CENTRO UNIVERSITÁRIO SÃO JOSÉ
CURSO DE DIREITO

Igor Caetano Fuly

A aplicabilidade da nossa legislação nos crimes cibernéticos

Rio de Janeiro

2020

IGOR CAETANO FULY

A APLICABILIDADE DA NOSSA LEGISLAÇÃO NOS CRIMES CIBERNÉTICOS

Projeto de pesquisa apresentado para a Disciplina de TCC II, Plano de Negócio sob a orientação do prof (a) Daniela Vidal.

Rio de Janeiro

2020

RESUMO

O presente artigo visa abordar o nosso ordenamento jurídico nos crimes cibernéticos praticados no Brasil, com o intuito de identificar e criar soluções que possam amenizar esses delitos. É notório que a falta de uma legislação específica causa sérios problemas à sociedade, os crimes cibernéticos vêm crescendo a cada dia no mundo, inclusive no Brasil, afetando diversas esferas que incluem o campo político, econômico e social o que torna preocupante a segurança da ordem e do respeito às regras, interferindo assim, no exercício pleno da cidadania. Nesse sentido, abordaremos o conceito de Cibercrimes, como também, a maneira como esses delitos vêm sendo praticados, suas características e os principais órgãos que atuam no combate aos mesmos.

Palavras-chaves: Direito Penal, Crimes Cibernéticos, Tecnologia, Ambiente Virtual, Cibercrime, Internet, Legislação.

SUMÁRIO

INTRODUÇÃO

É indiscutível que o mundo globalizado propiciou o acesso a informação e interação entre as pessoas de uma forma extremamente rápida e fácil. Nos dias atuais, o acesso a internet alcança uma grande maioria de pessoas que, conectados ao mundo, deixam informações que acabam sendo utilizadas por indivíduos que tem por objetivo cometer diversos crimes cibernéticos.

Nesse sentido, a legislação precisa se adequar a essas novas práticas de crimes e estabelecer regras que prevêem todas as condutas, e desta forma, combater de modo eficiente os criminosos que atuam nessa área.

Sendo assim, esse trabalho tem como proposta o estudo dos principais crimes cibernéticos praticados no Brasil tendo a finalidade de analisar a atuação dos órgãos especializados no combate aos crimes virtuais, como também, a forma como nossa legislação está empenhada em punir crimes cibernéticos, explicando o seu conceito, suas características, o avanço tecnológico.

A seguir será informado como é o posicionamento do Brasil no sentido das medidas que estão sendo tomadas para evitar esses crimes, como também, serão mostrados quais os órgãos especializados no combate aos mesmos e de que forma eles atuam.

Em seguida serão desenvolvidos alguns argumentos sobre a falta de uma legislação especifica ao combate aos crimes cibernéticos, analisando algumas penas do nosso ordenamento jurídico.

É imprescindível mencionar que a metodologia usada consiste em pesquisas bibliográficas, leis e artigos publicados na internet que nos darão suporte para o embasamento das questões supracitadas.

1. HISTÓRIA E DESENVOLVIMENTO DO COMPUTADOR

1.1 ORIGEM

A etimologia da palavra computador vem de “computar” que significa calcular, essa criação vem desde a idade antiga. Uma das primeiras invenções foi o “ábaco”, instrumento criado pelos chineses no século V aC., funcionava como uma espécie de calculadora. No decorrer dos tempos, houve grandes matemáticos que contribuíram para o surgimento do computador.

O matemático francês Joseph Marie Jacquarde foi o responsável pela primeira máquina mecânica programável, entre outros temos, o matemático George Boole criador da álgebra booleana, como também, o matemático Charles Babbage a máquina analítica, que chega ser comparada com o conceito de computador que nós temos hoje com memória e programas. Sendo assim, chegou a ser considerado por alguns estudiosos como o pai da informática.

O alemão Konrad Suze e o americano Jhon Alanasoff, foram os responsáveis pela criação dos primeiros computadores digitais. Nesse sentido, o físico Jhon Mauchly, no ano 1946 criou o ENIAC (Eletronic Numerical and Calculator), o primeiro computador a realizar múltiplas funções, sua construção foi financiada pelos Estados Unidos.

No ano de 1968, Douglas Engelbert inventou o mouse e o teclado, o que tornaria o computador que nós conhecemos, sendo um marco histórico para evolução tecnológica, no entanto, somente nos fins dos anos de 70 e inicio dos 80, através de Steve Jobs e Steve Wozniak que desenvolveram a série de computadores Apple, ocorreu a primeira grande comercialização de sucesso desta máquina.

A Xerox corporation em 1981, desenvolveu o primeiro sistema operacional baseados em janelas, com auxilio das tecnologias de interface. Em 1982,a Intel criou o primeiro microprocessador.

A década de 90 foi marcada pela expansão dos computadores pessoais e os softwares integrados. E a partir de 2000 começou a surgir os computadores de mão, como tablet, ipad, ipod, Smarphones, que tornou a conexão móvel com a navegação a internet.

1.2 SURGIMENTO DA INTERNET

A criação da internet surgiu no contexto histórico da Guerra Fria tendo como finalidade a utilização da mesma no âmbito militar que buscava avanços tecnológicos para os meios de comunicação.

Um ponto relevante nesta época foi a criação da ARPANET (Advanced Research Projects Administration – Administração de Projetos e Pesquisas Avançados, rede de comunicação militar, criada em 1969, cuja finalidade era compartilhar informações, pesquisas e estratégias militares. No ano de 1972, a internet foi apresentada à sociedade.

Em 1985, foi criada a Worl Web (WWW) criada por Tim Bernes Lee, a internet passou a ser mundial. A partir desse momento surgiu a globalização que interligava os países diminuindo as fronteiras geográficas. Na década de 90 a internet passou a ser popular no Brasil.

Vale ressaltar que a expansão das conexões via internet ocorreu e ocorre devido aos grandes avanços tecnológicos que a cada dia chegam de forma mais acessível a toda população mundial.

2.0 O QUE SIGNIFICA CIBERCRIME

O Cibercrime constitui-se como atuações criminosas que surgiram através de práticas delituosas no meio informático. O exemplo disso tem ameaças, violações de

marcas, manipulações de caixas bancárias, pirataria de programas de computador, bullying, pornografia infantil, fake news, entre outros.

Observa-se que crimes como esses afetam o cotidiano da sociedade de um modo geral, levando as pessoas a ficarem vulneráveis a partir do momento que têm suas informações divulgadas e alteradas, pois esses crimes podem surgir a partir de qualquer dispositivo que o aparelho esteja conectado a internet.

De acordo com WENDT

> "Pode-se reconhecer que a evolução da tecnologia ocasionou um upgrade e/ou impulsionou alguns tipos de crimes antes restritos tão somente ao "mundo real". (Wendt, Emerson. Crimes Cibernéticos 2. Ed. BRASPORT:2002.)

Delitos computacionais, crimes de computador, crimes eletrônicos, crimes de informática, crimes virtuais, crimes cibernéticos, entre outros, são algumas das denominações para o cibercrime.

A doutrina classifica os crimes cibernéticos como puros, simples, mistos, comuns, próprios e impróprios. Nesse sentido, observaremos as diferenças de cada modalidade, no que se refere aos crimes cibernéticos puros o agente tem por objetivo atingir o computador através do sistema de informática ou dados e as informações utilizadas, no qual aparecem as atuações dos hackers que utilizam seu grande conhecimento informático com a finalidade de invadir ou prejudicar o sistema ou servidores.

Os crimes cibernéticos mistos o sistema de informática não é o foco, mas se torna essencial para a condução da prática do delito.

Os crimes cibernéticos comuns são aqueles em que a internet é utilizada como meio para a realização de um crime já tipificado em lei. (Pinheiro, 2002, p 85-87)

> “Aquele em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofende o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não computacionais ou diversos da informática.”

No caso dos crimes virtuais próprios são utilizados o sistema tecnológico como objeto e meio da execução do crime, tendo por objetivo corromper dados da vitima, seja para modificar,alterar, inserir dados falsos, só podendo ser concretizado por meio de computador.

Os crimes virtuais impróprios são aqueles realizados com a utilização do computador onde é utilizado como instrumento para realização de condutas ilícitas, o objetivo é atingir um bem jurídico comum, como exemplo o patrimônio do individuo através de um sistema informático para sua execução. (VIANNA, MACHADO, 2013p. 30,32)

É preocupante a evolução dessa prática de crime no mundo todo, e principalmente no Brasil, onde cada vez mais cresce o índice dessas condutas que prejudicam diretamente vidas e também a própria economia do nosso país.

Nas palavras de Damásio Evangelista de Jesus (aput CARNEIRO, 2012[N.P].

> “Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da maquina e periféricos) é o objetivo jurídico tutelado.”

> “Crimes eletrônicos impuros ou impróprios são aquele em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofende o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não computacionais ou diversos da informática.”

3.PRINCIPAIS DELITOS PRATICADOS NO BRASIL

3.1 WHATSAPP

Whatsapp é um aplicativo multiplataforma de mensagens instantâneas e chamadas de voz para smartphone. Além de mensagens de texto, os usuários podem enviar imagens, vídeos e documentos em PDF, além de fazer ligações grátis por meio de uma conexão com a internet.

O whatsapp tem falhas de segurança graves, e com isso diariamente vários delitos são praticados no ambiente virtual. O Brasil em 2017 passou a ser o segundo país com maior número de casos cibernéticos, causando prejuízos de bilhões de dólares. Um dos motivos desse avanço é a popularidade dos smartphones, com isso houve o aumento significativo de crimes e golpes que tornou a principal ferramenta para hackers no Brasil.

Os cibercriminosos estão investindo na disseminação de links maliciosos, de acordo com a empresa de segurança digital PSafe e seu laboratório de segurança,o DFNDR Lab são mais de 44 milhões de casos. O watsapp também pode ser um meio utilizado para organização de crimes.

A Constituição Federal de 1988 trata a honra como direito fundamental: Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à

liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 1988).

Assim, além da natureza jurídica de direito fundamental, a honra também constitui um dos direitos da personalidade, isto é, “aqueles que têm por objeto os atributos físicos, psíquicos e morais da pessoa em si e em suas projeções sociais” (GAGLIANO; PAMPLONA FILHO, 2012, p. 160).

Os crimes de calúnia, difamação e injúria, estão previstos respectivamente nos artigos 138, 139 e 140 do Código Penal Brasileiro.

Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.

Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa.

Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou decoro: Pena - detenção, de um a seis meses, ou multa. (BRASIL, 1940)

3.2 INVASAO DE PRIVACIDADE

A violação da privacidade que por si só já é violação de um direito fundamental e caracteriza crime. Invadir dispositivo informático alheio conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com fins de obter, adulterar ou destruir dados de informações sem autorização expressa ou tácita do titular é considerado crime de invasão de privacidade e poderá perante a justiça ser condenado à multa e ou prisão.

Com o surgimento do caso de grande repercussão, não só nacional, mas sim no mundo inteiro, que foi o caso da atriz Carolina Dieckmann, no ano de 2012, situação na qual teve fotos íntimas vazadas houve a necessidade de criar uma lei para combater tal crime. Dessa forma, o congresso nacional se mobilizou e então foi promulgada a Lei 12.737/2012, que surgiu a partir do projeto de lei nº 2793/2011, que foi aprovada após esse caso. Entrando em vigor no dia 02 de abril de 2013 e passou a ser chamada Lei "Carolina Dieckmann", que torna crime a invasão de aparelhos eletrônicos para obtenção de dados particulares. Essa lei alterou o Código Penal Brasileiro, acrescentando os artigos 154-A e 154-B que estão dentre os crimes contra a liberdade individual.

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:(incluído pela Lei nº 12.737, de 2012) Vigência Pena – detenção, de 3(três) meses a 1 (um) ano, e multa, (incluído pela Lei nº 12.737, de 2012) Vigência

§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. (Incluído pela Lei nº 12.737, de 2012) Vigência

§2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. (Incluído pela Lei nº 12.737, de 2012) Vigência

§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: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa,se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012) Vigência.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiros, a qualquer título, dos dados ou informações obtidas. (Incluído pela Lei nº12. 737, de 2012) Vigência.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) Vigência.

I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência.

II – Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência.

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembléia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012) Vigência.

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº12. 737, de 2012) Vigência.

Art.154-B. Nos crimes definidos no art.154-A, somente se procede mediante representação, salvo se o crime e 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. (Incluído pela Lei nº 12.737, de 2012) Vigência.

Essa lei veio resguardar a liberdade individual, o sigilo, a intimidade e a vida privada.

3.3 CYBERBULLYING

Todo comportamento agressivo, repetitivo praticado por uma única pessoa ou um grupo de pessoas contra outra(s) sendo por agressões físicas e psicológica a quem sofre o ato é conceituada de bullying.

O cyberbullying é a pratica dessas agressões por meio da internet, o que diferencia é que o agressor pode ser uma pessoa anônima, podendo ser até mesmo de outro país.

Para SHARIFF (2010.p.62) o cyberbullying se conceitua:

> “Pela sua natureza, os meios eletrônicos permitem que as formas tradicionais do bullying assumam características que são especificas do ciberespaço.”

> “O nosso código penal vem sendo utilizado no combate ao cyberbullying, pela tipificação dos crimes contra a honra nos artigos 138 e 145, que podem ser aplicados a qualquer crime praticados no meio eletrônico, seja Twiter, Facebook, Instagram, Youtube, E-mails ou qualquer outra rede social que seja utilizada para hostilizar alguém na internet.”

Os crimes de calúnia, difamação e injúria, estão previstos respectivamente nos artigos 138, 139 e 140 do Código Penal Brasileiro.

Contudo, para que haja configuração do crime contra a honra por meio das redes sociais, é preciso que estejam presentes todas elementares do tipo penal, bem como o elemento subjetivo do delito. No caso da calúnia, é necessária a imputação da prática de determinado fato, e que este seja qualificado como crime, sendo consumada quando a referida atribuição se torna conhecida por terceiro (BITENCOURT, 2011, p. 320-321).

Esses ataques por motivos fúteis têm por finalidade causar graves sofrimentos às vítimas, sendo que poucos que sofrem esse tipo de crime, tem coragem de denunciar, pois a grande maioria tem medo e a dificuldade para localização desses infratores acaba não conseguindo localizar o agressor.

Mesmo tendo dificuldades de encontrar esses criminosos o nosso poder judiciário, na esfera civil já existe condenações baseadas em atos de bullying e cyberbullying, incluindo até atos praticados por menores, nesses casos o entendimento é que o dano moral é incontestável.

3.4 FRAUDES ELETRÔNICAS

As fraudes eletrônicas atualmente representam ameaça as grandes empresas e as pessoas físicas.

A fraude eletrônica consiste na ação de enganar a vítima, por intermédio de dispositivos de informática para obter vantagens ilícitas e por conseqüência transtorno patrimoniais para a vitima enriquecimento ilícito do fraudador. No nosso código penal, as fraudes eletrônicas mais comuns é o estelionato (art.171), o furto qualificado mediante fraude e concurso de agentes (art.155 §4º, II) e a extorsão (art.158). Os fraudadores digitais em boa parte utilizam de uma técnica conhecida como engenharia social, onde os criminosos vinculam a uma instituição respeitável para conseguir os dados para fazer as fraudes.

Atualmente as mensagens falsas com liks fraudulentos (pishing) estão sendo utilizadas pelos criminosos onde tem criados sites falsos de lojas e tentam atrair as vitimas com ofertas e descontos extraordinários.

3.5 PEDOFILIA E PORNOGRAFIA INFANTIL

A pedofilia e a Pornografia infantil é um crime que causa danos psicológicos e físicos a vida das crianças, traumatizando e comprometendo quem sofrem esse tipo de abuso. Os criminosos que cometem esse tipo de delito podem criar perfis, fakes,enviar mensagens,marcar encontros,enviar vídeos íntimos,aliciar crianças e adolescentes para realizarem atividades sexuais ou explorem a sua nudez.

A pornografia também pode consistir em produzir, publicar, vender e adquirir pornografia infantil na internet. Constitui pornografia infantil a representação de uma criança ou adolescente envolvido em atos sexuais, podendo ser real ou simulado e a exposição dos órgãos sexuais para fins sexuais já configura crime.

O artigo 240 e 241 do Estatuto da criança e do adolescente, lei 8079/90 prevê:

Art.240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar por qualquer meio, cena de sexo explicita ou pornográfico, envolvendo criança ou adolescente (Redação dada pela Lei nº 11.829, de 2008).

Pena – reclusão de 4 (quatro) a 8 (oito) anos e multa

Art. 241. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explicito ou pornográfica envolvendo criança ou adolescente: (incluído pela Lei nº 11.829, de 2008).

Pena – reclusão de 4 (quatro) a 8(oito) anos,e multa

É preciso mencionar que quem acessar frequentemente imagens em sites de pedofilia estará sujeito a investigação criminal. O fato de armazenar imagens já constitui o crime conforme citado no **art.214-B**

Seguindo nesse estudo, tem-se o art. 241-A da ECA, que tratou do crime de divulgação de pornografia infantil:

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:

Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

Ainda, o artigo 241 – B do mesmo dispositivo legal tipifica o ato de posse de pornografia infantil, ou seja, ter em poder, de qualquer forma, foto, vídeo ou em qualquer meio de registro, pornografia infantil, ou seja, aquele que guarda em seu computador ou aparelho celular fotos íntimas de menores de idade, cuja pena é de 1 a

4 anos de reclusão e multa. De certa forma a referida inclusão serviu ao propósito de responsabilizar penalmente o indivíduo que armazena conteúdo erótico envolvendo crianças e adolescentes (NOGUEIRA, 2009, p. 84 apud COUTINHO, 2011, p. 17).

O artigo 241- C trata dos crimes de produção de pornografia infantil simulada/montagem; e por fim o artigo 241-D elenco os crimes de aliciamento de criança.

Cumpre ainda, fazer uma distinção entre a Pedofilia e a Pornografia Infantil, na primeira, há uma perversão sexual, a qual o adulto experimenta sentimentos eróticos com crianças e adolescentes, já na Pornografia Infantil não é necessário à ocorrência da relação sexual entre adultos e crianças, mas sim, a comercialização de fotografias eróticas ou pornográficas envolvendo crianças e adolescentes (INELLAS, 2004. P.46).

Assim, a internet tem sido o meio de comunicação preferido dos criminosos para a prática desse tipo de crime, tendo em vista a facilidade na transmissão de imagens e vídeos, bem com a sensação de anonimato que o meio digital proporciona, tendo em vista que existe maior dificuldade para sua identificação e posterior punição. Nesse sentido, destacam Christiane H. Kalb outros motivos para o aumento da pornografia infantil na internet:

> "Alguns dos motivos para que o abuso sexual e a publicação de fotos e vídeos pornográficos aumentassem significativamente foram a "confidencialidade de usuários de salas de bate-papo; hospedagem de *sites* nos mais variados países, dificultando a identificação e a prisão dos responsáveis; pouca legislação específica para crimes de informática, etc." (KALB, 2008, p. 121 apud COUTINHO, 2011, p. 15).

Dessa forma, a internet modificou o mercado da pornografia infantil, permitindo facilmente a sua distribuição, expandindo seu público alvo. As facilidades proporcionadas pela internet contribuíram de forma significativa para formas acessíveis

á conteúdo pornográfico envolvendo crianças e adolescentes. Sendo possível obtê-los sem sair de casa, acessando apenas um site, ou recebendo por e-mail, ou ainda por meio de compartilhamento de arquivos, e até mesmo com envio de mensagens instantâneas (MITANI, 2012, p. 121).

Conseguinte, existe a grande dificuldade para que se chegar ao individuo que praticou as referidas condutas, sendo necessária na maioria das vezes à quebra de sigilo, para conseguir rastrear e localizar o culpado. Muitas vezes ainda é preciso que as provas eletrônicas passem por uma perícia tecnicamente rigorosa, para que sejam aceitas em processo.

Denota-se que se trata de uma realidade preocupante e assustadora, a disseminação de vídeos e imagens pornográficas que envolvem crianças e adolescentes pela internet é uma triste realidade, onde grande quantidade de material é distribuída diariamente na rede.

Assim, devido à internet ser um meio vulnerável para a prática de crimes, e pela facilidade em manter o anonimato, a pornografia infantil tem crescido significativamente, tendo em vista que sua prática nesse meio garante a dificuldade em se chegar à identidade de quem pratica esses crimes, e que esses indivíduos venham a ser penalizados.

3.6 FAKE NEWS

No contexto atual, a fake news atua como umas das formas mais eficazes para disseminar e manipular notícias falsas que se espalham rapidamente causando danos gravíssimos no campo político, econômico e social. Nesse sentido, o objetivo é legitimar um ponto de vista ou prejudicar uma pessoa ou grupo, geralmente figuras públicas.

Apesar do recente uso do termo Fake News, esse conceito vem de séculos passados e não há uma data oficial de origem. A palavra "fake" é relativamente nova no vocabulário, como afirma o Dicionário Merrriam-Webster. As Fake News sempre estiverem presentes ao longo da história, bem antes do jornalismo ser prejudicado

pelas fakes, escritores já espalhavam notícias falsas sobre seus desafetos por meio de comunicados e obras.

O advento das redes sociais trouxe um turbilhão de notícias falsas impulsionadas por pessoas de grande influência, geralmente políticos, que contratam equipe para que produzam um material que se torne viral, e assim, consigam alcançar seus objetivos, lançando mão da premissa de vencer e derrubar o seu oponente utilizando qualquer meio, mesmo que isso venha prejudicar a sociedade como um todo.

Alguns produtores de fake news compram ilegalmente os endereços de e-mail e números de telefone celular de milhões de pessoas para tornar "viral" os conteúdos falsos. Sendo assim, nas redes sociais são criados perfis falsos que ao interagir com outros indivíduos acabam dando veracidade às notícias que se espalham rapidamente.

Há um grande investimento em tecnologia e estratégias para que os produtores não sejam identificados ou rastreados, que utilizam a alteração do IP (endereço eletrônico do computador) guardando o conteúdo produzido nas chamadas "nuvens". Além da dificuldade em localizar os culpados, a legislação brasileira não têm uma punição exclusiva para esse tipo de delito.

É imprescindível ressaltar o perigo da Fake News, pois ao compartilharmos informações falsas, fotos e vídeos, podemos promover e trazer danos a saúde pública, incentivar o preconceito e resultar em mortes. Um dos exemplos mais emblemáticos são os movimentos antivacinação que ao espalharem notícias falsas propagando suas visões de que as vacinas fariam mal colocaram a população em perigo, com isso, deram retorno a doenças consideradas erradicadas no país como, sarampo, catapora, coqueluche, caxumba e poliomielite. Nesse sentido, o Ministério da Saúde precisou promover campanhas para combater as fake news e passou a disponibilizar um número de whatsapp para envio da população. O canal não é um SAC (Serviço de Atendimento ao Consumidor), mas, um espaço exclusivo para receber informações virais que serão apuradas pelas áreas técnicas e respondidas oficialmente se é verdade ou mentira, ou seja, qualquer pessoa poderá enviar gratuitamente mensagens com imagens ou textos

que tenha recebido nas redes sociais para confirmação se a informação procede ou não.

É alarmante o modo como às notícias falsas se espalham e os danos irreversíveis que elas podem causar, a exemplo temos os casos de preconceito e xenofobia contra os imigrantes venezuelanos que após um discurso de ódio espalhados pelas redes sociais sofreram ataques nos acampamentos em que estavam alocados. Em 2014, o Brasil presenciou um caso de fake news que acabou de forma trágica, uma mulher foi linchada até a morte após um boato no facebook de que a mesma seqüestrava crianças para rituais de magia negra.

O combate a fake news é algo difícil, no caso do usuário da internet é de extrema importância conseguir identificar uma notícia falsa ou sensacionalista e não compartilhar conteúdo duvidoso. Nesse caso, enfrentamos também, uma falta de empatia com o outro. Ao compartilhar um conteúdo mesmo sabendo que pode destruir a vida de uma pessoa sem nenhum senso crítico nos torna co-autores de delitos gravíssimos.

4. ÓRGÃOS ESPECIALIZADOS NO COMBATE AOS CRIMES CIBERNÉTICOS

O combate aos crimes cibernéticos é de responsabilidade federal e estadual, quando se trata de âmbito federal temos a atuações do Ministério Publico Federal que trabalha juntamente com a Policia Federal e a organização não governamental Safernet , organização que tem como objetivo combater a pornografia infantil, hoje é uma referencia nacional pelo enfretamento aos crimes cibernéticos e as violações aos direitos humanos na internet, na esfera estadual a responsabilidade é da policia civil.

As delegacias especializadas nos crimes cibernéticos são encontradas em vários estados brasileiros, podemos encontrar os endereços no site Safernet. Quando não houver delegacia especializada na cidade e nem na região da pessoa que foi vitimada, a indicação é que a pessoa procure uma delegacia comum.

A Polícia Federal investiga os crimes de natureza transnacional em que o Brasil tenha se comprometido por meios internacionais, e também contra a Administração Pública direta e indireta.

O Ministério Público Federa (MPF) é responsável pelos crimes de pornografia infanto-juvenil, racismo, crime de ódio, fraudes bancárias vinculadas à Caixa, que é uma instituição federal.

O Ministério Público Federal no ano de 2018 redigiu duas notas técnicas para nortear a atuação dos procuradores nos casos de Fake news no âmbito criminal, eleitoral e para as empresas multinacionais de internet como Facebook que tramita no STF.

5. A FALTA DE UMA LEGISLAÇAO ESPECÍFICA

Hoje se faz necessário a criação de uma legislação específica para os crimes cibernéticos ou cybercrimes, onde surgem duas figuras,sendo elas, o hacker e o cracker. Embora a expressão hacker geralmente apareça associada a infrações virtuais, são os crackers os reais criminosos. No Brasil, há insuficiência de leis para punição de infrações virtuais.

Os hackers são programadores com um extenso conhecimento acerca de sistema que não tem propósito de causar danos, já os crackers, segundo Cassant “... deriva do verbo inglês “to crack”, que significa de quebrar. Entre as ações, está a prática de quebra de sistema de segurança, código de criptografia e senha de acesso a redes, de forma ilegal e com intenção de invadir e sabotar para fins criminosos.” Alguns buscam lucrar com vendas de informações, já outros, almejam unicamente notoriedade. Tal carência leva crackers e até mesmo pessoas comuns a propiciar consideráveis danos, tendo como exemplos pedofilia, publicações de informações pessoais e crime

contra honra. O judiciário apresenta soluções imediatas que não sanam o problema de forma permanente e eficaz.

A internet tem se expandido, com isso esse tipo de crime está aumentando a cada ano e paralelo a isso o número de usuários, segundo Emerson Wendt, são " A evolução tecnológica e o barateamento dos computadores e dispositivos móveis de acesso à rede mundial", dessa forma devem ser criados mais leis mais rígidas para inibir os criminosos a prática de delitos no ambiente virtual, pois algumas condutas não são tipificadas e outras para que haja investigação as informações.

Alguns crimes cibernéticos são tipificados pelo código penal, como os crimes contra a honra. O código é de 1940, tem previsões legais, o problema é que as penas são muito brandas com base nas conseqüências sofridas pela vitima. O que existe no Brasil é alguns artigos e leis para atuações específicas, não abrange todas as situações desses crimes.

Foi criada a lei 12.737 em 30 de novembro de 2012, visando proteger a privacidade e a intimidade, que estão presentes no artigo 5º da Constituição Federal de 1988, existindo certas críticas a essa lei.

Art.5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros, residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: Outra lei foi a de 2014 chamadas de "Marco Civil da Internet", Lei 12.965.

Tem a finalidade de preencher espaços deixados pelo nosso ordenamento jurídico a respeito dos crimes virtuais.

Ficou tipificado os princípios de liberdade, neutralidade e privacidade. Determinou garantias, direitos e deveres do ambiente virtual.

Um dos principais direitos e garantias resguardadas que merece um destaque é da intimidade e da vida privada. Mesmo com proteção desses direitos e garantias, os artigos não abrangem por completo todas as práticas dos criminosos deixando espaços que só podem ser completados por outra legislação. Exemplo é o caso de compra on-line tem como proteção pelo Código de Defesa do Consumidor.

6 - CONCLUSÃO

No presente artigo, abordamos o ponto relativo aos crimes cibernéticos, desde o momento em que a sociedade passou a utilizar o mundo virtual, como também, o modo como os criminosos começaram a usufruir desse ambiente com o intuito de obter vantagens, prejudicar a imagem de terceiros ou apenas danificar dados ou dispositivos eletrônicos.

É notório, que ao longo dos anos os criminosos foram se aperfeiçoando ao ponto de causar impactos gigantescos, gerando uma grande dificuldade na vida das autoridades competentes. Como já mencionamos anteriormente os crimes virtuais cresceram de forma absurda alterando o curso de vidas, empresas e campo político o que deixa as pessoas temerosas em relação à linha tênue da verdade ou mentira, e nos coloca também no limite da consciência humana entre ética, caráter e cidadania.

Nesse sentido, é preciso urgências em atualizar o código penal, com o intuito de coibir tais ações, como também, deixar o país equiparado a de outros países para que possamos trabalhar em conjunto nos crimes de caráter transacionais.

Portanto, é preciso que as esferas jurídicas estejam verdadeiramente pró-ativas a promoveram tais mudanças e aperfeiçoamentos para que desta forma possamos combater esses delitos de forma severa, protegendo assim, os cidadãos de bem do nosso país.

7. REFERÊNCIAS BIBLIOGRÁFICAS

- JUSBRASIL – Chantagem contra atriz Carolina Dieckman por causa de 36 fotos nuas. Disponível em: <https: //espaco-vital. jusbrasil.com. br> acesso em: 30 Novembro.2019.

- JUS.COM. BR – Insuficiência das leis em relação aos crimes cibernéticos.

Praticados no Brasil. Disponível em: < https: //jus.com. br>. Acesso em 07 de novembro de 2019

- JUSBRASIL – Estatuto da Criança e do Adolescente, Lei 8069/90. Disponível em: < https: //presrepublica. jusbrasil.com. br >. Acesso em 01 Abril 2019.

- MINISTÉRIO PÚBLICO FEDERAL - Crimes cibernéticos levam MPF a atuar em

2.611 processos em 2018. Disponível em: < http://www.mpf.mp.br > Acesso em: 03 Novembro 2019.

- NOTÍCIAS - O Brasil já é considerado um pólo de cibercrime mundial.

Disponível em: < http://www.administradores.com.br > acesso em: 28 Outubro de 2019.

- NOTÍCIAS. UOL – Brasil é o segundo país do mundo com maiores números de crimes cibernéticos. Disponível em: <https: //noticias. uol.com. br > acesso em: 27 Novembro. 2019.

- NOTÍCIAS UOL – Whatsapp vira ferramenta favorita de hackers para aplicar golpes no Brasil. Disponível em: <https: //noticias. uol.com. br> acesso em: 27 Agosto 2019.

- SAFERNET – Delegacias cibercrimes. Disponível em: < https: //new. safernet.org. br > acesso em: 16 de Novembro de 2019.

- SAFERNET - Quem somos. Disponível em: < https: //www.safernet.org.br > Acesso em: 03 julho de 2019.

- SENADO FEDERAL- Senado Notícias - Sancionada lei que autoriza infiltração na internet para investigar pedofilia. Disponível em: < https: //www12. senado.leg. br >.Acesso em: 01 Agosto de 2019.

- SHARIFF, Shaheen – Cyberbullying: questões e soluções para a escola, a sala de aula e a família. Porto Alegre de 2010.

- STF – Notícias STF - 1a Turma nega HC a condenado por armazenamento e Disseminação de pornografia infanto-juvenil. Disponível em: <http://www.stf.jus.br >. Acesso em: 01 Novembro de 2019.

- TODA MATÉRIA-HISTÓRIA e desenvolvimento do computador. Disponível e<https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/>. Acesso em: 06 Novembro de 2019.

- WENDT, Emerson. Inteligência Cibernética, a insegurança virtual no Brasil. São Paulo; Delfos. 2011. CANALTECH-O que é Cibercrime? Disponível em: < https: //canaltech.com. br > acesso em: 27 Outubro de 2019.