedada pelo mesmo, como discorre o Professor Túlio Viana:

> Não há, porém, como o intérprete sanar o problema, pois a analogia *in malam partem* é vedada no Direito Penal pelo princípio constitucional da legalidade. Espera-se, pois, que o legislador corrija esta lacuna por meio de uma nova lei.

A hipótese a ser investigada é, o Estado em executar o *ius puniend,* precisa assegurar aos usuários dos meios virtuais uma legislação capaz de punir e incentivar que novas práticas não venham acontecer.

O presente trabalho acadêmico terá como marco teórico a base de raciocínio do Professor Rogério Greco, onde este discorre em seu livro Código Penal Comentado de 2012:

> "Entendemos que essa exigência, isto é, a violação indevida de mecanismo de segurança, impede que alguém seja punido pelo tipo penal previsto pelo art. 154-A do diploma repressivo quando, também, mesmo indevidamente, ingresse em dispositivo informático alheio sem que, para tanto, viole mecanismo de segurança, pois que inexistente".[1]

Tal entendimento encontra-se substrato à confirmação da hipótese em que o caput do artigo o qual dispõe que o crime ocorrerá caso o agente viole mecanismo de segurança de dispositivo informático alheio, poderá ser uma brecha para a prática do delito, uma vez que nem todos os dispositivos informáticos possuem *firewall* ou senha.

Nesse sentido a monografia será dividida em três capítulos distintos. No primeiro serão apresentados princípios do Direito Penal sobre a ótica Constitucional.

No segundo capítulo será abordada a aprovação da lei e suas implicações legais. E por fim, no terceiro e último capítulo, o tema Crime Cibernético será conceituado e analisando quanto aos danos que uma vítima de tal conduta poderá sofrer.

[1]GRECO, Rogério. **Código Penal Comentado**. 7. ed. Niterói: Impetus, 2013. p. 444.

CONSIDERAÇÕES CONCEITUAIS

Antes de adentramos ao tema principal do nosso trabalho de conclusão de curso, entendemos que é importante oferecer um norte acerca de algumas questões preliminares.

Ineficácia se trata daquilo que é Inútil; aquilo que falta eficácia; sem utilidade; que não ocasiona os resultados esperados, incapaz de realizar suas funções. Nas palavras de Kamila Kayumi Sampei:

> A ocorrência do crime virtual, perante as leis penais insuficientes, tornou-se costume para os criminosos, uma vez que eles, diante de uma punição fraca da Lei 12.737/2012 voltam a cometer tais crimes por não terem medo da sanção. Para eles é vantajoso voltar a praticar esses delitos uma vez que não estarão sujeitos e penas restritivas de liberdade. A Ineficácia dá lei é visível. [2]

Nas palavras de Emanuel Alberto Sperandio Garcia Gimenes:

> Crimes virtuais são os delitos praticados por meio da Internet que podem ser enquadrados no Código Penal brasileiro, e os infratores estão sujeitos às penas previstas na lei.[3]

Atualmente no Brasil temos poucas leis que punem os crimes praticados na internet, as duas principais leis são: a lei 12.737 de novembro de 2012 e a lei 12.965 de abril de 2014 conhecidas também por lei Carolina Dieckmann e Marco Digital, respectivamente. Em um primeiro momento, acreditamos que estamos protegidos, porém na pratica não é assim, pois se formos analisar constataremos que não só os crimes são tratados de maneira superficiais como as penas são ineficazes.

Para o autor Tarcísio Teixeira:

> A internet é a interligação de redes de computadores espalhadas pelo mundo, que passam a funcionar como uma só rede, possibilitando a transmissão de dados, sons e imagens de forma rápida.” [4]

Além de que não existem muitas delegacias especializadas e preparadas para tratar crimes desse meio, nem mesmo para investiga-los, por conta disso muitos criminosos acabam ficando impunes, sem responder pelo que praticam ou causam a

---

[2] Revista de doutrina da 4ª região publicação da escola da magistratura do trf da 4ª região – emagis.
[3] GIMENES,Emanuel Alberto Sperandio Garcia.Juiz Federal Substituto publicado em 30.08.2013
[4] TEIXEIRA, Tarcisio. *Curso de Direito e processo eletrônico*. São Paulo. Saraiva, 2015.

outrem. Leva-se assim então a necessidade de estabelecer-se legislação especifica para tratar o tema de forma mais severa, além do investimento do governo, com delegacias e pessoas especializadas e prontas para a tratativa do tema devido a grande quantidade de casos que existem e que vem aumentando cada vez mais.

Tipificar significar tornar crime uma conduta. Para isso é necessário descrever com precisão a conduta e atribuir uma pena. Por exemplo, se um indivíduo causa, intencionalmente, a morte de uma outra pessoa, para que haja responsabilização criminal é preciso verificar se há uma descrição dessa conduta em um tipo penal na lei. Por exemplo: “Matar alguém. Pena: reclusão de seis a vinte anos”. Sendo assim, o ato de matar alguém é crime de homicídio.

A lei nº 12.737, por exemplo, foi criada com a pretensão de disseminar e punir os crimes do meio computacional, os ataques entre outras condutas. A Lei 12.737/2012 (Lei “Carolina Dieckmann”) foi criada no intuito de punir esses criminosos com a conduta devidamente tipificada no Código Penal. Nesse sentido foram inseridos os arts. 154-A e 154-B no Código Penal, criando a “invasão de dispositivo informático” e regulamentando sua ação penal.

> Art. 1º:Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Art. 2º: O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B: “Invasão de dispositivo informático.Art. 154-A. 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. § 1º:Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º:aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. § 3ºSe da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.” “Ação penal: Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer

dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.” [5]

[5]http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm

CAPÍTULO I – MARCO CIVIL DA INTERNET

Os computadores surgiram para facilitar nosso dia a dia, as tarefas que antes eram realizadas em espaços de tempo muito longos, passaram a ser realizadas quase de forma instantânea, o computador é uma maquina que armazena e transforma informações, sob o controle de instruções predeterminadas. [6]

1.1 HISTÓRICO

Desde os primórdios até os dias atuais, o homem vem buscando desenvolver novas máquinas e ferramentas que lhe torne as atividades do dia a dia mais fáceis e de certa forma mais prazerosas.

Uma alteração significativa que o mundo experimentou foi a Revolução Industrial, a qual modificou as feições do mundo moderno, alterou o modo de vida da população mundial, e, trouxe avanço significativo na mudança do homem do campo para as cidades, iniciou primeiramente no Reino Unido, por volta do século XVIII, talvez porque a Inglaterra possuísse grandes reservas de carvão mineral em seu subsolo, a principal fonte de energia para que as máquinas daquele período. As maquinas começaram a surgir em larga escala, as cidades começaram a se desenvolver, os trabalhadores que antes trabalhavam de forma artesanal passaram a controlar máquinas, as fábricas passaram a produzir cada vez mais, e as novas invenções, navios e locomotivas a vapor, fizeram com que a circulação das mercadorias se tornasse cada vez mais rápido, fazendo com que as matérias primas chegassem mais rapidamente as pessoas, e começaram a surgir de forma mais expressiva os inventores que viriam a mudar a maneira que vemos o mundo.

Podemos citar grandes invenções, como por exemplo, a Fotografia (1839), Telefone (1876), Luz Elétrica (1879), Televisão (1924), dentre outras tantas invenções que alteraram a forma como as pessoas viviam na época em que surgiram estes inventos, e de certa forma, o modo o qual vivemos hoje.

O primeiro computador digital eletrônico foi o ENIAC, desenvolvido em 1946, o qual a sigla significa Eletronic Numerical Integrator and Calculator, o qual o

[6]FRAGOMENI, Ana Helena. **Dicionário Enciclopédico de Informática**. Vol. I. Rio de Janeiro: Campus, 1987, p.125.

desenvolvimento foi todo por parte do exército norte-americano o equipamento pesava por volta de 30 toneladas, e media cerca de 140 metros quadrados.

O primeiro computador com mouse e interface gráfica é lançado pela Xerox, em 1981; já no ano seguinte, a Intel produz o primeiro computador pessoal 286, desde o surgimento do primeiro computador até os dias atuais a sociedade vive em constante mudança, mudamos dos escritos nas cavernas para o papel, do uso da pena com tinta ao código Morse, do e-mail para a videoconferência. [7]

No meio desta onda de transformações surgiu a internet, por volta da década de 60, aproximadamente no ano de 1996, algumas universidades se uniram para desenvolver a ARPANET (Advanced Research Projects Administration – Administração de Projetos e Pesquisas Avançados) primeiramente o surgimento da internet se deu por uma necessidade militar, pois naquela época estava retratado o cenário da Guerra Fria.[8]

Conforme definição de Zanellato, "A Internet é um suporte (ou meio) que permite trocar correspondências, arquivos, idéias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos".[9]

A Internet é uma Rede de computadores, integrada por outras Redes menores, comunicando entre si, os computadores se comunicam através e um endereço lógico, chamado de endereço IP, onde uma gama de informações são trocadas, surgindo ai o problema, existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando a disposição de milhares de pessoas que possuem acesso à internet, e quando não disponíveis pelo próprio usuário, são procuradas por outros usuários que buscam na rede o cometimento de crimes, os denominados Crimes Virtuais.[10]

Lévy, em referencia a obra *Cyberdémocracie: Essai de Philosophie Politique,* já havia identificado um crescente aumento por parte das pessoas que utilizavam a internet, e já previa um aumento substancial, tendo em vista o desenvolvimento de novas tecnologias, interfaces de comunicação sem fios, e o uso integrado de dispositivos portáteis.

Lévy estava certo, hoje a internet está disponível em vários dispositivos portáteis, das mais diferentes formas, milhares de pessoas permanecem por vezes mais tempo navegando na internet do que vivendo o mundo real, mídias sociais, leitura de livros,

---

[7]CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.30.
[8]ZANELLATO, Marco Antonio. **Condutas Ilícitas na sociedade digital**, Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet, n. IV, Julho de 2002.p. 173.
[9]PECK, Patrícia. **Direito digital**. São Paulo: Saraiva, 2002.p.13
[10]INELLAS, Gabriel Cesar Zaccaria. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004.p.3.

videoconferências, em fim, a rede mundial de computadores é acima de tudo uma rede mundial de Indivíduos, onde existem relações jurídicas fluindo, o Direito deve trazer soluções para os litígios que venham a ocorrer dentro deste ambiente virtual, o Direito é uma solução prática de planejamento e estratégia que só pode ser feita em equipe, num contato direto com as demandas e a própria evolução da sociedade, o Direito deve adaptar-se as demandas, os anseios da sociedade, onde as transformações são cada vez mais rápidas.[11]

Os primeiros crimes de informática começaram a ocorrer na década de 70, [12]na maioria das vezes era praticado por especialistas em informática, o qual o objetivo era driblar os sistemas de seguranças das empresas, com um foco principal nas instituições financeiras. Atualmente o perfil das pessoas que praticam crimes de informática já não são as mesmas da década de 70, os usuários mudaram, hoje em dia qualquer pessoa que tenha um conhecimento não tão aprofundado, mas que tenha acesso à internet pode praticar algum crime de informática, o usuário doméstico hoje já tem um conhecimento bem maior sobre o uso de computadores e tecnologia voltada para internet.

[11] LEMOS, André/LÉVY, Pierre. O futuro da Internet: em direção a uma ciberdemocracia. São Paulo: Paulus, 2010.p.10.

[12] PINHEIRO, Patrícia Peck. Direito Digital. 4. Ed. São Paulo: Saraiva, 2010.p.44 e 45. [11] CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <http://www.cert.br>. Acesso em: 10 mar. 2012.

1.2 - CONCEITOS DE CRIMES DE INFORMÁTICA

Os crimes de informática são aqueles perpetrados através dos computadores, contra os mesmos, ou através dele. A maioria dos crimes são praticados através da internet, e o meio usualmente utilizado é o computador[12].

Podemos conceituar o termo computador como:

> Máquina capaz de receber, armazenar e enviar dados, e de efetuar, sobre estes, seqüências previamente programadas de operações aritméticas (como cálculos) e lógicas (como comparações), com o objetivo de resolver problemas. [13]

Os Crimes digitais podem ser conceituados como sendo às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros.[14]

As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, abuso de computador, fraude informática, em fim, os conceitos ainda não abarcam todos os crimes ligados à tecnologia, e, portanto, deve-se ficar atento quando se conceitua determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual.[15]

Embora existam as divergências doutrinárias quanto a conceituar os crimes praticados em meio eletrônico, há uma grande leva de doutrinadores que os conceitua como “crimes digitais”.

A verdade é que a denominação dos delitos deve ser feita de acordo com o bem jurídico protegido, conforme diz Fragoso:

> A Classificação dos crimes na parte especial do código é questão ativa, e é feita com base no bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções.[16]

---

[13]CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003, p.9.

[14]HOLANDA FERREIRA, Aurélio Buarque de. **Novo dicionário da língua portuguesa**. 2ª Ed. Rio de Janeiro: Nova Fronteira, 2000.p.1016

[15]PINHEIRO, Patrícia Peck**. Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.46

[16]FRAGOSO, Heleno Cláudio. **Lições de direito penal: parte especial: arts. 121 a 212 do CP**. Rio de Janeiro: Forense, 1983.

Portanto, ao analisar um crime como sendo de informática, é necessário uma analise inicial, primeiramente para verificar se o mesmo é um *cibercrime* ou não, e depois aplicar o tipo penal correspondente, tendo em vista o bem jurídico tutelado.

CAPÍTULO II - A PROTEÇÃO DO ESTADO E A EXIGÊNCIA DE SEGURANÇA JURÍDICA NOS CRIMES CIBERNÉTICOS

O presente capítulo irá tratar da exigência que se faz ao Estado de garantir segurança à sociedade e aos indivíduos a que esta pertencem em relação aos crimes virtuais. Embora em nosso ordenamento jurídico nos dias atuais, estajam inseridas várias leis para coibir e proteger vários direitos e garantias fundamentais em relação ao tema do presente trabalho, estas leis já existentes se mostram insuficientes, tendo em vista que as penalidades são brandas demais, não sendo capazes de por si só coibirem a práticas de delitos ocorridos no âmbito virtual.

Como dito no parágrafo anterior, a respeito de algumas leis já existentes, temos como exemplo a Lei 11.829/08, que veio para combater a pornografia infantil na internet; a Lei 9.609/98, que trata da proteção da propriedade intelectual do programa de computador; a Lei 9.983/00 que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; a Lei 9.296/96 que disciplinou a interceptação de comunicação telemática ou informática; e a Lei 12.034/09, que delimita os direitos e deveres dentro da rede mundial, durante as campahas eleitorais; não obstante e/ou menos importante, temos ainda a Lei 12.737/12, também conhecida socialmente como “Lei Carolina Dieckmann”, da qual será tratada e analisada mais adiante.

Além de todas essas leis mencionadas no parágrafo anterior, ainda têm-se aqueles crimes já tipificados no Código Penal Brasileiro, cabendo relembrar aqui que o mesmo é do ano de 1940, onde o contexto daquela época era muito diferente de nossa atual realidade, onde são cometidos diversos crimes através de diversos meios tecnológicos, principalmente através do uso de computadores das mais variadas formas tais como, acesso a contas bancárias, difamação, calúnia, ameaça, racismo, uso de dados de terceiros para realizar compras, etc.

2.1 - GARANTISMO PENAL

Adentrando nesse tema do garantismo penal, se faz necessário abordarmos algumas considerações no que diz respeito a esse tema. A Teoria do Garatismo Penal foi elaborada pelo professor e filósofo Luigi Ferrajoli e com base em seu livro Direito e Razão, trata o autor de algumas explanações que dizem respeito ao propósito de abordar o presente trabalho.

Neste sentido, aludo Ferrajoli que:

> "Garatismo" designa um modelo normativo de direito: precisamente, no que diz respeito ao direito penal, o modelo de "estrita legalidade" SG, próprio do Estado de Direito, que sob o plano epistemológico se caracteriza como um sistema cognitivo ou de poder mínimo, sob o plano político se caracteriza como uma técnica de tutela idônea a minimizar a violência e maximizar a liberdade e, sob o plano jurídico, com um sistema de vínculos impostos à função punitiva do Estado em garatia dos direitos dos cidadãos. É consequentemente "garantista" todo sistema penal que se conforma normativamente com tal modelo e que o satisfaz efetivamente.[17]

Sendo assim, o "Garantismo" nada mais é que a segurança que os cidadãos, vivendo estes em um Estado Democrático de Direito, onde o poder de atuação do Estado deriva de um ordenamento jurídico obrigatório e tendo presente em seu corpo a Constituição Federal de 1988, age com uma garantia para minimizar o poder punitivo e garantir, ao máximo possível, a liberdade dos cidadãos.

Ademais, cabe ressalvar uma crítica construtiva de que, o Estado tenha que garantir essas liberdades, intervindo o minimamente possível no que tange e se refere o caráter punitivo, devendo assim, ter o Estado mecanismos suficientes para tais, quais sejam, normas fortalecedoras e que sejam estas eficazes mediante a prevenção da práticas de tais delitos já mencionados no tópico anterior.

Oberva-se, portanto, que existe aqui uma crítica feita pelo autor ao ordenamento jurídico que, em tese, teria um plano de fundo garantista, mas que na prática adotaria uma postura bastante diversa. Em suma, deveria haver o agir de forma válida e eficaz por parte o Estado, ou seja, um agir de forma a garantir a liberdade e o respeito aos direitos fundamentais previstos em nossa Carta Maior, mas que acaba atuando de forma diversa considerada por ele, mais eficaz, em face dos delitos cometidos na

[17] FERRAJOLI, Luigi. **Direito e Razão- Teoria do Garantismo Penal**. São Paulo: Editora Revista do Tribunais, 2010, p. 785/786.

sociedade como um todo, e em especial no âmbito virtual.

Atualmente, existem diversas discussões e também fortes críticas no que diz respeito ao entendimento da teoria do Garantismo Penal, por muitos juristas e autores à defenderem, que esse entendimento se divide em duas correntes A primeira delas se chama “garantismo negativo”, que seria aquela que se preocupa somente com a restrição indevida da liberdade do ser social. A segunda, a qual denomina o “garantismo positivo”, visa proteger os direitos fundamentais de terceiros de serem violados pelos criminosos, bem como o direito de ação do Estado para punir tais criminosos.

Como bem se posiciona Lenio Streck em relação ao dito no paragráfo anterior:

> Não se esgota na categoria da proibição de excesso, já que vinculada igualmente a um dever de proteção por parte do Estado, inclusive quanto à agressões contra direitos fundamentais provinientes de terceiros, de tal sorte que se está diante de dimensões que reclamam maior densficação, notadamente no que diz com os desdobramentos da assim chamada proibição de insuficiência no campo jurídico penal e, por conseguinte, na esfera da política criminal, onde encontramos um elenco significativo de exemplos a serem explorados.[18]

E ainda preconiza Sarlet que:

> (...) o Estado- também na esfera penal- poderá frustar o seu dever de proteção atuando de modo insuficiente (isto é, ficando aquém dos níveis mínimos de proteção constitucionalmente exigidos) ou mesmo deixando de atuar, hipótese por sua vez, vinculada (pelo menos em boa parte) à problemática das omissões inconstitucionais. É nesse sentido que – como contraponto à assim designada proibição de excesso- expressiva doutrina e inclusive jurisprudência tem admitido a existência daquilo que se convencinou batizar de proibiçao de insufiência (no sentido de insuficiente implementação dos deveres de proteção do Estado e como tradução livre do alemão Untermassverbot). [19]

Conforme o abordado até aqui, em relação ao garantismo penal, pode-se perceber que, em seu aspecto positivo tem-se a utilização do princípio da proporcionalidade em sua dupla face, onde é garantido os direitos daquele contra o qual o Estado exerce sua pretensão punitiva e, ao mesmo tempo são garantidos direitos fundamentais também aos demais membros da sociedade. Portanto, o

---

[18] SARLET, Ingo Wolfgang. **Constituição e Proporcionalidade: o direito penal e os direitos fundamentais entre proibição de excesso e de insuficiência.** Revista de Estudos Criminais, n. 12, ano 3, Sapucaia do Sul, 2003, p.86 segs. *Apud* STRECK, Lenio Luiz. A dupla face do princípio da proporcionalidade e o cabimento de mandado de segurança em matéria criminal: superando o ideário liberal-individualista-clássico.

[19] SARLET, Ingo Wolfgang. **Constituição e Proporcionalidade: o direito penal e os direitos fundamentais entre proibição de excesso e de insuficiência**. Revista de Estudos Criminais, n. 12, ano 3, Sapucaia do Sul, 2003.

entendimento é que a aplicação do principio da proporcionalidade como proibição de insuficiência reside na Constuição Federal e, mais precisamente, nos direitos fundamentais nela contidos, que dão legitimidade à aplicação do princípio da proporcionalidade visto sob a ótica do garantismo como forma de garantir segurança aos seres sociais que estão exposto à pratica dos delitos virtuais.

2.2 - ANÁLISE DO PRINCÍPIO DA PROPORCIONALIDADE

O princípio da proporcionalidade surgiu, inicialmente, no âmbito do Direito Administrativo, funcionando este como um limite à atuação do poder de polícia do Estado, baseado no ideal de garantir a liberdade individual em face dos interesses da administração.

Tal princípio, no âmbito do direito penal, nada mais é que a tutela punitiva que pertence ao Estado, sendo esta de extrema necessidade, uma vez que os homens vivem em sociedades, possuem direitos e interesses diversos, que merecem proteção; essa proporcionalidade também pode ser vista como uma adequeção, quando o autor menciona que caberá ao legislador escolher a pena em conformidade com cada espécie de delito, não devendo este, portanto, aplicar penas mais gravosas a um delito de menor gravidade, muito menos que ocorra o contário.

Como bem preconiza Paulo Bonavides, citando o ilustre entendimento de Pierre Muller, o qual diz que “quem utiliza o princípio da proporcionalidade, segunda este constitucionalista, se defronta ao mesmo passo com uma obrigação e uma interdição; obrigação de fazer uso dos meios adequados e interdição quanto ao uso dos meios desapropriados.” (BONAVIDES, 2015, P.407).

2.3- ANÁLISE AO PRINCÍPIO DA PROIBIÇÃO DA PROTEÇÃO DEFICIENTE POR PARTE DO ESTADO

Neste presente tópico será tratado o princípio da não proteção deficiente, ao passo que se exige uma atuação do Estado de maneira a proteger direitos fundamenatais, ou seja, o Estado não pode se omitir, tanto parcialmente, quanto de forma geral, em coibir, tratar e previnir os problemas sociais que se encontram presentes no meio social dos cidadãos. Aqui, destaca-se que em relação aos crimes virtuais, que é

matéria debatida no presente trabalho, o Estado não pode simplesmente “cruzar os braços” para esse tipo de problema social, pois se assim for estará o mesmo oferecendo proteção deficiente aos seres da sociedade, ao passo, as normas punitivas já existentes não são, por si só, capazes de suprirem a lacuna existente no ordenamento jurídico, no que diz respeito a prevenção, investigação e punição dos crimes praticado no ambiente virtual.

Nesse mesmo contexto, é relevante apontar os ensinamentos de Mougenot, a este respeito o autor destaca que:

> Assegura-se não somente uma garantia do cidadão perante os excessos do Estado na restrição de direitos fundamentais (princípio da proibição do excesso)- a chamada “proteção vertical”, na medida em que os cidadãos têm no princípio da proporcionalidade (modalidade proibição de excesso) um ampara constitucional contra o poder do Estado (verticalizando, portanto, de “cima para baixo”)- mas também uma garantia aos cidadãos contra a agressão de terceiros- “proteção horizontal”-, no qual o Estado atua como garantia eficaz dos cidadãos, impedindo tais agrassões (Tutelando eficazmente o valor da “segurança” garantida constitucionalmente) ou punindo os agressores (valor “justiça”, asssegurado na Constituição Federal). [20]

Sendo assim, restou-se claro a existência de um duplo viés em relação ao mencionado princípio, ao passo que, além de proibir o excesso, onde se encontra seus efeitos, em conjunto com a atuação dos direitos fundamentais na limitação do poder do Estado, trata-se também da exigência feita ao Estado de atuar de maneira a proteger os direitos fundamentais, não deixando existir lacunas no ordenamento juríco brasileiro.

Portanto, esse duplo viés existente serve como um parâmentro para não exceder aquilo que já se encontra previsto em lei como função estatal, bem como proibi também o Estado de deixar cumprir aquilo que é sua competência e função fazer para dar garantia e segurança a sociedade.

Portanto, integrar a prespectiva do direito penal na Constituição, tendo por finalidade garantir uma proteção integral dos direitos e garantias, não seria possível por si só dar a proteção devida, tendo em vista a grande expansão a que se chega a prática dos delitos no ambito virtual, deixando, no entanto, deficiente a proteção integral paras os casos de crimes em ambente virtual.

---

[20]BONFIM, Edilson Mougenot- **Curso de Processo Penal/ Edilson Bonfim Mougenot**- 10. Ed. p. 113.- São Paulo: 2015.

2.4. CONSIDERAÇÕES SOBRE A GLOBALIZAÇÃO E O AVANÇO DA INTERNET NO BRASIL

Nos últimos cem anos teve-se uma grande modernização em maior parte, e porque não dizer, em todos os setores da vida em sociedade. A tecnologia avançou de forma exponencial, podemos dizer até que, a evolução teve um salto gigantesco em pouquíssimo tempo. E ainda estamos nos adaptando a essas transformações constantes.

Um dos setores que teve tamanha mudança foi o setor da informação e consequentemente o acesso ao conhecimento, uma vez que com a crescente evolução o uso da internet e seus meios chegou a todos os setores sociais, desde o mais baixo ao mais alto, fazendo com que todos tivessem acesso a esse meio tecnológico tão avançado.

A informação é um direito de quarta geração e garantido na Constituição Federal, em seu artigo 5º, incisos, IV, IX, XIV, XXXIII, sendo assim é dever do Estado estar sempre atento as transformações sociais que o homem vem alcançando com o passar do tempo, uma vez que, estas alterações sociais, nada mais é que, o resultado dos interesses da própria sociedade que não mais almeja o costume e tradição social já existentes, mas sim, buscam cada vez mais a interação contínua com o mundo, na busca pelo conhecimento e sentimento, da conectividade uniforme entre os povos.

O Brasil, assim como os brasileiros, está inserido em uma conjunta globalização, de grande relevância, e em decorrência disto passa a se obter de recursos que são comuns e acessíveis a todos que seguem a tecnologia do mundo digital. A internet cresce cada vez mais, a cada passo que a tecnologia se evolui a internet à acompanha, pois, conforme já mencionado no parágrafo anterior, esse meio tão evoluído e crescente, se introduziu em todas as classes e povos de nossa sociedade, fazendo com que todos tenham acesso a ela, facilintando assim o uso dela para a prática dos crimes cibernéticos, tema do presente trabalho.

Rodrigo Alves Zaparoli ao discorrer sobre esta sociedade da informação, ou seja, uma sociedade assentada sobre a busca pela informação e conhecimento, alerta sobre os perigos que esta nova geração pode sofrer, uma vez que os adeptos a ela não encontre a devida proteção legal.

Zaparoli, a este respeito, se posiciona da seguinte forma:

> Entretanto, apesar de ser algo evidente em nosso cotidiano, o legislador pátrio não consegue evoluir e criar dispositivos com a mesma celeridade da empregada pela sociedade em suas transformações, logo, o legislador acaba pecando em relação à celeridade em que oferece o devido amparo legislativo.[21]

Com o crescente avanço da internet, os meios já existentes no Código Penal Brasileiro, para punir crimes, se tornaram quase que incapazes de por si só combaterem tais práticas, tendo em vista que no ano de 1940 quando o mesmo fora introduzido no ordenamento juridico, a internet quase não era vista, sendo assim não foi introduzido nada neste Código que visasse dar proteção e punição aos cirmes que viessem a ser cometidos tendo como meio a internet e o ambiente virtual. Fazendo-se necessario então, nos dias atuais, ser repensado pelo Estado a forma de garantir segurança à sociedade, pois os meios já existentes não suprem integralmente essa lacuna que existente, ou seja, tais meios não são capazes de acompanhar o grande avanço tecnológico.

[21] ZAPAROLI, Rodrigo Alves. **Comentários à Lei nº 12.737/12**. Disponível em: http://www.conteudojuridico.com.br/artigo,comentarios-a-lei-no-1273712,43118.html. Acesso em 23 de outubro de2018.

CAPÍTULO III – A (IN)EFICÁCIA DA LEI 12.737/2012

3.1 ANÁLISE LEGISLATIVA DO ARTIGO 154-A

A internet revolucionou o mundo e seu desenvolvimento provocou grandes mudanças na sociedade, inclusive para o direito. Ela é um verdadeiro fenômeno mundial, sua utilização cresce de forma descontrolada. A prática cultural depois da internet é totalmente diferente daquela praticada antes dela, pessoas têm acesso a coisas que jamais teriam antigamente. As características da *web* ajudam a divulgar conteúdos e dificultam a criação e a fiscalização de certas medidas.

Para os riscos apresentados por este grande fenômeno mundial existe a discussão no mundo jurídico quanto à necessidade de uma regulamentação específica dentro do direito, tanto na delimitação dos direitos dos internautas quanto na criminalização de alguns fatos específicos que "não possuem" tutela do direito penal. Segundo o advogado Alexandre Atheniense, especialista em leis de Internet, *"a internet não deve ser desprovida de qualquer lei e, para uma norma ser de fato eficiente na internet, é necessário que seja algo global".*

Em meados do ano de 2012, a atriz global Carolina Dieckmann teve seu computador invadido por hackers, os quais furtaram arquivos pessoais desta e divulgaram indevidamente na internet. A mobilização causada pela atriz e o apelo midiático proporcionaram a rápida tramitação dos PL 84/99 e PL 2793/2011 (conhecido como Lei Carolina Dieckmann).

Em Dezembro de 2012, foram sancionadas, pela presidente Dilma Rousseff, duas leis que tratam sobre *cybercrimes*, a lei 12.737, conhecida como Carolina Dieckmann, a qual estabelece penas de multa e prisão para vários tipos de crimes digitais e a Lei 12.735, a Lei Azeredo, esta tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares.

O artigo 154-A, acrescentado ao Código Penal por meio do art. 2º da lei 12737, tipifica a invasão do dispositivo eletrônico, visando a proteção da privacidade e da intimidade, bem como informações sensíveis ao proprietário ou usuário do dispositivo. A lei deixa claro que a invasão deve ter como fim o acesso, a alteração ou destruição de dados informações que devem ser preservadas, bem como que o sistema não esteja

fragilizado, prevê que o titular destes dados deve utilizar alguma medida protetiva, demonstrando claramente que eles não deveriam ser de conhecimento público ou de terceiros e também não deve autorizar expressa ou tacitamente o acesso ao dispositivo invadido.

Antes mesmo que fosse sancionada a lei 12737/2012, ao analisar o projeto de lei 84/99, o professor Tulio Vianna já considerava absurda a necessidade de uma “expressa restrição de acesso”. Deu ele como exemplo, o fato de alguém deixar seu notebook na mesa de um estabelecimento enquanto vai ao banheiro. Segundo Vianna, isso não torna lícita a conduta de quem se aproveita desta ausência para acessar os dados. Afirma categoricamente que “não é razoável exigir que o proprietário tenha que declarar expressamente que ninguém está autorizado a acessar seus dados”.

3.2 A IMPORTÂNCIA DA APLICABILIDADE DA LEI

Aqueles que defendem a necessidade de uma legislação específica para crimes cibernéticos suscitam a diferenciação entre crimes digitais próprios e crimes digitais impróprios. Os impróprios seriam aqueles que utilizam o meio informático como instrumento para a realização do crime, seriam os crimes comuns, em que já existiria tipificação na legislação penal. Ao passo que os crimes digitais próprios seriam aqueles cometidos contra o sistema informacional e só poderiam ser cometidos por este meio, são elencados como a supressão de dados informáticos, invasão de sistemas, destruição de dados informáticos e fraude de sistemas para obtenção de vantagem ilícita.

A grande maioria dos crimes são perfeitamente tutelados pela legislação penal, como por exemplo, nos artigos 155, 163 e 171 do Código Penal, crime de furto, crime de dano e estelionato, respectivamente.

Segundo opinião do doutrinador Tulio Vianna, o problema é que acredita-se, de um modo geral, que somente criminalizando condutas é que pode-se reprimi-las, o que o referido autor considera um grande erro, pois, muitas vezes outros ramos do direito são muito mais eficazes e céleres para tutelar determinados bens.

A pena privativa de liberdade é uma sanção muito rigorosa e às vezes, até ineficaz para a tutela de determinados bens.

Segundo a advogada Patrícia Peck Pinheiro, especialista em direito digital, não há

sociedade saudável sem que estejam claros os valores que são protegidos e sanção para quem as descumpra. Entretanto, tem-se que penalizar o infrator digital com uma pena que impacte sua esfera virtual, não apenas física, pois, segundo ela, de nada adianta colocar o criminoso eletrônico em uma cela na cadeia e ele continuar acessando a internet via celular, o que fará com que ele continue praticando o crime.

Na opinião dos autores Salete Oro Boff e Felipe da Veiga Dias[22], há uma deturpação da rede como espaço de ninguém, "terra sem lei", contudo, trata-se, na verdade, de outro ambiente no qual se efetivam relações entre pessoas, podendo ocorrer infrações ou lesões a direitos, bem como sua correspondente responsabilização.

Segundo Daoun, o Código Penal é plenamente aplicável ao meio eletrônico, porque ele é só mais um meio para se praticar crimes, para ele, a legislação penal no Brasil é suficiente para tutelar as novas condutas, porque as condutas são as mesmas, só que num formato diferente. Para ele, o Direito Penal para as relações virtuais deve ser um direito penal mínimo, não havendo necessidade de uma legislação nova, deve-se usar direito penal minimamente, usando os outros ramos do direito para coibir as situações praticadas no ambiente eletrônico. Deve o Direito Penal ser guardado e resguardado para situações extremas. Faz crítica o criminalista quanto à compulsividade de legislar, de criar lei penal, sob o argumento de que o Direito penal é o instrumento do direito mais drástico que se tem, pois, segundo ele, pagar indenização é uma coisa, perder a liberdade é outra. A criação demasiada de lei gera faz com que esse ramo do perca sua credibilidade.

3.3 - ALGUMAS CONSIDERAÇÕES SOBRE A LEI 12.737/12

A Lei 12.737/12, anterior Projeto de Lei n° 2793/2011, fora criada para tipificar condutas criminosas praticadas através da rede de computadores, dando assim, um amparo a aquelas pessoas que sofressem com tal invasão e também coibindo assim, a tentativa de novos atos como estes.

Antes de adentrarmos a mais neste contexto da Lei 12.737/12, cabe ressaltar, brevemente, a respeito do "Caso Carolina Dieckemann", caso este que, deu ensejo à criação da referida Lei. No ano de 2012 a atriz Carolina Dieckemann teve sua

[22]BOFF, Salete Oro e DIAS, Felipe da Veiga. **O acesso à informação no campo digital: Uma análise entre a sociedade da informação e a sociedade de risco.** Revista de Estados Jurídicos, ano 16, n.23, 2012, p. 330-331.

intimidade violada e exposta na internet. A princípio a atriz suspeitava ter sido funcionários de uma loja de infomática que praticarm tal delito, pois a atriz havia levado seu computador portátil para que fizessem um reparo no mesmo. Dois meses após este evento, a atriz foi contatada por pessoas que diziam estar em posse de suas fotos íntimas e que iria expô-la, caso a mesma não pagasse a quantia de dez mil reais. De início a atriz tentou resolver esta situação de forma sigilosa para exposições.[23]

No dia sete de maio do ano de 2012, Carolina Dieckemann foi até a delegacia expor o caso para que fosse, então, iniciada a investigação do caso, pois três dias antes de divulgarem suas fotos íntimas, haviam sido divulgadas também, fotos de seu filho menor em alguns sites.

Ao final da investigação, conclui-se que não haviam sido os funcionários da loja de informática que haviam copiado as fotos da atriz, mas sim um grupo de Crackers (diferente de hackers, uma vez que, estes são pessoas que buscam aperfeiçoar e proteger dispositivos informáticos e aqueles, usam seus conhecimentos apenas para o mal, ou seja, para práticas ilícitas[24]) que conseguiram acessar o email da atriz e subtraíram suas fotos e posteriormente as divulgaram.

Tais fatos causaram uma comoção e alerta nacional devido à intensa pressão da mídia que não apenas evidenciou a fragilidade que o Brasil tinha quanto à proteção do indivíduo em sua esfera privada, mas também aos danos que tal exposição podem causar.

A exposição de motivos da Lei 12.737/12 a respeito da Lei Azeredo:

> Ao nosso ver, o PL 84/1999, em sua redação atual, traz propostas de criminalização demasiadamente abertas e desproporcionais, capazes de ensejar a tipificação criminal de condutas corriqueiras praticadas por grande parte da população na Internet. Tal estratégia redacional, típica de uma sociedade de risco de uma lógica de direito penal do inimigo, busca uma antecipação da tutela penal a esferas anteriores ao dano, envolvendo a flexibilização das regras de causalidade, a tipificação de condutas tidas como irrelevantes, a ampliação e a desproporcionalidade das penas e a criação de delitos de perigo abstrato, dentre outras características. [25]

[23] G1. **Carolina Dieckemann fala pela 1ª vez sobre fotos e diz que espera Justiç**a. Disponível em: <http://g1.com/pop-arte/notícia/2012/05/carolina-dieckemann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>. Acesso em 30 de outubro de 2018.

[24] Redação Olhar Digital. **Qual a diferença entre hacker e cracker?**. Disponível em: <http://olhardigital.uou.com.br/fique_seguro/noticia/qual-a-diferença-entre-hacker-e-cracker/38024>. Acesso em 28 de outubro de 2018

[25] BRASIL. **PROJETO DE LEI 2793 DE 2011**. Disponível em: <http://www.camara.gov.br/proposiçõesWeb/prop_mostraintegra?codteor=944218&filename=PL+2793/2011>. Acesso em 30 de maio de 2019.

A mencionada Lei, que posteriormente se tornaria o Projeto Lei n° 89/2003, ao ir para o Senado,iria punir desta forma, atitudes que não carecem de repressão penal, como por exemplo, testes de segurança, não autorizados, de sistemas informáticos, mas que houve prévio anuncio, ou seja, ações que não possuem a intenção ou a finalidade de praticar um crime, mas pelo contrário, intensões benéficas, seriam punidas.

Paralelo a Lei 12.737/12 ou como era popularmente chamada, Carolina Dieckemann. Devido as inúmeras transformações sofridas pela Lei 84/99 não havia mais como ser alterada, desta forma alguns temas que não foram tratados neste projeto, como pontua o texto da exposição de motivos da referida lei:

> Ocorre que, em seu atual estágio de tramitação, por conta de questões regimentais, o Projeto e Lei referido não pode mais ver emendado ou alterado. Apresentamos, portanto, nossa proposta alternativa de criação de tipos penais específicos para o ambiente da Internet. Esta redação que apresentamos, e que ainda é passível da aperfoçoamento e contribuições- sempre de forma a garantir os direitos do cidadão na Internet e evitar a criminalização de condutas legítimas e corriqueiras na Internet. [26]

A referida Lei proprôs um equilíbrio das penas em consonância com a prática ilícita efetuada pelo agente delituoso. Cabendo ressaltar ainda que, um dos objetivos, segundo a justificação da mesma, é estabelecer uma harmonia entre ela com as já existentes no ordenamento jurídico.

A referida Lei foi sancionada em 02 de dezembro de 2012 pela ex Presidenta Dilma Rousseff. Proviniente do Projeto de Lei 2.793 do ano de 2011 apresentado em 29 de novembro de 2011, pelo Deputado Paulo Teixeira, que tramitou em regime de urgência e em tempo célere no Congresso Nacional, em comparação com outro projetos sobre delitos informáticos que as casas de leis apreciavam, como por exemplo, o Projeto Lei 84/1999, a “Lei Azeredo”, também transformado em Lei Ordinária 12.735/2012 em 3 de dezembro de 2012.

Talvez, a tramitação acelarada da mencionada lei, com o intuito de dar uma resposta à sociedade com maior permanência, dadas as circunstâncias daquele momento vivido no País, é que não se teve um tempo de manuntenção necessária para a lei encoporar e tornar uma ferramenta com maior poder para coibir os crimes nela previstos também aprofundar mais nesta matéria.

---

[26] BRASIL. **PROJETO DE LEI 2793 DE 2011**. Disponível em: <http://www.camara.gov.br/proposições Web/prop_mostraintegra?codteor=944218&filename=PL+2793/2011>. Acesso em 30 de outubro de 2018.

3.4 - ANÁLISE DA MATÉRIA TRATADA NA LEI 12.737/12

Conforme, o até aqui exposto, resta-se claro que, muitas são as tentativas do Estado, mediantes as normatizações já existentes, para tratar as mais variadas ações nos ambientes virtuais. Entretanto, apesar de ser algo evidente em nosso dia a dia, o legislador pátrio não consegue evoluir e criar dispositivos com a mesma celeridade da empregada pela sociedade em suas transformações, logo, o legislador acaba pecando em relação à celeridade em que oferece um amparo legislativo.

Cabendo, apontar ainda o reconhecimento que a sociedade está sempre a evoluir, se modificar, em diversas épocas, ela tende a se comportar de alguma determinada forma.

Neste sentido, cabe ressaltar Liliana Minardi Paesani que:

> Vivemos em uma época em que a produção normativa é insuficiente tanto para fazer frente às mudanças sociais, causadas pelo rápido avanço tecnológico, como para obter sua legitimação diante de grupos sociais cada vez mais fracionadas, que não compartilham seus valores com os demais e encontram um dos pocucos pontos de contato justamente no próprio avanço tecnológico, notadamente na internet. [27]

Contudo, apesar de o propósito aqui seja fazer uma breve crítica ao Estado, e apontar uma possível omissão, ainda que esta seja parcial, no que se refere aos crimes virtuais, há que se mencionar que o mínimo apresentado por parte do Estado, é a própria Lei 12.737/12, que já é um grande avanço para a sociedade.

A mencionada lei foi alvo de muitas críticas entre juristas e especialistas pois seus dispositivos são amplos, confusos e podem gerar dupla interpretação, o que pode ser utilizado para enquadramento criminal de condutas trivais ou memso para a defesa e respaldo dos infratores cibernéticos, que tornaria a lei injusta e ineficaz. Sob outro prisma, ainda, as penas são pouco inibidoras.

Com o advento dessa nova lei, o Código Penal Brasileiro fora modificado em quatro artigos, sendo eles: o artigo 154, violação do segredo profissional, que agora possui o artigo 154- A, que dispõe sobre a invasão de dispositivo infomático alheio. E artigo 154- B que serve como um complemento do artigo anterior, neste ficou definido que a ação penal será pública mediante representação, salvo se o delito tenha sido contra a administração pública direta ou indireta.

---

[27] PAESANI, Liliana Minardi (Coord). **O direito na sociedade de informação**. São Paulo: Atlas, 2007.

Pois bem, o artigo 154- A, versa sobre a invasão de dispositivos informáticos versando:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação idevido de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita de titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
> Pena- detenção, de 3 (três) meses a 1 (um) ano, e multa. [28]

Neste artigo, está tutelado a intimidade, a vida privada e o direito ao sigilo de dados constantes em dispositivos informáticos. Há também, ao final do caput, do patrimônio do titular do dispositivo violado, punindo a intencionalidade de obtenção de vantagem ilícita, ao agir, instalando vulnerabilidade no dispositivo da vítima.

O núcleo central da conduta típica, se consubstância no verbo "invadir" [29] é "ingressar virtualmente, sem autorização expressa ou tácita do titular do dispositivo". Portanto, o crime consiste em invadir computadores, *tablets, smartphone*, HD's, instalando programas ou conectando a outros dispositivos e não necessariamente precisa estar conctado à internet.

Preconiza Capez ainda que:

> A invasão deve se dar por meio de violação indevida de mecanismo de segurança estabelecido pelo usuário do dispositivo. Como exemplo de segurança, podemos citar; *firewall*, ativirus*, antimalware, antispyware*, senha restrita para acesso pessoal de usuário e etc. [30]

A finalidade no presente caso seria de buscar a obtenção, a adulteração ou a destruição de dados ou informações, sem este elemento o crime não se aperfeiçoa. No tocante a este caput, Capez aponta uma polêmica, e ainda alega que existe ali uma redação com diferentes interpretações, uma vez que, ao final do caput é descrita a conduta de instalar vulnerabilidades para obter vantagem ilícita, passando assim, a existir duas descrições típicas distintas, quais sejam, a já mencionada de invasão de dispositivo, com o fim de obter, adulterar ou destruir dados ou informações, como também, o de instalar vulnerabilidades para os fins de obtenção de vantagem ilícita. Neste último, o crime se aperfeiçoa somente com a instalação de vulnerabilidades, não

---

[28] Disponível em: <http://www.planalto.gov.br/ccvil_03/decreto-lei/Del2848compilado.htm>. Acesso em 02 de novembro.
[29] CAPEZ, Fernando**. Código Penal Comentado**. Fernando Capez, Stela Prado. - 6. Ed.- São Paulo: Saraiva, 2015. P. 347.
[30] CAPEZ, Fernando. **Código Penal Comentado.** Fernando Capez, Stela Prado. - 6. Ed.- São Paulo: Saraiva, 2015. P. 347.

sendo, portanto, a ocorrência da obtenção de vantagem ilícita; já no primeiro caso, a consumação se dá no simples fato de invadir, mesmo que não haja a obtenção, adulteração e destruição de dados, ambas as condutas são crimes formais.

Ante todo o exposto acima, Capez alega que:

> Pode surgir também a interpretação de que só há um verbo no tipo penal, consistente na ação de invadir. Nesta hipótese, a invasão se daria com o fim especial de: (a) obter, adulterar, ou destruir dados; (b) instalar vulnerabilidade apenas um crime, portanto. É crime formal. A parte final, nessa hipótese, seria apenas mais sobre as finalidades exigidas pelo tipo penal (invadir dispositivo informático com o fim de instalar vulnerabilidades).[31]

Portanto, dá-se no entendimento de haver dois crimes distintos, primeiro o agente invade dispositivo alheio com o fim de obter, adulterar ou destruir dados e posteriormente instala vulnerabilidades com o fim especial de obter vantagem ilícita.

3.5 – DA FRAGILIDADE DA LEI 12.737/12

Ao analisarmos a matéria tratada no dispositivo legal acima mencionado, encontramos uma série de falhas em sua redação, falhas estas que trazem como atípicas algumas condutas que pode ser praticadas por cibercriminosos.

O tema em foco do presente trabalho se encontra no artigo 154-A da referida lei, que discorre da seguinte maneira em seu caput:

> Art. 154-A. 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.[32]

O que define sujeito ativo e passivo está bem no início do artigo, no trecho em que diz “Invadir dispositivo informático alheio”, invadir aqui, de acordo com os ensinamentos de Rogério Greco se traduz em, violar, penetrar ou acessar. [33]Com isso, sujeito ativo, neste caso, é aquele que invade um dispositivo informático alheio, e o sujeito passivo, é quem sofreu a lesão.

No que diz respeito a isso, Tulio Viana e Felipe Machado ensinam que o legislador ao optar pela expressão “invadir dispositivo informático alheio”, acaba

---

[31]CAPEZ, Fernando. **Código Penal Comentado**. Fernando Capez, Stela Prado. - 6. Ed.- São Paulo: Saraiva, 2015. P. 348

[32] BRASIL. **Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 12 de novembro de 2018.

[33]GRECO. Rogério. **Código Penal Comentado**. 7. Ed. Niterói: Impetrus, 2013. P. 443.

tornando atípica as condutas daquele que invadir dispositivo próprio para obter, indevidamente, dados alheios que lá estejam armazenados. [34]

Sendo assim, aqueles que acessam uma "lan house", um computador de uma empresa, ou qualquer outro dispositivo de terceiros, está com sua privacidade em risco, pois o proprietário do dispositivo informático poderá ter acesso a informações que ali possam estar contidas. Como por exemlo, um empregador que pode acessar o dispositivo informático que seu empregado usou e, sendo assim, usar as informações que ali existam.

Túlio Vianna ensina a essse respeito:

> Trata-se obviamente de uma situação absurda, pois o que se deve tutelar é a inviolabilidade dos dados, independentemente de quem seja o proprietário da máquina. Não há, porém, como o intérprete sanar o problema, pois a analogia *in marlam partem* é vedada no Direito Penal pelo princípio constitucional da legalidade. Espera-se, pois, que o legislador corrija esta lacuna por meio de uma nova lei. [35]

A lacuna do artigo mencionado, não se limita no que fora dito acima, mas torna-se cada vez mais incongruente ao exigir a presença de um mecanismo de segurança e bem como, sua indevida violação para que, assim, seja tipificado o crime.

Rogério Grego discorre que "essa exigência, isto é, a violação indevida de mecanismo de segurança, impede que alguém seja punido pelo tipo penal previsto pelo art. 154-A".[36]

Tal condição para que o delito possa ser caracterizado, embora ao ser criado tivesse uma blindagem de boas intenções, de acordo com a exposição de circunstâncias já apresentado, deixou muito frágil o objeto repressivo da lei, criando mais condutas atípicas.

Tulio Vianna assim discorre:

> O elemento normativo "mediante violação indevida de mecanismo de segurança" faz com que seja atípica a conduta quando o dispositivo informático não possuir qualquer mecanismo de segurança, tais como senhas de acesso, antivírus, *firewalls* ou similares. É imprescindível que o agente supere este obstáculo tecnológico para que a conduta sejs tipificada. [37]

O absurdo dessa exigência, qual seja "violação indevida de mecanismo de segurança" mostra claramente a ausência de conhecimento do legislador. Essa lei não

---

[34]VIANNA, Túlio; MACHADO, Felipe. **Crimes Cibernéticos**. Belo Horizonte: Fórum, 2013. P. 94.
[35]VIANNA, Túlio; MACHADO, Felipe. **Crimes Cibernéticos**. Belo Horizonte: Fórum, 2013. P. 95.
[36] GRECO, Rogério. **Código Penal Comentado**. 7. Ed. Niterói: Impetrus, 2013. P. 444.
[37] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos.** Belo Horizonte: Fórum, 2013. P. 96.

considerou que uma grande parcela da população ainda não tem conhecimento do grande avanço que ocorreu nos últimos tempos, e relação a rede mundial de computadores trouxe, assim, não os protegendo quando faz estas exigências supracitadas para configurar o crime.

Assim, resta-se claro então, o risco eminente que corre as pessoas que ainda não acompanharam esse avanço tecnológico, no que diz respeito a sua intimidade e vida privada. Vivemos, hoje, em um cenário onde o avanço da tecnologia se torna real e necessário para nosso meio, e paralelo a isso espera-se que o Estado dê a preservação dos direitos conquistados há bastante tempo, podendo assim atuar de forma eficiente em sua manutenção.

A pena para aqueles que praticam os atos descritos no caput do artigo 154-A do Código Penal, assim como, aquele que oferece, distribui, vende ou difunde programa que facilite ou faça a prática descrita no caput, se realizada será pena de detenção de três meses a um ano, ou multa.

O Centro de Apoio Operacional Criminal do Ministério Público de São Paulo, afirma ainda que a mencionada lei possui deficiências que deixam frágeis a obtenção de uma resposta por parte do Estado, tendo em vista os ataques cibernéticos, deficiências estas que vão muito além de uma má redação, mas também se estende a má elaboaração da pena a ser aplicada:

> Além das imperfeições na redação dos tipos, as penas cominadas na nova lei são ínfimas se considerada a potencial gravidade das condutas incriminadas, bastando dizer que um ataque de denegação de serviço pode colocar em risco vidas de uma população inteira. Implicam, por outro lado, a competência do Juizado Especial Criminal, cujo procedimento sumaríssimo é incompatível com a complexibilidade da investigação e da produção da prova de crimes de alta tecnologia (perícia no dispositivo informático afetado, por exemplo)[38]

Conforme todo o demonstrado até o presente momento, os crimes virtuais estão se tornando, cada vez mais, uma realidade devido ao acesso e o combate contra os agentes criminosos, não é feito de forma simples e de fácil solução para tal problema, demanda uma investigação bem apurada e muito eficiente.
Encerra o Ministério Público de São Paulo, afirmando que a Lei 12.737/12 não consegue, por si só, desestimular aqueles que abusam das facilidades tecnológicas,

[38] Ministério Público de São Paulo. **Novas Leis de crimes cibernéticos entra em vigor.** Centro de Apoio Operacional Criminal. Disponível em:<http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR>. pdf. Acesso em: 05 de junho de 2019.

bem como não é capaz de investigar e chegar até aqueles que praticam tais atos ilícitos usando da internet e dispositivos informáticos.

O parágrafo primeiro do artigo 154-A, “na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput”, também possui uma lacuna em sua disposição legal, tendo em vista que, a ação penal do crime, seja aquele definido no caput, ou no parágrafo primeiro, estabelecido pelo artigo 154-B, define que tais crimes somente se procederão mediante representação da vítima, exceto em algumas hispóteses relacionadas a Administração Pública direta ou indireta.

De acordo com Rogério Sanches Cunha, a vítima definida no parágrafo primeiro é indeterminada, tendo em vista que, diferente do caput, onde neste último a vítima é facilmente identificada, no presente caso, não tem como se definir quem foi a vítima, pois a punição cairá sobre aquele que vende programa que facilita o crime descrito no caput. Sendo assim, não conseguindo existir tal definição, como se procederá a punição penal, já que a vítima deverá fazer a representação?[39]

Rogério Sanches ensina ainda que existem duas correntes para este caso, a primeira diz que tal parágrafo é letra morta, pois houve desatenção do legislador por não ter previsto a possibilidade da ação penal pública incondicionada; a segunda corrente afirma que no silêncio do legislador deverá se proceder com a ação penal pública incondicionada.[40]

Sendo assim, restou claro o quão complexo é o artigo da referida lei, e na mesma medida, o quão falha é sua redação, deixando uma lacuna em questões que deveriam ser tratadas de forma diferente, e não conseguindo agir de forma efetiva na proteção da dignidade da pessoa humana, bem como, em sua privacidade.

[39] CUNHA, Rogério Sanches. **Art. 154- A CP: Violação de segredo profissional**. Disponível em: <http://www.youtube.com/watch?v=YcOv-yv_H2c>. Acesso em: 08 de novembro de 2018.
[40] CUNHA, Rogério Sanches. **Art. 154- A CP: Violação de segredo profissional**. Disponível em: <http://www.youtube.com/watch?v=YcOv-yv_H2c>. Acesso em: 08 de novembro de 2018.

CONSIDERAÇÕES FINAIS

Em nossa sociedade atual já se tornou uma dependência o uso dos computadores e internet para nossa comunicação. Ao passo de que, a sociedade está ligada diretamente com o avanço tecnológico que, sem dúvidas, nos trouxe facilidades. No sentido de que, não se esperavam que a internet fosse avançar tanto ao passo de ser usada com um meio para a prática de atos ilícitos, e as leis existentes, por si só, não fossem capazes de punir tais práticas.

Internet, como o próprio nome já diz, trata-se de conexão, ou seja, ligação, união, e, neste campo, ficou claro que devido as facilidades que esta tecnologia possui, enfretamos um problema do acesso indevido e os danos que eles podem causar a nossa esfera privada e nossa vida íntima, com esse grande avanço, nossa privacidade fica, por muitas vezes, expostas. Informações que vão desde senhas de redes sociais à até mesmo sigilos bancários, não esquecendo, assim, da intimidade, no sentido restrito da palavra, presente em nossos dispositivos informáticos.

Cabe ao Estado, juntamente com a sociedade, a manutenção do direito a privacidade. Por parte do Estado entende-se a criação de mecanismos que consigam garantir a liberdade individual, ou seja, a não restrição da liberdade, com a defesa da vida privada no que diz respeito a meios que visam protege-la. Em relação ao cidadão, suas atitudes deverão ser diárias, acompanhando o desenvolvimento social e tecnológico, bem como observar os males que isso pode trazer, não para criar um isolamento da sociedade, mas sim, o conhecimento das ameaças, e o prigo que a exposição em excesso poderá causar, é possível a diminuição da ação opressora que busca violar a esfera privada.

A lei 12.737/12, criada pelo Brasil, para os fins de aumentar a proteção à sociedade e diminuir práticas ilícitas no ambiente virtaul, mostrou-se, claramente, insuficiente, tendo em vista sua má elaboração. Neste trabalho, a hipóstese aqui apresentada deixou bem claro essa lacuna existente no dispositivo legal acima mencionado, lacuna esta que, como fora já mencionado, trará situações atípicas deixando os cidadãos vulneráveis e sem uma resposta contra aqueles que praticam tal ato.

No presente trabalho, fora abordada a fragilidade do texto da lei, e observa que esse texto não está restrito apenas a violação de mecanismos de defesa, mas também a invasão de dispositivo informático alheio, o que aumenta ainda mais os riscos, pois

esta configuração está mais presente na sociedade, como dito anteriormente, em “lan house” ou outros estabelecimentos privados.

Devida a má elaboração da redação a Lei 12.737/12, restou-se claro o desconhecimento de nossos legisladores a respeito do tema do presente trabalho. Um projeto de lei, não é voltado e aprovado de forma rápida, sem nenhuma avaliação prévia, esse projeto não foi diferente, passou por várias etapas de avaliações, o que agrava ainda mais o problema, pois, acaba por nos colocar em um situação onde aqueles que devam criar mecanismos que nos garantem proteção, não possuem o conhecimento necessário para tal ato.

Os crimes virtuais são reais e infelizmente os casos vêm crescendo em nosso meio de forma alarmante.

REFERÊNCIAS BIBLIOGRAFICAS

ASSIS, José Francisco de. **Direito à privacidade no uso da internet**: omissão da legislação vigente e violação ao princípio fundamental da privacidade. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=12848> . Acessado em 11 de maio de 2015.

ALEXY, Robert.**Teoria discursiva do direito**. Organização, tradução e estudo introdutório Alexandre Travessoni Gomes Trivisonno. 1. ed. Rio de Janeiro: Forense Universitária, 2014.

BATTAGLINI, apud, JESUS, Damásio E. de**. Direito Penal**. São Paulo: Saraiva, 2003.

BECCARIA, Cessare. **Dos delitos e das penas**. Trad. Neury Carvalho Lima. São Paulo: Hunter Books, 2012.

BONAVIDES, Paulo. **Curso de Direito Constitucional** . 26. ed. São Paulo: 2011.

BONFIM, Edilson Mougenot- **Curso de Processo Penal**/Edilson Bonfim Mougenot-10.Ed.-São Paulo:2015

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado, 1988.

BRASIL. STF. **HC nº 84.203/RS.** Relator: Min. Celso de Mello. Informativo STF nº 366. Decisão: 19 outubro 2004.

BRASIL. **PROJETO DE LEI 2793 DE 2011**. Disponível em: <http://www.camara.gov.br/proposiçõesWeb/prop_mostraintegra?codteor=944218&filename=PL+2793/2011>. Acesso em 30 de outubro de 2018.

BRASIL. **Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto

-lei/Del2848compilado.htm>. Acesso em 12 de novembro de 2018.

BRITO, Auriney. **Direito Penal Informático.** São Paulo: Saraiva, 2013.

CANOTILHO, J.J.Gomes. **Direito Constitucional**. Coimbra: Almedina, 1993.

CAPEZ, Fernando. **Curso de Direito Penal: Parte Geral**. V.1.16 ed. São Paulo: Saraiva, 2012.

CAPEZ, Fernando**. Código Penal Comentado**. Fernando Capez, Stela Prado.- 6. Ed.- São Paulo: Saraiva, 2015.

CARVALHO, Kildare Gonçalves. **Direito constitucional.** 17. ed. Belo Horizonte: Del Rey, 2011.

COSTA, Renata. **Como surgiu a Declaração dos Direitos do homem e do cidadão**. Disponível em: http://novaescola.org.br/conteudo/320/como-surgiu-a-declaracao-dos-direitos-do-homem-e-do-cidadao. Acesso em: 12 de outubro de 2016.

CUNHA, Rogério Sanches. **Art. 154- A CP: Violação de segredo profissional**. Disponível em: <http://www.youtube.com/watch?v=YcOv-yv_H2c>. Acesso em: 08 de novembro de 2018.

Disponível em: <http://www.planalto.gov.br/ccvil_03/decretolei/Del2848compilado.ht

m>. Acesso em 02 de novembro.

FERRAJOLI, Luigi. **Direito e razão – Teoria do Garantismo Penal**. São Paulo: Editora Revista dos Tribunais, 2010.

FERREIRA, Ivete Sensive. **A criminalidade Informática.** Bauru: Edipro, 2000.

FILHO, Casado. **Coleção saberes do direito: Direitos fundamentais**. São Paulo: Saraiva, 2012.

FONTELES, Samuel Sales. **Direitos fundamentais para concursos**. Salvador: Juspodivm, 2014.

G1. **Carolina Dieckemann fala pela 1ª vez sobre fotos e diz que espera Justiç**a. Disponívem em: <HTTP://g1.com/pop-arte/notícia/2012/05/carolina-dieckemann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>. Acesso em 30 de outubro de 2018

GIMENES, Emanuel Alberto Sperandio Garcia. **Revista de doutrina da 4ª região** publicação da escola da magistratura do trf da 4ª região – emagis. publicado em 30.08.2013.

GRECO, Rogério. **Código Penal Comentado**. 7. ed. Niterói: Impetus, 2013.

JESUS, Damásio E. de. **Direito Penal**. São Paulo: Saraiva, 2003.

LIMA. Paulo Marco Ferreira. **Crime de Computador e Segurança Computacional**. 2. Ed. São Paulo: Atlas, 2013.

MACEDO. **Enciclopédia**. Saraiva do direito. Verbete: Princípio.

MALUF, Sahid- **Teoria Geral do Estado**/Sahid Maluf; atualizador prof. Miguel Alfredo MalufeNeto.-31 ED.- São Paulo: Saraiva, 2013.

MENDES, Gilmar Ferreira. **Curso de Direito Constitucional**. Gilmar Ferreira Mendes e Pauo Gustavo GonetBranco.-10. Ed. Ver. E atual.- São Paulo: Saraiva, 2015. (Série IDP).

Ministério Público de São Paulo. **Novas Leis de crimes cibernéticos entra em vigor.** Centro de Apoio Operacional Criminal. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR>. pdf. Acesso em: 05 de novembro de 2018.

MIRABETE, Julio Fabbrini. **Manual de Direito Penal**. V 31. Ed. São Paulo: Atlas, 2015.

MIRANDA, Jorge**. Manual de Direito Constitucional**. 4ª ed. Coimbra: Coimbra Editora, 1990, p.138, *apud* MORAES, Alexandre de. Direito constitucional. 10 ed. São Paulo: Atlas, 2001.

MORAES, Alexandre de**. Direito constitucional.** 22. ed. São Paulo: Ímpetus, 2007. p.49.

NOVELINO, Marcelo**. Manual de direito constitucional.** 9. ed. Rio de Janeiro: Forense, 2014.

PAESANI, Liliana Minardi (Coord). O direito na sociedade de informação. São Paulo: Atlas, 2007.

SARLET, Ingo Wolfgang. **Constituição e Proporcionalidade: o direito penal e os direitos fundamentais entre proibição de excesso e de insuficiência**. Revista de Estudos Criminais, n. 12, ano 3, Sapucaia do Sul, 2003, p.86 segs. *Apud* STRECK, Lenio Luiz. A dupla face do princípio da proporcionalidade e o cabimento de mandado de segurança em matéria criminal: superando o ideário liberal-individualista-clássico.

VELLOZO. Jean Pablo Barbosa. **Crimes Informáticos e criminalidade contemporânea**. Disponíevl e,: <http://jus.com.br/artigos/44400/crimes-informaticos-criminalidade-contemporanea/1>. Acesso em 29 de outubro de 2018.

VIANNA, Túlio; MACHADO, Felipe. **Crimes Cibernéticos**. Belo Horizonte: Fórum, 2013.

WENDT, Emerson; JORGE; Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. 2. Ed. Rio de Janeiro: Brasport, 2013.

ZAPAROLI, Rodrigo Alves. **Comentários à Lei nº 12.737/12**. Disponível em: <http://www.conteudojuridico.com.br/artigo,comentarios-aleino1273712,43118.html>. Acesso em 23 de outubro de 2018.