FACULDADE EVANGÉLICA DE GOIANÉSIA

CURSO DE DIREITO

CRIMES CIBERNÉTICOS: A EVOLUÇÃO DA LEGISLAÇÃO.

WELTON ALVES VIEIRA

GOIANÉSIA

2020

WELTON ALVES VIEIRA

CRIMES CIBERNÉTICOS: A EVOLUÇÃO DA LEGISLAÇÃO.

Artigo Científico apresentado junto ao Curso de Direito da FACEG Faculdade Evangélica de Goianésia, como exigência parcial para a obtenção do grau de Bacharel em Direito. Orientador: Prof. Me. Kleber Torres de Moura.

GOIANÉSIA

2020

FOLHA DE APROVAÇÃO

CRIMES CIBERNÉTICOS; A EVOLUÇÃO DA LEGISLAÇÃO.

Goianésia, Goiás____ de _____de 2020.

Banca examinadora:

Nome do Arguidor: _____ Evangélica Goianésia, _____.

Nome do Arguidor: _____ Evangélica Goianésia, _____.

Nome do Arguidor: _____ Evangélica Goianésia, _____.

“O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fará coisas admiráveis.”

- José de Alencar.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela minha vida, por ter me dado saúde força e por me ajudar a ultrapassar todos os obstáculos encontrados ao longo do curso. Sem Ele nada seria possível.

A minha esposa Luiza Fernanda, que sempre esteve ao meu lado, por todo apoio e incentivo nas horas difíceis, a meu filho Wender Gabriel, pela paciência e compreensão em todos esses anos de faculdade.

Agradeço também a minha mãe Luzinete Alves, irmãos Edson, Janete e Janilson, padrasto e amigo Elias, sogro Adriano e minha sogra Maria Lúcia, e a todos meus familiares e amigos, que de uma forma contribuíram é incentivaram nos momentos difíceis e compreenderam a minha ausência enquanto eu me dedicava à realização deste trabalho.

Quero agradecer o meu orientador Me. Kleber Torres de Moura, pelo empenho aqui dedicado ao meu projeto de pesquisa. Sou grato a todos os professores, Colaboradores da Faculdade Evangélica de Goianésia, em especial as colaboradoras da Biblioteca Cleonice, Elizabete e Luiza por todos os conselhos e ajuda durante os meus estudos e elaboração do meu TCC, agradeço também aos meus amigos de sala e agora da vida que não deixaram de contribuir nessa caminhada. O meu muito obrigado.

CRIMES CIBERNÉTICOS: A EVOLUÇÃO DA LEGISLAÇÃO.

WELTON ALVES VIEIRA

Resumo: O presente trabalho tem a intenção de promover uma breve análise e reflexão sobre os crimes cometidos em redes sociais. O avanço da tecnologia, seus benefícios e principalmente aqui abordado os seus malefícios. Assim analisamos alguns tópicos contando o avanço desta conexão via internet, procedimentos usados para investigação de um ato cometido via rede sociais, crimes de informática, vírus, fraudes eletrônicas, pornografia, mídias, invasões de sistema de segurança, crimes homofóbicos, ausência de evidencias, ameaças causada pelas redes sociais, punição e aplicação de leis quando o crime assim for descoberto. Como fonte de Pesquisa foram utilizadas as seguintes obras: Damásio de Jesus, Emerson Wendet, Patrícia Peck, Spencer Toth Sydow, Túlio Vianna, e outros. Foi feita a lei 12.737/2012 conhecida como lei Carolina Dieckmann e a lei 12.695/2014 Lei do Marco Civil no sentido de punir esses infratores.

Palavras Chaves: Crimes, Redes sociais, Investigação, Internet, Brasil.

Abstract: The present work intends to promote a brief analysis and reflection on the crimes committed in social networks. The advancement of technology, its benefits and mainly its harms are addressed here. So we analyzed some topics counting the progress of this internet connection, procedures used to investigate an act committed via social networks, computer crimes, viruses, electronic fraud, pornography, media, security system invasions, homophobic crimes, absence of evidence, threats caused by social networks, punishment and enforcement when the crime is so discovered. The following works were used as a research source: Damásio de Jesus, Emerson Wendet, Patrícia Peck, Spencer Toth Sydow, Túlio Vianna, ande others. Law 12,737/2012, known as Carolina Dieckmann law, and law 12,695/2014 Marco Civil Law, in order to punish these offenders, were made.

Keywords: Crimes, Social Networks, Investigation, Internet, Brazil.

INTRODUÇÃO

Na década de 1980 os usuários começaram a se comunicar para troca de arquivos e envios de mensagens, usando o mesmo endereço de IP. A partir de 1988, ficou mais conhecida por ser usada para fins comerciais, surgiu daí a conexão via dial-up, ou a internet discada que é uma forma de acesso de rede pública de telefonia para estabelecer uma conexão com provedor através de um número de telefone com outra linha de telefone. A World Wide Webe (www), criado por Tim Berners-Lee cientista da computação foi possível ajudar a Organização Europeia

nas suas investigações nucleares, trabalhando assim várias pessoas em um mesmo documento.

Nos anos 90 criaram o Hyper Text Tranfer Protocol Secure (HTTPS) foi o que transformou a internet em um fenômeno mundial, onde muitos buscaram ter em casa seu computador, para fazerem buscas em sites (WENDET, 2013). O tema aqui exposto, Crimes cibernéticos; e a evolução da legislação, em uma justificativa sobre os crimes cometidos por redes sociais, fala-se desde a criação da internet no mundo até os efeitos cometidos por ela e aplicação das leis. Diante disto aqui expondo os problemas que as redes sociais vêm causando no decorrer dos anos e a investigação não muito aplausíveis nesse contexto, para a punição do infrator.

Deste modo a presente pesquisa tem por objetivo falar dos crimes cometidos pelas redes sociais, que na maioria das vezes trás a dificuldade da descoberta do ato cometido, tendo em vista sua instabilidade, ou seja, a sua perca de provas que podem ser apagadas, alteradas, excluídas, perdida ou até mesmo editadas.

Portanto, o artigo tem como objetivo tratar dos crimes que podem ser cometidos e suas dificuldades para aplicar a lei nesses atos cometidos pelo ciberespaço do crime digital. Assim, o artigo foi dividido em quatro tópicos; no primeiro falamos sobre a internet no mundo, quando se popularizou, a sua evolução, os sites e suas ameaças. O segundo relata sobre as possíveis ameaças, os crimes cibernéticos, e os vírus, palitando a impossibilidade de evitar esses ataques. Já o terceiro aprofunda nos crimes cibernéticos no Brasil, quais os procedimentos para investigação, falsidade e fraude, pornografia infantil, e pedofilia virtual que cresce a cada dia mais, não podem deixar de falar das mídias e redes sociais que são usados a fim de disseminar conteúdos, opiniões, ideias, todos os tipos de forma colaborativa ou não. E por último o quarto item, dos desafios da legislação, investigação e combate aos crimes cibernéticos no Brasil, a aplicação destas leis, o que está sendo feito e o que precisa ser melhorado.

Será feita uma breve análise das principais leis referentes aos crimes cibernéticos que são a lei 12.737/2012 e lei 12.965/2014, conhecidas como Lei Carolina Dieckmann e Lei do Marco Civil, onde a intenção para criação destas leis

foram as punições para quem comete o crime virtual, as lacunas existentes e as tipificações.

A metodologia aqui utilizada foram pesquisas bibliográficas em livros, artigos científicos, monografias e sites. O trabalho em questão tem uma importância muito grande em relação a nossa sociedade atual, uma vez que a internet tem feito cada vez mais parte do nosso dia- dia.

1. A INTERNET NO MUNDO.

Segundo Guizzo (1999), entre os anos de 1995 a 2000 a internet veio a se popularizar, ficando assim mais fácil o acesso aos usuários. A tecnologia foi evoluindo de uma forma que a internet discada foi dando espaço para internet banda larga junto com a conexão 3G, que é bem mais rápido. Vieram também os sites que compartilha músicas e arquivos e as primeiras redes sociais que no ano 1995 recebeu o nome de O site classmates.com, que foi muito utilizado no Canadá e Estados Unidos. Na época era usado entre amigos de colégios de faculdades. O surgimento da internet foi parecido com do computador. No ano de 1963 nos Estados Unidos o matemático Joseph Licklider desenvolveu a internet, de uma forma bem diferente daqui temos hoje, sendo mais simples e com estrutura diferente, onde seu propósito era obter uma ferramenta de comunicação com capacidade de cruzar vários caminhos para que a mensagem chegasse ao seu destino final (GUIZZO, 1999).

Seu intuito era que mesmo se de alguma forma o caminho a ser percorrido pela internet estivesse bloqueada, ela teria a capacidade de encontrar outro trajeto a fazer para concluir o envio, Rosa (2002, p. 29) esclarece:

> O departamento de Defesa dos EUA apoiou uma pesquisa sobre comunicações e redes que poderiam sobreviver a uma destruição parcial, em caso de guerra nuclear. A intenção era difundi-la de tal forma que, se os EUA viessem a sofrer bombardeios, tal rede permaneceria ativa, pois não existiria um sistema central e as informações poderiam trafegar por caminhos alternativos até chegar ao seu destinatário. Assim, em 1962, a ARPA encarregou a Rand Corporation (um conselho formado em 1948) de tal mister, que foi apresentar seu primeiro plano em 1967. Em 1969, a rede de

> comunicações militares foi batizada de ARPANET (rede da agência de projetos avançados de pesquisa).

Rosa (2002) continha a dizer que no ano de 1966, para desenvolver a Advance Research Projects Administration – Administração de Projetos e Pesquisas Avançados (ARPANET) 1972, Ray Tomlinson inventa o correio eletrônico, até hoje a aplicação mais utilizada na NET. Em 1973, a Inglaterra e a Noruega Foram ligadas à rede, tornando-se, com isso, um fenômeno mundial. Foi quando no mesmo ano veio a público a especificação do protocolo para a transferência de arquivos, o FTP, outra aplicação fundamental na Internet. Portanto, nesse ano, quem estivesse ligado à ARPANET já podia se logar como terminal em um servidor remoto, copiar arquivos e trocar mensagens. Devido ao rápido crescimento da ARPANET, Vinton Cerf e Bob Kahn propuseram o Transmisson Control Protocolo/Internet Protocol (TCP/IP), um novo sistema que utilizava uma arquitetura de comunicação em camadas com protocolos distintos, cuidando de tarefas distintas. Ao TCP cabia quebra mensagens em pacotes de um lado e recompô-las de outro, garantindo a entrega segura das mensagens. Ao IP cabia descobrir o caminho adequado entre o remetente e o destinatário e enviar os pacotes.

A internet precisava ser mais inteligente, para oferecer o máximo conforto e segurança aos usuários no dia-a-dia. Com o passar dos anos vieram outros tipos de redes sociais, que são o que usamos hoje como Face book, Twitter, Linkedin, Instagram e outros. A internet também é uma ótima ferramenta hoje muito necessária para comunicação, pesquisa, apoio escolar, sendo também uma porta ao conhecimento (ROSA, 2002, p.30).

Benakouche (1997) afirma que a internet é maior rede mundial de comunicação existente na atualidade. As redes de computadores permitem que seus usuários se comuniquem através de um baixo custo que tenham acesso a fontes inesgotáveis de informação, reduzindo relativamente à distância entre as pessoas, através de um clique interagindo assim com pessoas de todo o planeta. Tal utilização possibilitou até mesmo a inserção de outros tipos de cultura através da rede mundial de computadores. Dessa maneira, os meios que possibilitam o acesso à internet estão crescendo gradativamente, sendo que, antes a única forma de acesso era através de computadores simples e atualmente o acesso também pode

ser feito através de tablets, celulares, relógios, dentre outros equipamentos disponíveis (AGUIAR, 2001).

De acordo com Comer (2016, p. 3) as redes de comunicações têm crescido explosivamente:

> A partir dos anos 1970, a comunicação via computador transformou-se em uma parte essencial de nossa infraestrutura. A ligação de computadores em rede é usada em cada aspecto dos negócios, incluído propaganda, produção, transporte, planejamento, faturamento e contabilidade. Consequentemente, a maioria das corporações tem múltiplas redes. As instituições de ensino em todos os níveis, do ensino fundamental à pós-graduação, estão utilizando redes de computadores para fornecer a estudantes e professores o acesso instantâneo a informações em bibliotecas on-line em todo mundo.

Sabemos que nas nossas redes dos computadores, há diversas circulações de informações de informáticas como; textos, figuras, vídeos, imagens, sons, mas a mais evoluída na atualidade é WhatsApp, que pode ser usado em nossos telefones móveis (celulares).

1.1. A INTERNET NO BRASIL

No Brasil o Instituto Brasileiro de Geografia e Estatística (IBGE) passa a se utilizar deste recurso a parti de 1964, neste mesmo ano foi criado Centro Eletrônico de Processamentos de dados do Estado do Paraná, proporcionando muitos avanços para o país. Nos anos seguintes foram criados o Serviço Federal de Processamento de Dados, a Empresa Brasileira de Telecomunicações, que era um órgão vinculado ao Ministério das Comunicações, ambos criados nos meados de 1965. O Brasil se associa ao Consórcio Internacional de Telecomunicações por Satélite (INTELSAT).

A Universidade Federal de São Paulo (USP), consegue em 1972 fabricar o primeiro computador no Brasil e em 1974 é inaugurada a fábrica da Computadores Brasileiros S.A (COBRA), cinco anos mais tarde cria-se a Secretaria Especial de Informática. A Fundação de Amparo a Pesquisa do Estado de São Paulo (FAPESP) e o Laboratório Nacional de Computação Científica (LNCC), juntos com a Universidade Federal do Rio de Janeiro, consolidam a partir de 1988, a internet no Brasil. ((WENDET e JORGE, 2013).

Em 1995, Rodrigo Baggio lançou o Comitê para Democratização da Informática (CDI), no Rio de Janeiro. Com o apoio inicial do IBASE e depois de várias organizações comunitárias, filantrópicas e do setor privado, o CDI desenvolveu a Escola de Informática e Cidadania (EIC), que se tornou cada vez mais orientada para a Internet. Cobrando uma pequena taxa simbólica para os seus alunos, ela se espalhou rapidamente e em 2004 atingiu o número de 830 EICs em 20 estados brasileiros e dez outros países. (KNIGHT, 2014).

Ainda hoje existem escolas de informática para capacitação de pessoas não só para os estudos, mas para o mercado de trabalho que tem uma cobrança muito grande que seu contratado tenha. Fazendo assim que os cursos de informática ainda seja uns dos mais procurados dos últimos tempos.

Conforme Dertouzos (1997), desde início discussões podiam ser percebidas sobre a necessidade de criar mecanismos de controle para a internet. A autonomia e liberdade pareciam perigosas a setores do governo e parcelas conservadoras da sociedade. E talvez possamos dizer que isso não mudou; discussões como está ainda acontecem em várias partes do mundo, incluindo o Brasil, onde já tivemos alguns casos em que o Poder Judiciário decidiu retirar sites como Youtube, a pedido de cidadãos que se sentiram ofendidos com vídeos postados. Dertouzos (1997) ainda acreditava ser difícil criar mecanismos realmente eficientes de controles dados as características da Internet. É neste ponto que as características da ferramenta Internet parecem estabelecer relação com o tipo de cultura e de dinâmica de produção estabelecida na *Web.* (DERTOUZOS, 1997).

Com grande aspecto que a Internet serve para vários fins, levando para lados positivos e negativos, obtivemos também as grandes ameaças levadas as mentes criminosas, que não perdem oportunidade do uso para praticar seus atos, que na maioria das vezes são terríveis. Tendo em vista que muitos culpados não são encontrados, devido a falta de obrigação dos servidores de gravar os dados de seus usuários.

1.2. AS PRIMEIRAS AMEAÇAS

A internet é um dos meios propício para as mentes criminosas, com essa facilidade de acessos de hoje em dia, essa troca de informações os criminosos

podem ter acesso a todos os dados sejam eles bancários, fotos das redes sociais, e ainda usam esse ciberespaço para a realização de fraudes, ofensas à pessoa, exploração sexuais e várias outras condutas. Esses crimes podem ser conhecidos como crimes de informática, crime cibernético, e-crime, cibe crime, crime eletrônico ou crime digital, que são usados para toda prática criminosa que se utiliza o computador, celulares e outros meios de acessos.

Para Peck (2002), o crime virtual é, em princípio, um crime de meio, ou seja, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, aquele cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, mas que algum modo pode ser enquadrado na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa é que é virtual, não o crime (PECK, 2002).

Já para Castro (2003), os crimes cibernéticos são cometidos através de computadores, celulares e diversos outros meios informáticos. A maioria dos crimes é praticada através de rede de internet e os meios usualmente utilizados são os computadores. Castro também afirma que os crimes cibernéticos existem desde os anos 70:

> Os primeiros crimes de informática iniciaram-se na década de 70, sendo executados em sua grande maioria por pessoas especializadas no ramo informático com o objetivo principal de adentrar ao sistema de segurança das grandes empresas, tendo como maior foco as denominadas como instituições financeiras o perfil atual dos criminosos que atua nessa área foi alterado, já que nos dias atuais qualquer pessoa que tenha um conhecimento, porém não tão aprofundado basta ter acesso à rede mundial de computadores para que consiga lograr êxito na execução de um crime virtual (CASTRO, 2003, p.9).

Peck (2002) ressalta que, com a chegada da Internet Móvel, a individualização do usuário cresce, fazendo com que o celular se torne um prolongamento de sua existência no mundo digital, a partir do qual ele pode realizar uma série de negócios eletronicamente. O roubo e furto de celulares torna-se comum – não apenas motivado pelos recursos conseguidos com a venda do aparelho no mercado paralelo e pelo uso da linha para ligações ilegais – torna-se quase um sequestro, onde a identidade da pessoa proprietária do aparelho é

assumida pelo praticante do roubo por um determinado período de tempo. De acordo com o autor com o roubo o criminoso pode ter acesso a todos os dados do celular, facilitando assim acesso a contas pelos aplicativos do seu celular, podendo transferir dinheiros para suas contas, podem também ter acessos a suas fotos e demais documentos arquivados no mesmo (PECK, 2002).

Além disso, cabe evidenciar que assim que for roubado o Celular, é necessário que tenha informações sobre o mesmo, como IMEI, que é o número que identifica o aparelho. Assim o proprietário do celular poderá bloquear, para impedir que o criminoso tenha acesso a todos os dados nele armazenados. Faça também um boletim de ocorrência assim ficará mais fácil provar que não estava com o aparelho quando o mesmo for usado para práticas ilícitas.

Assim segundo Viana (2013), os crimes cibernéticos podem ser cometidos por qualquer indivíduo que tenha os meios necessários para fazê-lo. Uma vez que apenas um envio de imagem pode ser caracterizado como crime, sendo que não há necessidade que o agente domine a área da informática ou tecnologia, precisando apenas do conteúdo do telefone celular ou computador da vítima, por exemplo. Através disso, os crimes cibernéticos foram se tornando mais frequentes, isto porque os dispositivos eletrônicos estão a cada dia mais presentes no cotidiano da grande maioria da população onde em alguns casos uma pessoa possui mais de um dispositivo em casa, aumentando assim as possibilidades de o agente cometer o crime, (VIANA; MACHADO, 2013. p.40-47).

Diante disso qualquer pessoa com a intenção de cometer o crime, mesmo não sendo especialista, com apenas um envio de imagem a pessoa estará cometendo o crime, seja ela adulta ou não. Pois tem pessoas que possuem não só apenas uns dispositivos mais vários em sua casa, podendo facilitar sua atuação no momento do ato criminoso. A segunda sessão irá aborda a luz do código penal brasileiro, a relação dos crimes cibernéticos mais comuns, e a forma de combatê-los.

2. REDE MUNDIAL DE COMPUTADORES E POSSÍVEIS AMEAÇAS.

Quando se diz em ameaças causadas pelo meio de rede de computadores, fazemos uma referência à internet. Sabemos que não é possível usa-la em total segurança. Confiar algo pessoal em um serviço desconhecido como imagens, aberturas de contas bancárias, redes sociais, é algo que na maioria das vezes nos decepciona, trazendo consequências desagradáveis.

De acordo com Jesus (2016 *apud* GONZAGA, 2013, p.28) A sociabilidade do brasileiro pode ser identificada como favorecedora dos crimes digitais, sobretudo numa era envolvendo *apps* falsos, que muitas vezes não são checados por seus usuários antes de serem instalados. E o risco aumenta, pois cibercriminosos passam a focar na Internet das Coisas, como TVs, geladeiras e carros conectados. Cinquenta e sete por cento dos usuários de *smartphone* brasileiros foram vítimas de crime virtual móvel. (JESUS, 2016. p. 28).

Já para Sydow (2015) também é uma prática bastante comum nas redes informáticas a indução de vítimas futuras e eventuais a instalarem arquivos que geram falhas de segurança ou criam verdadeiras portas de acesso livre nos dispositivos alheios. Uma vez instalados tais códigos maliciosos, o delinquente pode ingressar no sistema. (SYDOW, 2015. p. 115).

Isso é um ato ardil cometido por um hacker, o usuário não percebe este ato criminoso, essa invasão de privacidade, assim não se pode chamar de ato violento mais sim de uma cilada que a vítima caiu, pois a mesma não percebe que seu aparelho sofreu esta violação de dados pessoais. Assim o criminoso pode ter acesso a contas, senhas, e-mails, contatos, fotos e muito mais...

Ainda de acordo com Sydow (2015) o ingresso desautorizado, assim, viola a confidencialidade do acesso particular e, consequentemente, a segurança telemática, dando incertezas ao usuário violado e levando-o à perda de confiança num instrumento imprescindível para o desenvolver da sociedade. De certo modo, a Lei n. 12.737/2012 trouxe este delito ao ordenamento jurídico brasileiro, ainda que de modo inaplicável. (SYDOW,2015. p. 117).

2.1. CRIMES CIBERNÉTICOS

Crimes cibernéticos ou crimes informáticos como é mais conhecido, já sabemos que são crimes usados por ferramentas que tem o acesso a internet. Com a dificuldade de investigação do crime praticado, tem elevado os números de Autores desses atos, que também na maioria das vezes que são descobertos o crime já foi prescrito, ou seja, o Estado perde o direito de punir o acusado.

Conforme Wendt e Jorge (2013), diz que os crimes cibernéticos se dividem em crimes cibernéticos abertos e crimes exclusivamente cibernéticos. Com relação aos crimes cibernéticos abertos, são aqueles podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele. Já os crimes exclusivamente cibernéticos são diferentes, pois eles somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet.

Peck, (2002) diz que muitas pessoas que não cometem crimes no mundo real por medo de serem pegas acabam, de algum modo, interessando-se pela prática delituosa virtual. É o caso, por exemplo, do grande número de adolescentes de classe média, com grande conhecimento de informática, que praticam atos ilegais na rede e sentem-se bastante seguros em fazê-lo. Esse tipo de crime tem um traço cultural que se aproxima do vandalismo. (PECK, 2002. p. 129).

Existem diversos tipos de vírus, sendo os principais explicados abaixo. (CASSANTI, 2014).

Vírus de arquivo: são anexados ao código de um programa, normalmente utilizam-se de arquivos executáveis como .EXE, .MSI, e seu efeito inicia quando os arquivos são executados. (CASSANTI, 2014).

Vírus de boot: são considerados os precursores de todos os demais vírus, eles se fixam na partição de inicialização de sistemas, impedindo-o de iniciar. Eles se espalham através de disquetes, CDs, DVDs e pen drives, e sua infecção ocorre quando estão conectados ao computador durante a sua inicialização. (WENDT; JORGE, 2013).

Vírus time bomb.: caracteriza-se por sua ativação ser feita em determinada data e horário estipulado pelo programador que o desenvolveu. Dessa forma, a vítima não percebe nada na hora que o executou, dificultando a descoberta de sua real origem. Também é conhecido como bomba-relógio ou gatilho. (WENDT; JORGE, 2013).

Vírus de macro: são programas escritos na linguagem de macro de um aplicativo como por exemplo o Word e Excel da Microsoft. Para se tornarem ativos, eles precisam que a macro seja executada, alterando os componentes do programa e causando operações inesperadas ou se recusando a executá-las. Após a infecção, os demais arquivos abertos através desse programa também são afetados. (CASSANTI, 2014)

Worm; também conhecido como verme, caracteriza-se por residir na memória ativa do computador e se replicar automaticamente, não sendo necessária nenhuma ação do usuário. Ele se instala geralmente em computadores e programas que possuem 28 vulnerabilidades, sendo a principal delas a de estar desatualizado. Os Worms consomem muitos recursos do computador, degradando a sua utilização e podendo também lotar o seu disco rígido, devido à quantidade de cópias geradas de si mesmo. (WENDT; JORGE, 2013).

Cavalo de troia ou trojan; O cavalo de troia é um arquivo aparentemente inocente entregue através de algo conhecido como por exemplo um cartão digital, um álbum de fotos, protetor de tela ou jogos. O elemento principal é executado normalmente enquanto o elemento malicioso trabalha de forma oculta ao usuário. (CASSANTI, 2014).

Após infectado, o invasor pode se tornar administrador da máquina e assim alterar outras configurações de segurança, deixando o computador ainda mais vulnerável. Também é possível que ele capture informações do usuário e as envie por e-mail para o criminoso. (JESUS, 2016).

Botnets; são redes de computadores compostas por diversos bots, que são sistemas instalados por criminosos em estações servidores que respondem a comandos e funções enviados a ele. Os computadores se tornam “zumbis” e, devido 29 à grande quantidade de computadores invadidos, a descoberta da origem se torna difícil. (JESUS, 2016)

Diante disso sabemos que é impossível evitar esses ataques de vírus que são criados através dos equipados que tem acesso a internet, resta colocar mecanismos de cautela para garantir uma utilização boa e sem imprevistos. Para isso, a melhor forma é ter ciência sobre as soluções que estão sendo utilizados, como eles laboram e de que forma é admissível serem violados. Além disso, é admissível dizer com o uso de instrumentos que analisam e auxiliam em casos de risco, resguardando seus dados e equipamentos.

3. CRIMES CIBERNÉTICOS NO BRASIL

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 e causando um prejuízo de US$ 22 bilhões. No ano anterior, o Brasil era o quarto colocado na lista, mas agora fica atrás apenas da China, que em 2017 teve um prejuízo de US$ 66,3 bilhões. Um dos principais fatores deste aumento de crimes está na popularidade de smartphones, que agora chegam a 236 milhões de aparelhos no Brasil, ou 113,52 para cada 100 habitantes. Esse aumento também impacta no crescimento de cibercrimes, já que muitos acreditam que estejam mais seguros utilizando aparelhos móveis, explica o professor e coordenador do MBA em Marketing Digital da Fundação Getúlio Vargas em todo o Brasil, Andre Miceli. "O paradoxo segurança x liberdade, que sempre existiu no meio físico, existe no digital também. Quanto mais livres estivermos, menos seguros estaremos.'' (UOL, 2018).

Portanto o Brasil teve um prejuízo enorme por causa do aumento dos Smartphones, onde veio acompanhando também o crescimento de cibercrimes. Pode-se considerar que com a evolução da tecnologia nos últimos anos, com a facilidade do acesso a internet, corremos riscos diários. Riscos esse que na maioria das vezes não são descobertos.

Segundo Barreto (2017), constatando uma grave deficiência legislativa no Brasil, onde muitas dessas condutas ainda não são tipificadas pela legislação e encontram nela muitas brechas, sucede-se uma grande sensação de impunidade no meio virtual. Ao mesmo tempo, o Legislativo não acompanha as evoluções cibernéticas, ocasionando um ordenamento jurídico cada vez mais ultrapassado e inócuo. (BARRETO, 2017). Portanto fica inerente que na maioria das vezes não recebem a punição para o ato cometido.

Assim Jesus (2016) fala que enquanto no Brasil pouco se faz em estrutura investigativa, nos Estados Unidos o FBI convoca especialistas de segurança para o que anuncia ser uma “Guerra cibernética”, eis que o crime informático estaria se tornando uma ameaça maior que o próprio terrorismo. Crime informático não é só questão de segurança pública, mas de defesa nacional.

3.1. PROCEDIMENTOS ESPECIALIZADOS PARA INVESTIGAÇÃO

De acordo Soares (2013), as estatísticas criminais brasileiras indicam que o foco da repressão policial se concentra principalmente nas prisões em flagrante, as quais são mais fáceis de investigar. Porém, grande parte dos delitos não são sequer denunciados, por vários motivos como a opressão sócio - cultural ou os interesses particulares existentes no protecionismo político de esquemas criminosos sofisticados. Visto que esses crimes estão longe de serem desconhecimento público, é notório que a população e o Estado não possuem estatísticas que se aproximem à realidade fática criminosa. Uma vez que não são conhecidos, impossível criar mecanismos que solucionem esses problemas.

Outra grande dificuldade de se obter provas no mundo virtual é a instabilidade, ou seja, ela pode ser facilmente apagada, alterada, editada, excluída ou perdida. Isso se diferencia enormemente das investigações policiais em crimes do mundo real, uma vez que no mundo físico é muito mais difícil de exterminar por completo evidências das ações humanas. Já no mundo virtual, com essa possibilidade, o acesso aos vestígios criminosos são impalpáveis e demandam mais esforço da análise criminal. Além disso, devido a globalização, se torna muito mais simples a prática dos crimes virtuais uma vez que se pode acessar a internet de qualquer lugar do mundo, o que torna o ato criminoso muito mais fácil e rápido do que a identificação dele. Sobre isso, Corrêa (2008, p.74), discorre:

> O grande problema relacionado aos “crimes” digitais é a quase ausência de evidências que provem contra o autor, a inexistência da arma no local do crime. Uma gloriosa invasão a sistema alheio não deixaria nenhum vestígio, arquivos seriam alterados e copiados, e nenhum dano seria prontamente identificado. Um crime perfeito, sem traços, e, portanto, sem evidências. Justamente por essa qualidade da perfeição há a dificuldade em presumir o provável número desses “crimes”.

A quantidade de policiais capacitados e treinados na investigação de crimes virtuais ainda é escassa, e isso passa a tornar-se problemático, ao passo que dificulta a persecução penal dos responsáveis e, inevitavelmente, resulta na impunidade (WENDT e JORGE, 2013). Não se pode dizer que é fácil obter algum resultado na investigação desses crimes virtuais, vários meios tem que ser

identificados e também qual os tipos de ferramentas que o criminoso usou. Vendo por outro ângulo que no mundo real já é totalmente diferente, uma vez que praticado o crime fica difícil acabar por completo com todas as evidências.

O primeiro passo na investigação dos crimes cibernéticos é identificar a origem da comunicação. Por análise de dados, se chegará ao endereço IP de linhagem e ao usuário que está ligado a esse IP. Segundo Peck (2016), no direito digital, a identificação de um computador é feita por meio do endereço IP- *internet protocol* (Protocolo de Internet). O número IP é atribuído cada usuário ou internauta, toda vez que uma conexão for estabelecida com a rede mundial de computadores. Além de permitir a identificação virtual, o IP descreve todo o tráfego de rede e acessos feito pelo usuário em determinado período.

Assim uma vez identificado o endereço IP, serão analisadas possíveis provas da prática do delito. Essa análise, feita por peritos especializados, é uma atividade extremamente complexa, considerando a presença de programas de computador cujo o objetivo é o mascaramento da verdadeira identidade do autor, principalmente quando os computadores estão localizados em locais e redes públicas. (PECK, 2016).

Uma vez que na prática criminal virtual exigem mais esforços para essa análise, vendo que o criminoso pode acessar internet de qualquer lugar do mundo. Sobre isso Corrêa (2010), O grande problema relacionado aos “crimes” digitais é a quase ausência de evidências que provem contra o autor, a inexistência da arma no local do crime. Uma gloriosa invasão a sistema alheio não deixaria nenhum vestígio, arquivos seriam alterados e copiados, e nenhum dano seria prontamente identificado. Um crime perfeito, sem traços e, portanto, sem evidências. Justamente por essa qualidade da perfeição há a dificuldade em presumir o provável número desses crimes.

O meio virtual nos traz a refletir sobre os crimes que são cometidos por meio dele. O ciberespaço como também pode ser chamado abriu muitas oportunidades para a prática criminosa, sendo cada vez mais comum se ouvir falar nessas práticas, com o fato de as pessoas pensarem que esse ambiente é uma terra sem leis. Quando falamos nesses crimes, não temos a proporção de quantos são, vamos aqui falar de alguns que por sua vez são os mais cometidos:

De acordo com Jesus (2016) falsidade e fraude é a introdução, alteração, eliminação ou supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que sejam considerados ou utilizados legalmente como se fossem autênticos. no Brasil, não temos um tipo específico para tutelar esta conduta em casos de bancos de dados privados (podendo se cogitar do delito de falsidade ideológica – art. 299 do código Penal).

> **Art. 299** - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:
> Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, de quinhentos mil réis a cinco contos de réis, se o documento é particular. (Vide Lei nº 7.209, de 1984)

Já sobre Pornografia Infantil De Inellas (2004), fala que a pornografia infantil é caracterizada por fotografar ou publicar cenas de sexo explícito ou pornográfico que contenham crianças e adolescentes de acordo com o art. 241 do Estatuto da Criança e do Adolesceste.

> **Art. 241**-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008).

Portanto na pornografia infantil não necessita que exista um relacionamento para cometer o crime, bastando apenas divulgação e a venda de material erótico que envolva crianças e adolescentes. A lei 8.069/90, O Estatuto da Criança e do Adolescente, de acordo com o artigo 241.

> **Art. 241.** Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008).

Assim vender ou expor fotos, vídeos, cenas de sexo ou pornografia que tenha criança ou adolescente, o autor poderá ter uma pena de reclusão, de 4 a 8

anos, e multa. O mais correto a se fazer ao receber fotos, vídeos pornográficos, é apagar, fazer uma denúncia, seja ela anônima ou até um boletim de ocorrência, não continuar passando para frente esse tipo de vídeo e imagem, pois assim você estará contribuindo com o crime, podendo também responder por ele.

É necessário ter a clareza que a pedofilia foi impulsionada pelo meio virtual, principalmente da maneira e facilidade com que crianças e adolescente se deixam encontrar nas redes sociais, grande parte delas tem em suas residências pelo menos um computador com webcam, internet e outros dispositivos à sua disposição por 24 horas e por vezes, os utilizam sem limites ou sem orientações causando uma grande vulnerabilidade, tornando a ação dos criminosos fácil e rápida, na qual utilizam de artimanhas para chamar a atenção das vítimas, criando perfis falsos nas redes sociais e adotando uma linguagem de fácil compreensão (SERRA, 2009). Portanto assim as crianças e o adolescente ficam vulneráveis com os perfis falso dos criminosos que criam algo atraente para poder cometer o crime.

A pedofilia virtual cresce cada vez mais e mais rápido por todo o mundo. Estar em pleno século XXI e não colocar a pedofilia virtual como centro na pauta de debates gera preocupação. O ciberespaço já não pode mais ser visto apenas como um mundo imaginário e irreal e sim como um canal de fácil acesso para esses criminosos (SERRA, 2009).

No entendimento de Colares (2002), pode-se observar que:

> Constituem crimes eletrônicos a exposição em sites de Internet de fotos pornográficas com crianças ou adolescentes – enquadrando-se no art. 241 do Estatuto da Criança e do Adolescente – pedofilia; bem como o plágio de textos de terceiros e sua publicação em um site, caso em que há violação ao direito de autor – art. 184 do Código Penal (COLARES, 2002).

Para alguns autores a Pedofilia é considerada por uma pessoa que sente atração sexual por crianças, conhecido como pedófilo que tem fantasias, desejos. Estudos apontam que pedofilia é uma doença e não crime, conforme Silva (2009):

> Se alguém tem relações com uma menor de 14 anos, presume-se estupro. Pedofilia é outra coisa, e nosso direito não contempla essa figura. O mundo acadêmico fica dormitando sobre a situação, e políticas públicas de combate a "pedofilia" não são levadas à efeito. A precariedade da saúde e a precariedade do sistema penal se

> entrelaçam com a falta de vontade do Estado de encarar a situação, resultando daí o agravamento da mesma. (SILVA, 2009).

Silva (2009) ainda fala que cumpre lembrar que a Classificação Interna de Doenças (CID 10) da Organização Mundial da Saúde (OMS), item F65.4, define a pedofilia como "Preferência sexual por crianças, quer se trate de meninos, meninas ou de crianças de um ou do outro sexo, geralmente pré-púberes". (SILVA, 2009).

3.2. Mídias e Redes sociais

Para falarmos de mídias e redes sociais, e importante dar as diferenças entre os conceitos mídias sociais e redes sociais que são empregados aqui, vamos tomar as definições a seguir entre mídia social e rede social. Mídias sociais, segundo Aimola (2010), são tecnologia é prática online que são usadas por pessoas e empresas a fim de disseminar conteúdo, compartilhando opiniões, ideias, experiência e perspectivas, ou seja, é o conjunto de todos os tipos e formas de mídias colaborativas. Nessa classificação contém muitos dos sites de armazenamento multimídia, como Youtube, Flickr, Wikipedia, Twitter, os blogs, os sites colaborativos, como o Delicious e o Digg, e os sites de relacionamento, como Orkut, Facebook e MySpace. Nesse sentido, nem todos envolvem o conceito de rede social.

Já a definição de redes sociais que vamos usar é a de que são os sites empregados cujo material principal é a troca de informações e experiências. De acordo com Recuero (2009, p.29):

> “Rede social é gente, interação, é troca social. É um grupo de pessoas, compreendido através de uma metáfora de estrutura, a estrutura da rede social”.

Existem regras fundamentais para o compartilhamento de informações nas redes sociais que, se não forem cumpridas, podem gerar transtornos muitas vezes irreversíveis. Segundo Cherry (2014, p.93), essas seriam algumas recomendações básicas sobre o que não deveria ser compartilhado na Internet:

> Nenhuma informação pessoal.
> Nada que você não gostaria que seus avós vissem.
> Nada que você não gostaria que seus pais vissem.
> Nada que você não gostaria que seus filhos vissem.
> Nada que você não gostaria que seu chefe visse.

> Nada que você não gostaria que sua seguradora visse.
> Nada que você não gostaria que o governo visse.

Já esclarecido algumas recomendações, é importante que ao usar as redes sociais tenham em si o cuidado de não cometer transtornos com compartilhamentos desnecessários, pensar e agir de forma que não venha a prejudicar ou ofender a honra de alguém, uma vez que feito pode ser considerado um crime ou uma ofensa muito grave em um âmbito familiar, empregatício, ou até mundial.

4. OS DESAFIOS DA LEGISLAÇÃO, INVESTIGAÇÃO E COMBATE AOS CRIMES CIBERNÉTICOS NO BRASIL.

Uma das Leis que ficou mais conhecida foi “Lei Carolina Dieckmann” Lei n.12.737/2012 sancionada pelo Governo de Dilma Rousseff, que promoveu alterações no Código Penal Brasileiro. Segundo Jesus, (2016) o tipo mais polêmico trazido com a Lei n. 12.737/2012, invasão de dispositivo informático, representa um crime de perigo abstrato, onde não se espera a ocorrência de resultado, forma legislativa que cresce diante do avanço da tecnologia e o temor do risco do seu uso indevido. (JESUS, 2016).

Segundo Jesus (2016) esta lei foi apelidada de “Lei Carolina Dieckmann”, a Lei n. 12.737/2012, que tipifica os crimes cibernéticos, adveio do Projeto de Lei n. 2.793/20115, sendo agilizado no início de 2013 pelo “casuísmo em que fotos íntimas da atriz teriam sido supostamente copiadas de seu computador e divulgadas na internet”. Na verdade, a legislação veio atender a uma demanda antiga do setor financeiro, duramente impactado com os golpes e fraudes eletrônicas, ainda que considerada uma lei absolutamente “circunscrita”, em comparação aos projetos sobre crimes cibernéticos que tramitavam no congresso nacional. (JESUS, 2016).

De acordo com o art. 154- A do código Penal, invadir um dispositivo é:

> 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.

O artigo 154-A do CP diz que o Individuo ao invadir qualquer dispositivo de outra pessoa, para fins de adulterar, destruir informações sem a permissão da mesma, violando a intimidade da pessoa, pode pegar de três meses a um ano de cadeia ou multa pelo ato cometido.

Já a parte B do artigo 154 diz que os crimes definidos no art. 154-A, apenas procedem através de 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.

A legislação brasileira tem uma segunda lei específica sobre os crimes cibernéticos. Essa lei foi criada no ano de 2014, com o Nº 12.965 foi dada o nome de Lei do Marco Civil. O Marco Civil veio para a proteção dos usuários da Internet, assim passou a ser chamada como a Constituição da Internet. Foi considerado um avanço na legislação brasileira quando se trata de crimes praticados pela internet.

Segundo o Art. 1º da Lei nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, determinando suas diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. (Brasil, 2014). A sua regulamentação veio através de um decreto de nº 8.771/2016, assinado também pela presidente Dilma Rousseff, em 11 de maio de 2016.

Segundo Otoboni (2019) Este decreto prescreveu que tivesse procedimentos para armazenar e proteger os dados dos usuários da rede, elencando também que as garantias da transparência quando houvesse requisição por parte da Administração Pública para conferir dados cadastrais dos respectivos usuários fossem assegurados de forma segura. (OTOBONI, 2019).

Os princípios estão especificados nos incisos do Art. 3º quando se trata da Lei Marco Civil da Internet que são:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I – Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II – Proteção da privacidade;
> III – proteção dos dados pessoais, na forma da lei;

> IV – Preservação e garantia da neutralidade de rede;
> V – Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI – Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII – preservação da natureza participativa da rede;
> VIII – liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Apesar dos desafios para legislação, para se adaptarem e aprofundar seus conhecimentos no extenso mundo da informática, na adequação de suas leis, buscaram assim uma possível forma de caracterizar e punir os crimes cibernéticos.

Seu principal princípio é o que está previsto no inciso IV, Art. 3º e depois pautado no Art. 9º que é o da neutralidade da rede. De acordo com Marcacini (2016, p. 41):

> Trata-se de questão fundamental, em primeiro lugar, pois diz respeito diretamente à preservação das liberdades que a Internet tem proporcionado aos seus usuários, desde sua criação; a disposição também é importante sob os ângulos da defesa da concorrência, do estímulo à inovação e da priorização de critérios meritocráticos na oferta online de produtos e serviços. Suas polêmicas derivam do forte jogo de interesses sobre a questão objeto dessa norma, ou de argumentos evidentemente equivocados sobre qual é, tecnicamente falando, o significado da neutralidade definida no texto legal.

Portanto, averiguar que o principal objetivo do princípio da neutralidade do Marco Civil da Internet é abonar a isonomia dos dados preparados para os usuários, permitindo a mesma rapidez do tráfego na rede, procurando o livre acesso de conteúdo colocado nos mesmos dispositivos, com a mesma intensidade da informação para ambas as pessoas que acessem o que foi compartilhado e publicado na internet. Além disso cabe evidenciar que a lei nº 12.965/14 tem como objetivo regulamentar o uso da internet, a sua interação e comunicação, podendo assim estimular a criação de novas tecnologias e proteger seus usuários e provedores.

Nesse sentido, ainda tem que ser feita várias mudanças legislativas a lei do Marco Civil da Internet uma vez que haja proteção aos termos de responsabilidade civil e criminal.

Falando sobre Pacote Anticrime apresentado pelo Ministro Sérgio Moro, aprovado no dia 04/12/2020 pela Câmara e seguindo agora para o Senado, D' Urso (2019) fala que neste projeto existe a previsão de alteração de questões com relação aos crimes contra honra praticados nas redes sociais (internet). Nós temos no Código Penal a previsão dos crimes contra a honra, que são calúnia, difamação e injúria. A calúnia ocorre quando alguém imputa um crime a terceiro, mas na verdade este crime inexiste. A pena hoje é de 6 meses a 2 anos de detenção. Já a difamação ocorre quando alguém ofende a reputação de terceiro, isso quer dizer, imputa-lhe fato ofensivo, e este ataque chega ao conhecimento de terceiros. A pena nestes casos é de 3 meses a 1 ano de detenção. No caso da injúria, não há imputação de um fato, mas sim um ataque direcionado à vítima, que tem sua dignidade ofendida. A pena é de 1 a 6 meses de detenção.

D'Urso (2019) ainda fala que atualmente, quando estes crimes são praticados pela internet, se aplica um aumento de pena de 1/3, que está previsto no Código Penal, em seu artigo 141, inciso III. Isto ocorre, pois o Código Penal, mesmo sendo de 1940, trouxe um aumento de pena para quando estes crimes contra a honra fossem praticados "por meio que facilite a divulgação", ou seja, como por exemplo pela internet.

Sobre o projeto anticrime, a alteração proposta, é a inclusão de um novo parágrafo no artigo 141, com a seguinte redação: "se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores (internet), aplica-se a pena no triplo". (D'URSO,2019).

Assim a pena para o projeto anticrime, assim que aprovada, será triplicada, quando ocorrer injúria, difamação e calúnia pelas redes sociais, trazendo um caráter mais punitivo e severo para os praticantes destes crimes virtuais.

CONCLUSÃO

Tendo em vista os aspectos aqui observados, o objetivo desse estudo foi demonstrar que com o avanço da tecnologia, com as inovações dos aparelhos eletrônicos ficou mais difícil manter a privacidade dos usuários resguardada, uma vez que esses dispositivos facilitam a divulgação de conteúdos de caráter privado.

Além do que o avanço da tecnologia e sua facilidade de acesso as redes sociais, trouxe junto a prática de crimes. O primeiro crime foi na década de 70, executado por pessoas especializadas em informática com o objetivo de invadir o sistema de segurança de grandes empresas da época.

Assim, desde muito tempo há discussões sobre o que podia ser feito para controle do uso da internet. No Brasil houve casos em que o Poder Judiciário chegou a retirar sites, a pedido de usuários que se sentiram ofendidos com vídeos postados.

Portanto, com o tempo foram criadas leis como 12.737/12 e 12.965/14 para fins de diminuir os delitos no âmbito virtual, buscando um meio de punir os crimes cibernéticos. Feita uma breve análise das leis, certifica-se que deve ser criadas novas leis mais justas para a punição desses infratores. Ainda há uma grave deficiência legislativa no Brasil, onde tem uma sensação de impunidade, quando se trata de crimes virtuais.

Constata-se também, que mesmo coma melhor das leis no decorrer dos anos, o correto e de grande importância é o usuário se resguardar, tendo todo cuidado com o acesso desses dispositivos, sempre que possível ser instalados nos mesmos programas para a sua proteção. Ainda vale ressaltar, o perigo que ocorre quando acessa dispositivo públicos, uma vez que pode ficar salvo dados pessoais nessas máquinas.

Por fim, são necessários muitos ajustes para a punição desses infratores, aplicando punições severas para que não haja prática desses delitos ou evitando à prática do mesmo.

REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR, Sonia; Dantas, Vera. **Memórias do computador:** 25 anos de informática no Brasil. 2001.

AIMOLA, Veridiana N. **Empresas que criam as próprias redes de relacionamento**. In :LAS CASAS, Alexandre L. (Org.) Marketing Interativo: A utilização de Ferramentas Digitais. São Paulo: Saint Paul Editora, 2010.

BARRETO, Erick Teixeira. **Crimes Cibernéticos sob a égide da Lei 12.737/2012.** Disponível em: <https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/>. Acesso em 18 Abr. 2020.

BRASIL. **Art. 241 do Estatuto da Criança e do Adolescente - Lei 8069/90.** Disponível em: <https://www.jusbrasil.com.br/topicos/10582366/artigo-241-da-lei-n-8069-de-13-de-julho-de-1990>. Acesso em 27 Mar. 2020.

BRASIL. **Código Penal Brasileiro**, 07 de dezembro de 1940.

BRASIL. **Lei 12.965 de 2014**. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> . Acesso em 29 Abr. 2020.

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

CASSANTI, Moisés de Oliveira**. Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014. Disponível em: . Acesso em: 22 de mar.2020.

COLARES, Rodrigo Guimarães. **Cybercrimes: os crimes na era da informática**. disponível em: <https://jus.com.br/artigos/3271/cybercrimes-os-crimes-na-era-da-informatica> acesso em 28 de Abr. 2020.

COMER, Douglas. E.. **Redes de computadores e internet [recurso eletrônico].** 6. Ed, Porto Alegre: Bookman, 2016.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 4 ed. São Paulo, Saraiva, 2008.

CHERRY, Denny. Tradução de Christiane Leonor Simyss Moreira. **Fundamentos da privacidade digital:** Ferramentas para proteger suas informações pessoais e sua identidade na internet. 1 ed. Rio de Janeiro: Elsevier, 2014. Disponível em: < https://play.google.com/books/reader?id=hFkaBQAAQBAJ&printsec=frontcover&output=reader&hl=pt_BR&pg=GBS.PP1>. Acesso em 01 de Abr. 2020.

DE INELLAS, Gabriel Cesar Zaccaria**. Crimes na Internet.** São Paulo: Juarez de Oliveira, 2004, p. 27.

DERTOUZOS, M. **O que será: como o novo mundo da informação transformará nossas vidas**. São Paulo: Companhia das letras, 1997.

D'URSO, Luiz Augusto Filizzola. Projeto Anticrime aprovado na Câmara altera pena para ofensas nas redes sociais. Entenda o que mudou. 2019. Disponível em: <https://www.migalhas.com.br/depeso/316629/projeto-anticrime-aprovado-na-camara-altera-pena-para-ofensas-nas-redes-sociais-entenda-o-que-mudou>. Acesso em 27 de Abril. 2020.

GUIZZO, Erico. **Internet:** O que é, e o que oferece, como conectar-se. Ática, 1999.

JESUS, Damásio de**. Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

KNIGHT, Peter, T. **A internet no Brasil: origem, estratégia, desenvolvimento e governança.** 2014. Disponível em: < https://books.google.com.br/books?hl=pt-

BR&lr=&id=1xOcAwAAQBAJ&oi=fnd&pg=PP1&dq=INTERNET+NO+BRASIL&ots=v-JU0UX2kM&sig=mpV4HZe2fF0VVNWIzl68JTmw_W0#v=onepage&q=INTERNET%20NO%20BRASIL&f=false>. Acesso em: 01 Mar. 2020.

MARCACINI, Augusto**. Aspectos Fundamentais do Marco Civil da Internet: Lei 12.965/2014.** São Paulo: Edição do autor, 2016.

OTOBONI, Gustavo Henrique dos Santos. **Crimes Cibernéticos: Phishing.** 2019. Disponível em: < https://ambitojuridico.com.br/edicoes/revista-191/crimes-ciberneticos-phishing/> Acesso em: 28 Abr.2020.

PECK, Patrícia**. Direito digital**. São Paulo: Saraiva, 2002.

PINHEIRO, Patrícia Peck, **Direito digital**. 6.ed., atual. e ampl. São Paulo: Saraiva, 2016.

RECUERO, Raquel. **Redes Sociais na Internet.** Porto Alegre: Editora Sulina, 2009.

ROSA, Fabrízio. **Crimes de Informática.** 2002.

SERRA, T. M. G. (2009). **A pedofilia na internet à luz do estatuto da criança e do adolescente.**
Monografia (Graduação em direito) – FESP Faculdades, João Pessoa.

SILVA, Francisco Deliane e. **Pedofilia, crime ou doença? O direito da loucura ou a loucura do direito.** 2009. Disponível em:< https://jus.com.br/artigos/13877/pedofilia-crime-ou-doenca>. Acesso em: 22 de Abr. 2020.

SOARES, Luís Eduardo. **PEC - 51: revolução na arquitetura institucional da segurança pública**. In:Boletim do IBCCrim, ano 21, no 252, novembro de 2013. São Paulo.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. 2.ed. São Paulo: Saraiva,2015. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502229495/cfi/4!/4/4@0.00:61.9>. Acesso em 26 Mai. 2020.

UOL. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**, São Paulo, 15.fev.2018. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm>. Acesso em 24 Mai. 2020.

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

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