CENTRO DE EDUCAÇÃO SUPERIOR DE INHUMAS

FACULDADE DE INHUMAS

CURSO DE DIREITO

WELINGTON VAZ DA COSTA FILHO

CRIME INFORMÁTICO

INHUMAS-GO

2019

WELINGTON VAZ DA COSTA FILHO

CRIME INFORMÁTICO

Monografia apresentada ao Curso de Direito da Faculdade de Inhumas (FacMais), como requisito parcial para a obtenção do título de Bacharel em Direito.

Professor orientador: Ms. Camila Santiago Ribeiro

INHUMAS – GO

2019

WELINGTON VAZ DA COSTA FILHO

CRIME INFORMÁTICO

AVALIAÇÃO DE DESEMPENHO DOS ALUNOS

Monografia apresentada ao curso de Direito da Faculdade de Inhumas (Fac-Mais) como requisito para obtenção do título de Bacharel em Direito.

Inhumas, 16 de maio de 2019

BANCA EXAMINADORA

_____

Prof. Me. Camila Santiago - FacMais
(Orientador e presidente)

_____

Prof. Me. Rodrigo - FacMais
(Membro é convidado)

Dados Internacionais de Catalogação na Publicação (CIP)

BIBLIOTECA FACMAIS

C837c

COSTA FILHO, Welington Vaz da
CRIME INFORMÁTICO/ Welington Vaz da Costa Filho. – Inhumas: FacMais, 2019.
36 f.: il.

Orientadora: Camila Santiago Ribeiro.

Monografia (Graduação em Direito) - Centro de Educação Superior de Inhumas - FacMais, 2019.

Inclui bibliografia.

1. Rede de internet; 2.Crimes cibernéticos; 3.Máxima e mínima punição. I. Título.

CDU: 34

“Dedico este trabalho primeiramente a Deus, por ser essencial em minha vida, autor do meu destino, meu guia, socorro presente na hora da angústia, Ao meu pai Welington Júnior, e minha mãe Maria do Carmo e aos meus irmãos.”

“Aos meus pais, irmãos, minha esposa Vanessa Cristina, e a toda minha família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa da minha vida.”

“Agradeço aos meus professores e colegas de classe pela harmoniosa convivência em muitos aprendizados e troca de experiências”.

RESUMO

Na atual realidade da era digital, estamos vivenciando um período em que a tecnologia está mais aprimorada a todos os tipos de pessoas tornando mais fácil a sua utilização, disto as mentes criminosas estão cada vez mais aplicando fraudes nesta área digital, pelo fato de que constantemente aumenta-se o índice de usuários da rede de internet. Mesmo que existam algumas penalizações por essas condutas os crimes cibernéticos estão multiplicando os seus cometimentos, de logo a sociedade se encontra no meio de um conflito no qual existem duas posições, a máxima punição ainda mais dos crimes virtuais, ou a diminuição dos crimes visando à educação como forma de solucionar este conflito. Neste sentido, o presente trabalho de pesquisa pretende enfrentar esse conflito.

Palavras-Chave: Rede de internet; Crimes cibernéticos; Máxima e mínima punição.

ABSTRACT

In the current reality of the digital age, we are experiencing a period in which technology is improved to certain types of people making its use easier, criminal minds are increasingly applying fraud in this digital area, as it constantly increases is the index of users of the internet network. Even though there are some penalties for these conduct cyber crimes are multiplying their commitments, soon the society is in the middle of a conflict in which there are two positions the maximum punishment even more of virtual crimes, or the reduction of crimes aimed at education as a way to resolve this conflict. In this sense the present research work intends to face this conflict.

KEY WORDS: Internet network; Cyber crimes; Maximum and minimum punishment.

SUMÁRIO

INTRODUÇÃO

A internet se originou de um fruto militar, embora naquela época fosse só transmitida internamente, com o objetivo de possibilitar o mais rápido possível os fatos de tratamento militares. Aconteceu que, as classes governamentais perceberam que essa ferramenta poderia facilitar grandes avanços e com isso transmitir, de forma mais célere a comunicação entre a sociedade. (DIANA, 2018).

Como a internet se propagou de forma gradativa, nos resta dizer que quase toda a população do mundo inteiro se encontra conectada via internet. De acordo com os dados do IBGE de 2016, publicado pelo G1, menciona que são 116 milhões de brasileiros conectados na internet, somando 64,7% da população (SIMÕES, H. 2018).

E de fato que a internet nos dias de hoje tem muita serventia, e o caso da facilidade em comunicação, nas buscas pessoais, nos estudos e muito mais, trouxe inovações como as redes sociais que fez com que muitos indivíduos se conectarem com outros, mesmos distantes.

Aliada com os dispositivos móveis possibilitou-se que muitos indivíduos que não tinham condição de adquirir um computador em casa, obtivessem em mãos a tão sonhada internet, além de poderem transitar e se comunicarem pelo famoso whatsapp e o facebook.

Porém, esta grande evolução cibernética abriu possibilidades para a criminalidade, por ser uma ferramenta tanto para bens de serviço em geral, quanto para meio da convivência, permitindo como falado anteriormente, facilitar a comunicação entre os indivíduos socialmente logados nessa grande rede cibernética.

Diante disso, percebe-se que os crimes informáticos têm muita relevância nos dias atuais pela popularização que a internet adquiriu, fazendo com que se tornasse necessária a classificação dos crimes virtuais e a distinção dos autores destes crimes.

Nesta perspectiva os crimes virtuais foram tipificados pelas Leis nº 12.737/12 (Lei Carolina Dieckmann) e nº 12.735/12 (Lei Azeredo), as quais criminalizar algumas condutas praticadas por meio da internet, porém mesmo com as tipificações que são recentes os crimes virtuais continuam acontecendo.

Busca-se nesta pesquisa responder a seguinte pergunta: Como é possível a erradicação dos crimes informáticos, criminalização ou educação? A metodologia a ser utilizada no presente artigo será de cunho científico, tendo por base o método dedutivo, utilizando o procedimento bibliográfico, realizado por meio de levantamento em material teórico e jurídico em bibliotecas institucionais e acervo particular. Além destes, outros recursos, como jornais, periódicos e documentos digitais (e na internet), também serão consultados.

O primeiro capítulo terá como foco a prática dos crimes pela internet. Nele será abordada a classificação dos crimes cibernéticos, quem são os sujeitos envolvidos nessas práticas criminosas, bem como as principais normas que passam a dispor sobre os crimes informáticos.

No segundo capítulo será conceituada a ideia de direito penal mínimo e direito penal máximo, visando esclarecer qual posicionamento se mostra o mais adequado no contexto brasileiro.

Já no terceiro capítulo serão abordados os crimes cibernéticos no Brasil, o qual terá como foco a criminalização e o cenário atual, bem como a criminalização ou a educação como possíveis soluções para a diminuição da prática dos crimes informáticos. Fazendo menção a junção de todos os capítulos para buscar enfrentar o problema da pesquisa.

Como referencial teórico o trabalho abordará três eixos temáticos: i) prática dos crimes pela internet; ii) direito penal mínimo e direito penal máximo: fundamentos do poder-dever de punir do Estado; iii) a máxima criminalização das condutas praticadas pelo uso da internet; tendo com luz a reflexão de alguns autores sobre o assunto:

Nesse sentido, a partir dos autores Mário Furlaneto Neto e Damásio de Jesus busca-se compreender a prática dos crimes pela internet. No que se refere ao direito penal mínimo, utilizou-se aqui os conceitos apresentados por David Garland e Luiz Luisi, enquanto os ensinamentos de Louise da Silva Trigo (2019) e Fabrízio Rosa e Silveira Filho (2011) auxiliaram na compreensão do conceito de direito penal máximo.

Ainda, para tratar do direito penal máximo no contexto brasileiro, buscou-se auxílio em A. S. Franco e Wilson dos Santos da Silva. Por fim, Eudes Quintino de Oliveira Junior e Jason Albergaria apresentam a máxima criminalização

das condutas praticadas pelo uso da internet, no Brasil e no cenário atual.

1.Prática dos crimes pela internet

Nos Estados Unidos, em 1969, foi criada a internet chamada anteriormente de Arpanet, tendo como função conexão dos laboratórios de pesquisa, entretanto, no mesmo ano um professor da universidade da Califórnia enviou um e-mail para um colega em Stanford sendo o primeiro e-mail da história, segundo Werner, (2001).

Já no Brasil, o histórico da internet foi bem atrasado em 1988, pela (Fapesp) Fundação de Amparo à Pesquisa do Estado de São Paulo e (LNCC) Laboratório Nacional de Computação Científica no Rio de Janeiro. Porém só em 1991 foi disponibilizado o uso para o público em geral. Menciona (TEIXEIRA, 2007, p.9).

Daí em diante a internet se alastrou, tornando-se indispensável na vida dos seres humanos, e, hoje se encontra bastante em comento, pois seu meio de utilização está sendo usado para crimes pela facilidade e por conta que todas as pessoas se encontram conectadas neste ciberespaço·. Dispositivos como computadores, tablets, celulares, hoje tomou toda a população, e por esse motivo aumentou-se os crimes de informática, na qual essa utilização fez com que os maliciosos se aproveitassem dessa expansão para praticarem crimes.

Com a propagação dos serviços de internet pelo mundo, e a facilidade de acesso a toda a população, o ambiente virtual tornou-se propício para a prática de crimes virtuais.

O histórico desses crimes, se remonta a década de 1985 que, por sua vez, foi definido o termo “Hacker” pela primeira vez, portanto, sendo aquele indivíduo com capacidades técnicas, que promovem invasões, difusões de pragas virtuais. Porém, é de se analisar que hoje em dia, não se precisa tanto ter um conhecimento técnico a mais para se tornar um Hacker, pois atualmente na própria internet se ensinam técnicas que são prejudiciais às outras pessoas RODRIGUES (2019).

Segundo Queiroz (2008) citado por Ribeiro (2015) menciona que quando a internet em dezembro de 1994, foi liberada comercialmente no Brasil, a intenção era a facilitação da comunicação, entre as pessoas, nos países, nas empresas, a fim de aprenderem umas com as outras. Porém com a facilidade que a internet propicia, abriu brechas para a criminalidade.

Mário Furlaneto Neto condizente com a ideia diz:

> […] Os transgressores da lei penal logo viram no computador e na Internet formidáveis instrumentos à consecução de vários delitos. Como se não bastasse, essa revolução tecnológica também deu azo à criatividade delituosa, gerando comportamentos inéditos que, não obstante o alto grau de reprovabilidade social, ainda permanecem atípicos (NETO, p. 264).

Entretanto, algumas coisas mudaram levando para seara dos dias atuais no qual já se existem tipificações a essas condutas reprováveis, embora que na medida em que se apunhalam elas se aglomeram ainda mais, fazendo menção que a cada dia, horas, segundo um crime virtual está sendo cometido no mundo.

1.1. CLASSIFICAÇÃO DOS CRIMES INFORMÁTICOS

Os crimes de informática são classificados em próprios e puros, e também em impróprios e impuros, vejamos:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial (FERREIRA apud CARNEIRO, 2012, [n.p.]).

Na realidade, a classificação mais adequada é que os crimes podem ser próprios e impróprios (ADENEELE, 2019).

Os crimes virtuais próprios são aqueles em que o sujeito ativo manipula o sistema informático do sujeito passivo, utilizando o sistema do computador como seu objeto e meio de execução.

Conceitua corroborando, em suas valiosas lições Damásio Evangelista de Jesus (apud CARNEIRO, 2012, [n.p.]) menciona:

> Crimes eletrônicos puros ou próprios são aqueles que são praticados por computador e se realizam ou se consomem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

Nestes crimes não está só a ideia de invasão de dados não autorizados, no entanto, todas as interferências em dados informatizados é o exemplo destas:

invasão de dados armazenados no computador com intenção de alterar, modificar, inserir dados falsos, ensejando, atingir diretamente o *software*[1] e *hardware*[2] do computador. Porém só pode ser realizado por computador e seus periféricos.

Colaborando com esta ideia, Marco Túlio de Viana, diz que os crimes virtuais próprios “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)” (VIANA, 2003 apud CARNEIRO, 2012).

Disto, vê se que a conduta exposta aqui é a invasão do computador, necessitando deste para sua consumação, a qual sem o equipamento, isto é o computador e seus periféricos nada aconteceriam. O cometimento deste tipo de crime visa se obter por meios informáticos, exemplos: invasão de computador, invasão nas redes sociais, e danificação do computador por invasão de vírus, alteração de documentos e muitos outros.

Já o crime virtual impróprio é aquele que se utiliza do computador para se obter a consumação do ato, necessitando da máquina como meio de instrumento para se realizar os atos ilícitos já tutelados. Disto, percebe-se que os crimes já tipificados na norma penal podem ser cometidos com a utilização do computador e da rede.

Diante disso, menciona o jurista Damásio E. de Jesus (2012 apud CARNEIRO, 2012, [n.p.]). In verbis:

> Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não computacionais ou diversos.

O crime informático impróprio são aqueles crimes que visam atingir um bem jurídico comum, como um patrimônio, e se utiliza dos sistemas informáticos apenas como animus operandi, ensejando, um novo meio de execução (SCHMIDT, 2019).

---

[1] Software: programas que comandam o funcionamento do computador. Meus Dicionários, Disponível em: https://www.meusdicionarios.com.br/software acessado em 02 de Janeiro de 2019.

[2] Hardware: são as partes que podemos ver do computador, ou seja, todos os componentes da sua estrutura física como o monitor, o teclado, o gabinete e o mouse. Significados Br. Disponível em: https://www.significadosbr.com.br/hardware acessado em 02 de Janeiro de 2019.

1.2 SUJEITOS DOS CRIMES INFORMÁTICOS

1.2.1 Sujeitos Ativos

Os sujeitos ativos e passivos dos cibercrimes são diferenciados e classificados pela doutrina. De acordo com professor Damásio Evangelista de Jesus, “sujeito ativo é quem pratica o fato descrito na norma penal incriminadora”. (JESUS, 2005, p. 147)

Sabendo disso, o sujeito ativo é aquele que usa do meio informático, este “meio” sendo a parte física do computador em si, ou quando usa do computador pelo motivo da internet, para se obter sua conduta criminosa.

Para facilitar a compreensão, mencionaremos aqui os diferentes tipos de sujeitos ativos destes crimes.

Hacker é um termo muito utilizado para mencionar criminosos virtuais, porém muitos deles, mesmo que sejam altamente habilidosos nesta área, não a usam para prática criminosa. É o exemplo do técnico de computador, de programa e sistema de segurança (FREITAS; SILVA. 2019).

Mencionam também Alessandra Mara Freitas e Cristian Kiefer Silva (2019) que muitos desses sujeitos ativos, cometem estes crimes por curiosidade, necessidade profissional, vaidade, patriotismo, ativismo ou até mesmo crime. Já aquele Hacker que comete crimes a fins imorais, ilegais ou prejudiciais é chamado de Cracker.

Segundo Henrique Cezar Ulbrich e James Della Valle citado por Alessandra Mara Freitas e Cristian Kiefer Silva (2019) afirmam que os crackers são denominados “hackers do mal” ou “hackers sem ética” e que esses indivíduos são especializados em burlar as senhas de software comerciais a fim de pirateá-los.

Além de serem ótimos programadores, pela razão de invadirem computadores e sites com propósito de crime, eles criam programas que infectam ou destroem por completo os sistemas da vítima sem deixar vestígio. É um habilidoso nato, faz uso de ferramentas que percebe a vulnerabilidade do sistema que quer invadir. Tendo totais noções de improvisação se algo acontecer (ULBRICH, 2004, p.30).

Sobre as reflexões de Henrique Cezar Ulbrich e James Della Valle citado por Alessandra Mara Freitas e Cristian Kiefer Silva (2019), Wannabe é o indivíduo que deseja ser hacker, porém não sabe como iniciar, só tem uma noção intermediária.

Phreaker são os indivíduos que hackeiam as redes telefônicas, (phone + freak ou phreak). Já no Brasil há muito pouco tempo que eles agem aqui, porém com essa proliferação de telefones eles vieram à tona, clonando celulares e até mesmo fazendo escutas telefônicas via frequência (FREITAS; SILVA. 2019).

Segundo Henrique Cesar Ulbrich e James Della Valle (2004, p. 30) conceitua que phreaker é o *hacker* de sistemas telefônicos, que é exímio conhecedor de eletrônica e telefonia e pode fazer chamadas de qualquer local sem, contudo, pagar por elas.

O Carder é aquele sujeito especializado em fraude de cartão de crédito. Conseguem obter lista de cartões válidos em sites que utilizam, gerando numeração falsa que é reconhecida por ter clonado ou roubado os cartões das vítimas, os sujeitos passivos que falaremos posteriormente Conforme mensura Henrique Cesar Ulbrich e James Della Valle (2004, p. 30).

Os carders costumam trabalhar em grupos ou sozinhos na internet com a intenção de conseguir dados de cartões de créditos para fraude on-line. Os que trabalham em grupos chamados de (*carding*) eles reúnem em salas de bate papo IRC (*internet realy site)* em servidores de máquinas vulneráveis. Habitualmente um dos carder analista determinado shopcar vai em busca de vulnerabilidade, com intenção principal de baixar (download) o banco de dados com os dados do cliente da loja (vítima). Após a extração dos dados da vítima, o card utiliza os dados para compra em outra loja (FREITAS; SILVA. 2019).

O War Drive é a denominação mais recente visando os demais, usam da vulnerabilidade das redes sem fio, para se conectar a elas. De acordo com quem nos ensina Henrique Cesar Ulbrich e James Della Valle (2004, p. 30).

1.2.2 Sujeitos Passivos

“Sujeito passivo é o titular do interesse cuja ofensa constitui a essência do crime. Para que seja encontrado é preciso indagar qual o interesse tutelado pela lei penal incriminadora” (JESUS, 2005, p. 153). Logo o sujeito passivo é o agente que sofre a ação, ou o titular do interesse jurídico, a vítima.

Outro doutrinador renomado Rogério Greco (2010, p 54) nos ensina que o sujeito passivo divide-se em formal e material, sendo aquele sempre o Estado, por ilícito cometido, sofrendo pela sua desobediência. E este o sujeito passivo material é o titular do bem ou do interesse jurídico tutelado a qual recai a conduta delitiva.

Sujeito passivo é a vítima do hacker que usa da vulnerabilidade do computador para satisfazer seus anseios, do cracker para infundir e destruir os programas do computador, do phreaker para sabotar telefones, e do carder que utiliza dos dados dos seus cartões de créditos.

1.2.3. Criminalização Antes e Após as Leis nº 12.737/12 (Lei Carolina Dieckmann) e nº 12.735/12 (Lei Azeredo).

Quando se fala em legislação antes da promulgação da lei nº 12.737/12, já se imagina que o país vivia uma baderna sem leis para punir estes tipos de crimes, porém muitos não sabem que as leis brasileiras alcançam cerca de 90 a 95% dos crimes virtuais. Pois os crimes virtuais próprios, ou seja, aqueles praticados pelo computador quase que habitualmente já são tipificados pelo código penal (ADENEELE, 2019).

Diante a essa situação a Delegacia de Repressão aos Crimes de Informática (DRCI), fizeram um quadro elencando alguns exemplos de crimes cometidos por meio da internet e que já possuem previsão legal (ADENEELE, 2019).

Calúnia	Art. 138 do código penal (“C.P.”)
Difamação	Art. 139 do C.P.
Injúria	Art. 140 do C.P.
Ameaça	Art. 147 do C.P.
Furto	Art. 155 do C.P.
Dano	Art. 163 do C.P.
Apropriação indébita	Art. 168 do C.P.
Estelionato	Art. 171 do C.P
Violação ao direito autoral	Art. 184 do C.P.

Pedofilia	Art. 247 da Lei 8.069/90 (Estatuto da Criança e do Adolescente)
Crime contra a propriedade industrial	Art. 183 e segs. Da Lei 9.279/96
Interceptação de comunicação de informática	Art. 10 da Lei 9.296/96
Interceptação de E-mail Comercial ou Pessoal	Art. 10 da Lei 9.296/96
Crimes contra software “Pirataria”	Art. 12 da Lei 9.609/98

Frente a este quadro numerado de crime, percebemos que mesmo antes da legislação atuante já se haviam tipificações, mas que não conseguia absorver todos os tipos de crimes que se inicia a cada dia.

A Constituição Federal menciona em seu art. 5º, XXXIX que “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”, demonstra que para se punir os crimes informáticos é indispensável que a conduta penal venha se adequar às normas já existentes (NUNES, 2012).

Logo suas lacunas também devem ser preenchidas. Nos dias de hoje é de fundamental importância que o conceito de informática seja incorporado à legislação vigente (NUNES, 2012).

Também nos alude Raphael Rosa Nunes (2012), que os primeiros manejos vieram do Plano Nacional de Informática e Automação (Conin), Lei n. 7. 232/84, na qual tratava das diretrizes da informática no Brasil, e logo após veio a Lei n. 7. 646/87. Sendo esta última revogada pela Lei n. 9. 609/98, a qual foi a primeira a mencionar infrações de informática em seu ordenamento, sendo possível citar alguns artigos:

> Art. 12. Violar direitos de autor de programa de computador:
> Pena – Detenção de seis meses a dois anos ou multa.
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
> Pena – Reclusão de um a quatro anos e multa.

> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
>
> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
>
> I – quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
>
> II – quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
>
> § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Com o advento de inúmeros crimes, mesmo com as tipificações gerais existentes, foi sancionado em 2012 duas leis específicas instituindo penas e alterando o atual código penal para punir condutas no mundo virtual.

A primeira é a Lei dos Crimes Cibernéticos (12.737/12), conhecida como Lei Carolina Dieckmann, por ter sido vazadas as fotos da atriz na mídia e com isso foi tipificado atos como invadir computadores (*hacking*), roubar senhas**,** violar dados de usuários e divulgar informações privadas (como fotos, mensagens etc). (CNJ, 2018)

Entretanto, mesmo que a Lei tenha ganhado espaço pelo caso da atriz, o texto já era reivindicado pelo sistema financeiro, tendo em vista o grande cometimento de golpes e roubos de senhas pela internet. (CNJ, 2018)

Os crimes instituídos no Código Penal e previstos na Lei de Crimes Cibernéticos (Artigo 154-A e art. 298). São:

> **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.
>
> § 3º Se 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 obtidos.
>
> § 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.
>
> Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:
>
> **Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.**
>
> Art. 266.
>
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.
>
> **Falsificação de documento particular.**
>
> Art. 298.
>
> **Falsificação de cartão.**
>
> Parágrafo único. Para “fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito”.

A segunda é a Lei 12.735/12 que determina que sejam instaladas delegacias especializadas em combate aos crimes virtuais. (CNJ, 2018)

Contudo em 2014 foi sancionado o Marco Civil da Internet (Lei 12.965/14), a qual regula os deveres e direitos dos internautas, protegendo os dados pessoais e a privacidade dos usuários. Fazendo menção que somente por ordem judicial pode se haver quebra de dados e informações privadas existentes em redes sociais ou em sites. (CNJ, 2018)

Vimos que mesmo antes da legislação em vigor, já havia meios para que fosse possível a atuação do poder de punir, e consequentemente com as legislações

atuais. Contudo, esta punição no que se observa até então está sendo positiva? Diante disto, enfrentaremos esta questão nos próximos capítulos.

1. DIREITO PENAL MÍNIMO E DIREITO PENAL MÁXIMO: FUNDAMENTOS DO PODER-DEVER DE PUNIR DO ESTADO.

2.1. DIREITO PENAL MÍNIMO

Na sociedade de hoje, parece comum a convivência da criminalidade com a sociedade. O policiamento privado, as políticas de lei e ordem, e a crença da efetivação do cárcere são comuns. (GARLAND, 2008, P. 41)

Segundo Carolina Freitas Paladino (2019), quanto mais se pune, mais violência se tem, mais crime surge. Desta forma o Direito penal não consegue e nunca conseguirá resolver estas relações.

Disto Raúl Cervini, (1995, p.69) diz que é possível atribuir algumas causas que levam a uma ineficiência da justiça sendo elas:

> A inflação legislativa; a existência de competentes da administração fragmentados e incomunicáveis entre si; a sobrecarga dos tribunais; a ineficiência das penas clássicas; a aplicação de tratamentos contraproducentes; a resistências dos sistemas tradicionais ineficientes; a demora na administração da justiça; e os próprios custos.

Daí gera um fenômeno de caos, fazendo com que propostas sejam criadas para conter esses movimentos, como o chamado “Minimalismo Penal”. O minimalismo penal visa diminuir os usuários dos sistemas prisionais, alcançando a prisão somente os sujeitos que acometem os crimes mais graves, além de aplicar penas alternativas (FREITAS 2019).

Para corroborar com a ideia parte da hipótese que:

> A violência é, desde logo, um problema social, mas também um problema semântico, porque somente a partir de um determinado contexto social, político e econômico pode ser valorada, explicada, condenada ou defendida. Não há, pois, um conceito de violência estático ou a-histórico que pode dar-se à margem do problema social em que surge. Não existe também uma fórmula mágica, um critério objetivo que seja válido para todos os tempos e lugares, que nos permita valorar aprioristicamente, a bondade e a maldade de um determinado tipo de violência. (CONDE, 2005, p. 3-4).

Outro doutrinador que colabora com ideia do minimalismo penal e o Luiz Luisi (2003, p. 38-39) que menciona um dos princípios que informam o direito penal é a última *ratio*, a qual traduzida à regra de que as relações sociais serão reguladas

pelos outros ramos de Direitos, cabendo só em último caso a aplicação do Direito Penal.

Disto, percebe que só será imposta a punição se colaborar com o meio necessário à proteção ao bem jurídico, porém deve se desaparecer se obtiver pena mais branda. (LUISI, 2003, p. 38-39).

A última *ratio,* valida o Direito Penal somente quando não há outra forma do convívio social ou fracassarem as políticas sociais. Assim o Direito Penal intervém para cessar a violência. (QUEIROZ, 2002, p. 69).

Entretanto, percebemos que na nossa realidade não é assim que acontece, o direito penal vem sendo usado aplicado indistintamente, não de forma que o princípio da ultima *ratio* estabelece.

1.2. DIREITO PENAL MÁXIMO

Ao se falar em aumento de criminalidade, logo se lembra do Direito Penal, por este ser a resposta a uma suposta violência globalizada. Disto se criam novas leis, aumentam-se as penas, restringem-se às garantias fundamentais, fazendo assim certas pessoas como “inimigas” do Estado (TRIGO, 2019).

O primeiro aparecimento do movimento de lei e da ordem foi na década de 1970 nos Estado Unidos, dando como resposta ao aumento da criminalidade recorrente, de acordo com Franco (2005, p.84).

Esta corrente se fortaleceu e teve como suporte para se expandir por alguns motivos que se ocorreram na década de 1970 e 1980:

> [...] a) no incremento da criminalidade violenta direcionada a segmentos sociais mais Privilegiados e que até então estavam indenes a ataques mais agressivos (sequestro de pessoas abandonadas ou de alto estrato político ou social, roubos a estabelecimentos bancários etc); b) no terrorismo político e até mesmo no terrorismo imotivado, de facções vinculadas tanto à esquerda como à extrema direita; c) no crescimento do tráfico ilícito de entorpecentes e de drogas afins; d) no avanço do crime organizado pondo a mostra a corrupção e a impunidade; e) no incremento da criminalidade de massa (roubos, furtos etc) que atormentam o cidadão comum; f) na percepção do fenômeno da violência como dado integrante do cotidiano, omnipresente na sociedade; g) no conceito reducionista de violência, fazendo-o coincidir com o de criminalidade; h) na criação pelos meios de comunicação social de um sentimento coletivo e individual de insegurança e no emprego desses mesmos meios para efeito de dramatização da violência para seu uso político (FRANCO, 2005, p.84).

Destaca-se também que na década de 1990, houve uma campanha da lei e da ordem e assim se intensificaram com a criação da política *tolerância zero*, a qual foi guiada pelo prefeito de Nova York, Rudolph Giuliani, no qual ganhou repercussão por propagar a teoria das Janelas quebradas (ROSA; SILVEIRA FILHO, 2011).

Esta teoria entende que a repressão imediata e severa das menores infrações e desentendimentos em vias publica evita a possibilidade de grandes atentados criminais, pois demonstra que existe uma autoridade responsável pela manutenção da ordem. Disto, menciona Wacquant (2004, n.p.), “prender ladrões de ovos permite frear, ou simplesmente parar, os potenciais matadores de bois, pela reafirmação da norma e dramatização do respeito à lei”.

De logo, entende-se que os seguidores dessa teoria amparam que o meio para combater a criminalidade é iniciar-se pela rigorosa repressão e perseguição das pequenas infrações, pelo motivo de conter a violência pela raiz e evitar a “*primeira janela quebrada”* (ROSA; SILVEIRA FILHO, 2011, p. 34).

Segundo menciona Callegari; Dutra (2007) este movimento da lei e da ordem mesmo que exercia uma função puramente simbólica, trouxe tranquilidade à população e disto, acabou se expandindo e conquistando adeptos em vários países, por motivo que o endurecimento da legislação penal trouxe uma resposta a essa crescente criminalidade.

2.3. DIREITO PENAL MÁXIMO NO CONTEXTO BRASILEIRO

No Brasil, Louise Trigo da silva (2019) menciona que há uma legislação de emergência que tem o objetivo de acalmar a população, ou simplesmente conter um determinado tipo de criminalidade, pela relativização dos direitos e garantias fundamentais previstas na constituição.

Demonstrando o caráter repressivo que o direito penal vem adotando, exemplo este é a Lei dos Crimes Hediondos, que veio com o objetivo de dar respaldo à sociedade, entretanto sem nenhuma efetividade na seara do Direito Penal, alude Franco (2000, p.502):

> A Lei 8.072, na linha dos pressupostos ideológicos e dos valores consagrados pelo Movimento da Lei e da Ordem, deu suporte à ideia de que leis de extrema severidade e penas privativas de alto calibre são suficientes para pôr cobro à criminalidade violenta. Nada mais ilusório.

Para Franco (2005), isto acontece porque o direito penal máximo tem serventia apenas para enfraquecer os direitos e garantias fundamentais e para acabar com o conceito de direito penal mínimo, danos motivos para a incrível convivência, em meio ao Estado Democrático de Direito, de um direito penal autoritário.

Já para Wilson dos Santos da Silva (2014), o direito penal máximo no contexto brasileiro embora a base seja uma intervenção penal mínima, percebe-se que há um posicionamento direcionado ao endurecimento do sistema e à supressão de direitos e garantias fundamentais dos indivíduos considerados inimigos dos Estados.

Além de mencionar que o direito penal máximo, aparece no âmbito da globalização econômica e tende, ao controle dos deserdados, não-consumidores e marginalizados, alcançando conter o clima de insegurança gerado, pelos meios de comunicação que mostram diariamente aos cidadãos as barbáries que esses indivíduos são capazes de fazer. (SANTOS, 2014).

Para corroborar afirma segundo Alamiro Velludo Salvador Netto[3], citado por Lilian Matsuura (2019, n.p.), que em oito anos o número de presos dobrou. Os presídios brasileiros abrigavam cerca de 232 mil presos, em 2000. Em dezembro do ano passado, de acordo com os dados do Ministério da Justiça, o número pulou para 446 mil.

Contudo, vimos que no Brasil mesmo que a base seja a intervenção mínima, o que se verifica é o endurecimento penal, no qual os direitos e garantias estão sendo relativizados e fazendo assim a multiplicação de presos, a cada ano.

[3] Professor de Direito Penal na Faculdade de Direito da USP.

2. A MÁXIMA CRIMINALIZAÇÃO DAS CONDUTAS PRATICADAS PELA INTERNET

3.1 CRIMES CIBERNÉTICOS NO BRASIL: A CRIMINALIZAÇÃO E O CENÁRIO ATUAL

É certo que a partir da normatização da Lei n. 12. 737/12, muitos crimes foram tipificados, entretanto antes disso o direito penal conseguia punir estes crimes virtuais, com a aplicação do tipo penal que mais se assemelhava à conduta praticada.

Contudo, os crimes foram se inovando fazendo com que a norma geral não conseguisse mais prevenir os novos crimes. Surgindo então a Lei n. 12.737/12 a qual foi apelidada Lei “Carolina Dieckmann” pelo motivo que foram vazadas fotos íntimas da atriz, e disso fez com que a lei visasse estes tipos de conduta, sendo elas: invasão de computadores, roubo e/ou furto de senhas e de conteúdos de e-mails e a derrubada intencional de sites. (OLIVEIRA JÚNIOR, 2013).

Mesmo com essas tipificações menciona André Miceli (2018 n.p.). “de acordo com um relatório da Norton Cyber security, em 2017 o Brasil passou a ser o segundo país com maior número de casos de crimes cibernéticos afetando cerca de 62 milhões de pessoas”.

Menciona também André Miceli (2018), que atualmente 54% dos brasileiros têm em suas residências acesso à internet e a conexão via dispositivos móveis, além do que em 2017 o Brasil encerrou com mais de 236 milhões de celulares, uma média de 113, 52 celulares por 100 habitantes.

> “Esse aumento também impacta no crescimento de cibercrimes, já que muitos acreditam que estejam mais seguros utilizando aparelhos móveis. O paradoxo segurança x liberdade, que sempre existiu no meio físico, existe no digital também. Quanto mais livres estivermos, menos seguros estaremos.” (MICELI, 2018, n.p.).

Disto percebe que de acordo com que a sociedade vai se atualizando o crime também se modifica, é o caso da população que acreditava que com a utilização dos aparelhos móveis tornaria mais segura a interação virtual, entretanto os criminosos virtuais se aprimoram de acordo com que o mundo virtual se atualiza.

De logo, mesmo com a máxima criminalização das condutas de crimes informáticos só se aumentam fazendo assim saber que a maximização por alguns instantes foi de fato suficiente para acalmar a sociedade. Porém no cenário atual o direito penal máximo não está resolvendo este conflito aparente.

Fazendo concluir que em nosso panorama atual, mesmo com as severas punições, aumentos de penas o Estado não está conseguindo intervir, abrindo este grande questionamento? Para uma resposta definitiva a esta questão, seria por meio de mais criminalização ou a partir da Educação.

3.2. CRIMINALIZAÇÃO OU EDUCAÇÃO

A criminologia é um estudo científico que visa explicar e prevenir o crime, além de intervir na figura do delinquente e avaliar os diferentes modos de resposta à criminalização, “Para cuja aplicação são necessárias novas profissões: psicólogo, assistente social, criminólogo, educador” (ALBERGARIA, 1999, p.19).

Segundo menciona Viviane Avelino Marcelos (2019), na criminologia as apreciações de prevenção são variadas, porém nos deteremos na figura do papel da escola enquanto instituição de ensino. Na qual se entende por prevenção a maneira de evitar o crime agindo pelo pressuposto de que são vários os fatores de sua ocorrência.

Para Orlando Soares (1983, p. 125), “o objetivo de prevenir ou dispor de maneira que evite dano ou mal, preparando medidas ou providências de antecipação”. Esta ideia visa a antecipação das causas antes que haja a violência.

Ao ponto de vislumbrarmos com o que é prevenção, atentarmos agora com a repressão a qual é:

> “ideia de ação ou efeito de reprimir, coibir, proibir por meios policiais ou judiciais a prática de determinados atos, considerados ilícitos penais, através duma reação, exercida de fato em nome do Direito, considerada reação social contra... o crime" (SOARES, p. 138).

Haja vista a definição do que é prevenção e repressão, refletiremos sobre os controles sociais formais e informais.

Antônio Garcia - Pablos de Molina (2000), explica que controles sociais é o “conjunto de instituições, estratégias e sanções sociais que pretendem promover e garantir referido submetimento do indivíduo aos modelos e normas comunitárias”.

Neste sentido, são controles sociais formais: a polícia, a justiça, a administração penitenciária, etc. Por sua vez, controles sociais informais: seria a família, a escola, a profissão, a opinião pública etc.

De logo, como alude Viviane Avelino Marcelos (2019), a prevenção e a repressão são meios estratégicos ou respostas de órgãos que usam das normas para conter a violência.

> A repressão ao crime por parte da polícia é limitada, primeiro, pela falta de efetivo para conter a criminalidade. Segundo, pela falta de condições de trabalho: armas obsoletas, viaturas em pequena quantidade, falta de combustível, etc. E terceiro é a falta de estabelecimentos prisionais capazes de absorver a população delitiva. O aumento do aparato judicial significa mais presos e não necessariamente menos delitos. A solução da criminalidade não está no fortalecimento da polícia em todos os seus aspectos, mas sim, na forma eficaz de prevenção AVELINO (2019, n.p.).

Para corroborar com a ideia Antônio Garcia - Pablos de Molina (2000, p.120), nos diz “A eficaz prevenção do crime não depende tanto da maior efetividade do controle social formal, senão da melhor integração ou sincronização do controle social formal e informal”.

Como vimos todo o amparo de leis não erradicaram os crimes informáticos, só fizeram o aumento desses crimes no qual percebe que o meio para a eficaz prevenção, não depende só do Estado na figura de poder de punir, mas sim da integração e a sincronização deste com todo o aparato do controle social informal.

Contudo, visto que a criminalização não foi suficiente para minimizar os crimes cibernéticos, no entanto, é preciso que o Estado invista em educação, como forma de evitar a prática de condutas criminosas para que só assim seja possível a erradicação dos crimes informáticos.

CONSIDERAÇÕES FINAIS

Como foi mencionado, a internet foi criada nos Estados Unidos, em 1969 por nome de Arpanet (WERNER, 2001). Daí em diante a internet se alastrou, fazendo a conexão de muitos povos, ao exemplo da facilidade de comunicação destes indivíduos a qual que se torna indispensável na vida destas pessoas. Por outro lado, essa facilidade na comunicação abriu possibilidade para a criminalidade.

Destas proliferações de crimes virtuais que se acometeram, foram então criadas formas para se distinguir os autores e os tipos de delitos, assim, foram classificados em próprios os crimes praticados pelo uso do computador, e impróprios aqueles crimes em que se utiliza o computador e a rede só como um meio para satisfazer seus anseios. Já os autores dos crimes virtuais foram estipulados de sujeitos ativos, e sujeitos passivos, este sendo o titular do interesse na qual institui a ofensa, aquele sendo o que praticou a ofensa descrita na norma incriminadora.

A partir daí, foi elucidado que mesmo antes das legislações específicas já existiam meios para que fosse possível a punição dos crimes cibernéticos, na qual se usava a lei penal no que cabia, porém mesmo assim não se resolvia o problema de tantos outros crimes virtuais. Diante desse cenário, foram então criadas às leis específicas que visavam alcançar os crimes virtuais, todavia mesmo com os aumentos de penalizações os crimes só dobraram como mencionado pelo relatório da Norton cyber security, segundo André Miceli (2018), sendo o Brasil o segundo país com alto índice de criminalidade virtual.

Foi então que para tentar resolver este conflito aparente trouxemos a diferenciação do direito penal máximo e direito penal mínimo, este tendo como ideia a diminuição de penas e meios que propiciem outras alternativas, à punição. Disto mencionado que na nossa realidade, está claro o posicionamento do endurecimento penal, visto porque os direitos e garantias estão sendo relativizados e o direito penal usado sem observância do princípio do último *ratio*.

De fato, o endurecimento penal foi benéfico em uns anos, a qual visava reprimir todos os tipos de crimes, desde os pequenos delitos aos grandes, porém na nossa realidade brasileira, esta ideia está fracassada porque ao se colocar mais indivíduos neste sistema carcerário falido, só desenvolverá para que o crescimento desta população criminosa se aumente.

Pelo motivo em que um presidiário de pena branda ao conviver com indivíduos de alta periculosidade, com o tempo estará se aprimorando ao mundo do crime pela simples convivência. Além de mencionar que muitos desses presidiários se familiarizaram tanto com o ambiente carcerário que quando saem cometem crimes, só para retornarem.

De logo, foi usada a criminologia para resolver esta questão, no qual foi exposta a ideia de repressão e prevenção usada juntamente com os controles sociais, sendo eles controles sociais formais e informais.

Conclui-se que, a melhor solução para a erradicação da criminalidade virtual seria a junção dos controles sociais, visto que o Estado no seu poder de punir não está conseguindo sozinho resolver este conflito, logo percebe que esta sincronização é a mais certa possível, porque a junção do Estado na figura de seus elementos como a polícia, a justiça e os demais, junto com a educação, a sociedade, a família criará indivíduos de comportamentos éticos e morais, fazendo com que essa cultura de indivíduos sem responsabilidades éticas e morais se acabe.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBERGARIA, Jason. *Noções de criminologia*. BH, Editora Mandamentos, 1999.

AVELINO, Viviane Marcelos. Prevenção da Violência. Disponível em: https://meuartigo.brasilescola.uol.com.br/sociologia/prevencao-violencia-1.htm Acesso em: 04 de abril de 2019.

COSTA, Marco Aurélio Rodrigues da. Crimes de Informática. Jus Navigandi, Teresina, ano 1, n. 12, maio 1997. Disponível em: <http://jus2.uol.com.br/doutrina/texto>. Acesso em: 30 mar 2018.

CNJ. *Crimes Digitais: quais são, como denunciar e quais leis os definem.* (25 de junho de 2018). disponível em: http://www.cnj.jus.br/index.php?option=com_content&view=article&id=87058:crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime&catid=813:cnj&Itemid=4640&acm=288999_10899. Acesso em 15 de abril de 2019.

CALLEGARI, A. L.; DUTRA, F. A. Direito penal dos inimigos e direitos fundamentais. *Revista dos Tribunais*, São Paulo, n. 862, ago. 2007.

CERVINI, Raúl. Os processos de descriminalização. São Paulo: RT, 1995.

DIANA, Daniela, Artigo revisado em 05/09/2018. Toda Matéria: conteúdos escolares. Disponível em: < https://www.todamateria.com.br/historia-da-internet/ > Acessado em: 06 Nov. 2018.

FRANCO, A. S. *Crimes hediondos.* 5. ed. São Paulo: Revista dos Tribunais, 2005.

FRANCO, A. S. *Crimes hediondos*: anotação sistemática à Lei no 8.072/90. 4. ed. São Paulo: Revista dos Tribunais, 2000.

FREITAS, Alessandra Mara , SILVA, Cristian Kiefer. O problema da tipicação dos crimes informáticos: aspectos controversos a respeito da aplicação do artigo 154-A da lei nº 1.737/2012 “Lei Carolina Dieckmann”. Disponível em:<http://www.publicadireito.com.br/artigos/?cod=2a5b63fbaadcaa8c> acesso em 14 mar. 2019.

FREITAS, Carolina Paladino. Política Criminal: Direito Penal Mínimo X Direito Penal Máximo. Disponível em: https://www.jfrj.jus.br/revista-sjrj/artigo/politica-criminal-direito-penal-minimo-x-direito-penal-maximo-political-criminal

Acesso em 28 de mar. 2019.

GARCIA, Adeneele Carneiro. Crimes virtuais: Elementos para uma reflexão sobre o problema na tipificação. Disponível em: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529

; acesso em 14 mar. 2019.

GOUVÊA, Sandra. O Direito na era digital: Crimes praticados por meio da Informática. Rio de Janeiro: Mauad, 1997. 163 p.

GARCÍA-PABLOS DE MOLINA, Antonio. Criminologia. SP, Editora Revista dos Tribunais, 2000.

GARLAND, David. A cultura do Controle. Crime e ordem social na sociedade contemporânea. Rio de Janeiro: Revan, 2008.

JESUS, Damásio E. de. Direito penal: volume 1: parte geral. 28. ed. rev. São Paulo: Saraiva, 2005. 750 p.

LUISI, Luiz. Os princípios constitucionais penais. 2. Ed. Porto Alegre: Sergio Antonio Fabris, 2003.

MICELI, André. Publicado em 19/02/2018. Brasil é o segundo país com maior número de vítimas de cibercrimes. Disponível em: <http://www.revistacobertura.com.br/2018/02/19/brasil-e-segundo-pais-com-maior-numero-de-vitimas-de-crimes-ciberneticos/> Acessado em: 26 de abril de 2019.

MATSUURA, Lilian. Números de presos dobra em oito anos no Brasil. Disponível em: https://www.conjur.com.br/2009-ago-26/numero-presos-dobra-reintegracao-deixa-objetivo-estado. Acesso em: 26 de junho de 2019.

MIRABETE, J. F. **Processo Penal**. 18ª. ed. São Paulo: Atlas, 2006.

MATOS, Wilson da Silva. Direito penal máximo e o Sistema prisional. Disponível em: https://www.progresso.com.br/variedades/direito-penal-maximo-e-o-sistema-prisional/128980/ Acesso em: 26 de junho de 2019.

NETO, Mário Furlaneto. GUIMARÃES, José Augusto Chaves. Crimes na internet: elementos para uma reflexão sobre a ética informacional. Disponível em: <http://www2.cjf.jus.br/ojs2/index.php/cej/article/view/523/704> Acesso em: 22 mar. 2019.

NUNES, Raphael Vieira de Paiva Rosa, Crimes Virtuais. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/crimes_virtuais_0.pdf

Acesso em 28 de mar. 2019.

OLIVEIRA JÚNIOR, Eudes Quitino de. **A nova Lei Carolina Dieckmann**. Disponível em: <http://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann>. Acesso em: 03 de abril de 2019.

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

PAIVA, Mário Antônio Lobato de. Ciência do Direito Informático. Disponível em <http://www.advogado.adv.br/artigos/2002/mlobatopaiva/cienciainformatica.htm> Acesso em: 29 de maio de 2018.

PINHEIRO, Patricia Peck. Direito Digital. 4ed. Ver., atual. e ampl. São Paulo: Saraiva, 2011.

PLANALTO, Lei nº 12.737 de 30 de novembro de 2012. Dispõe sobre a Tipificação Criminal de Delitos informáticos e da outras providencias. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm Acesso em: 03 de abril de 2019.

QUEIROZ, André. A atual lacuna legislativa frente aos crimes virtuais. Revista jurídica Unifox. Foz do Iguaçu, v.3, n.1, p. 169-178, jul./dez. 2008.

QUEIROZ, Paulo de Souza. Do caráter subsidiário do Direito Penal: lineamentos para um Direito penal mínimo. 2. Ed. Belo Horizonte: Del Rey, 2002.

REALE, Miguel. Lições Preliminares de Direito. 27.ed São Paulo: Saraiva, 2006.

RIBEIRO, Fellype. Breve relato da História dos crimes cibernéticos. Disponível em: < https://idireitodigital.wordpress.com/2015/04/14/breve-relato-da-historia-dos-crimes-ciberneticos/> acesso em 14 mar. 2019.

ROSA, A. M. da; SILVEIRA FILHO, S. L. da. *Para um processo penal democrático*: crítica à metástase do sistema de controle penal. Rio de Janeiro: Lumen Juris, 2011.

RODRIGUES, José Adilson de Sousa. Hacker x Cracker. Disponível em: http://roitier.pro.br/wp-content/uploads/2016/11/jose adilson_3593_assignsubmission_file_Artigo-Hacker-X-Cracker.pdf Acesso em: 04 de abril de 2019.

ROSA, Fabrízio. Crimes de Informática. Campinas: Bookseller, 2002. 138 p.

SILVEIRA, A. B. D. Conteúdo Jurídico. **Os Crimes cibernéticos e a Lei n° 12.737/2012**, 22 janeiro 2015. Disponível em: <http://www.conteudojuridico.com.br/artigo,os-crimes-ciberneticos-e-a-lei-no-12737 2012,52253.html>. Acesso em: 17 maio 2018.

SCHMIDT, Guilherme. Crimes Cibernéticos. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos Acesso em 27 de mar. 2019.

SIMÕES, H. Brasil tem 116 milhões de pessoas conectadas à internet, diz IBGE. **g1.globo.com**, 2018.Disponível em:<https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml>. Acesso em: 30 março 2018.

SOARES, Orlando. Prevenção e repressão da criminalidade. RJ, Ed. Biblioteca Jurídica Freitas Bastos, 1983.

TRIGO, Louise da Silva. Algumas Reflexões Sobre o Direito Penal Máximo. Disponível em:

<http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=13103> Acesso em 02 de abril de 2019.

ULBRICH, Henrique Cesar. VALLE, James Della, Digerati, **Universidade Hacker.** 3. ed. São Paulo: 2004.

VIANNA, Túlio Lima. Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais. Belo Horizonte: Forense, 2003.

WERNER, L. Internet foi criada em 1969 com o nome de "Arpanet" nos EUA. **Folha de S. Paulo**, 12 Agosto 2001. Disponivel em: <http://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml>. Acesso em: 30 mar 2018.