SEMANA ACADÊMICA
REVISTA CIENTÍFICA
ISSN 2236-6717

CRIMES CIBERNÉTICOS NO BRASIL

[ver artigo online]

Jéssica Lima Silvério dos SANTOS[1]
Delner do Carmo AZEVEDO[2]

RESUMO

A internet é uma rede mundial de dispositivos interligados com um propósito de servir os usuários. Através dela há socialização entre pessoas ou grupos, por meio das mensagens eletrônicas, e-mail, vídeo chamada e busca em sites em qualquer localidade do mundo. Diante de uma pandemia em pleno século XXI, o único meio de socialização veio através os dispositivos eletrônicos ligados a internet. Com apenas um clique você pode ter acesso a uma gama de conteúdos digitais, proporcionando aos usuários e internet uma grande facilidade de comunicação. Porém, essa viabilidade esconde um lado obscuro, organizações de rede de crime cometidos no submundo cibernético, este artigo como objetivo abordar os crimes cibernéticos, tais como, falsificação ideológica, pornografia infantil, calúnia, difamação, *bullyng,* extorsão, plágio, dentre outros previstos no Código Penal Brasileiro, bem como suas devidas penas.

Palavras-chave: Crimes. Cibernéticos. Pedofilia. Internet. Infantil.

CYBER CRIMES IN BRAZIL

ABSTRACT

The internet is a worldwide network of devices interconnected with the purpose of serving users. Through it there is socialization between people or groups, through electronic messages, e-mail, video calls and search on websites anywhere in the world. Faced with a pandemic in the middle of the 21st century, the only means of socialization came through electronic devices connected to the internet. With just one click, you can access a range of digital content, providing internet users with great ease of communication. However, this viability hides a dark side, crime network organizations committed in the cyber underworld, this article aims to address cyber crimes, such as ideological falsification, child pornography, slander, defamation, bullying, extortion and plagiarism, among others provided for in the Code Brazilian Penal Code as well as their due penalties.

Keywords: Crimes. Cyber. Pedophilia. Internet. Children.

1 Graduanda do curso de Direito da Faculdade São Lucas, Rondônia, e-mail jessicapazzini@gmail.com.
2 Professor Especialista e Orientador da Faculdade São Lucas, Rondônia, e-mail delnerazevedo@gmail.com.

http://dx.doi.org/10.35265/2236-6717-227-12357
FORTALEZA-CE. EDIÇÃO 227. V.10. ANO 2022.

INTRODUÇÃO

O presente artigo tem por realizar a importância da exposição e vulnerabilidade em relação aos crimes cibernéticos, o sistema jurídico brasileiro junto com o Código Penal tem apresentando uma certa ineficiência nas condutas ilícitas praticadas no ambiente virtual. Diante de uma pandemia em pleno século XXI, o único meio de socialização veio por meio de dispositivos eletrônicos ligados a internet. Com apenas um clique você pode ter acesso a uma gama de conteúdos digitais, proporcionando aos usuários de internet uma grande facilidade de comunicação. Porém, essa viabilidade esconde um lado obscuro, organizações de rede de crimes cometidos no submundo cibernético. Conceituando alguns dos crimes são: falsificação ideológica, pornografia infantil, calunia difamação, *bullyng*, extorsão e plagio dentre outros previsto no Código Penal Brasileiro, que serão abordados ao longo desse projeto de pesquisa.

Por fim, com a falta de uma punição é mais rigorosa da parte legislação específica, para tais atos ilícitos praticados no meio virtual, tem como base, para ser julgado dentro das diretrizes do Código Penal. Por demonstrar ser uma boa alternativa para a tipificação das ações ilícitas, feitas no ambiente da internet há um certo receio, sendo tratado com cautela pelo fato de ofender o princípio da legalidade.

REFERÊNCIAL TEÓRICO

A história das redes sociais

A internet é uma rede mundial de dispositivos interligados com um propósito de servir os usuários. Através dela há socialização entre pessoas ou grupos, por meio das mensagens eletrônicas, e-mail, vídeo chamada e busca em sites em qualquer localidade do mundo. O surgimento da internet está associado a fins militares, dando início nos anos de 1960, diante da Guerra Fria. Com o intenso conflito, o governo norte-americano desenvolveu um sistema de comunicação que não fosse vulnerável em um possível ataque de bombas, sendo capaz de unificar os pontos estratégicos com a base das Forças Armadas. (VIEIRA, 2003).

Na época, os Estados Unidos observaram as ações de seu rival, a União Soviética, avançando na corrida espacial, colocando o primeiro satélite em órbita o *Sputnik 1*, em outubro de 1957, mandando o primeiro ser vivo em uma viagem, a cadela *Laika*, a bordo da *Sputnik 2*, em novembro de 1957 e mandando o primeiro homem a viajar pelo espaço, *Yuri Gagarin*, em abril

de 1961, a bordo da *Vostok I.* (VIEIRA, 2003, p.4). Os Estados Unidos diante de um cenário na guerra fria de total desequilíbrio sabiam que a criação de um sistema de tecnologia poderia mudar o percurso da guerra, dando a vitória ou possivelmente a derrota. Tendo uma importante decisão, insistir no programa de desenvolvimento acadêmico nas pesquisas científicas voltado à área de tecnologia. (VIREIRA, 2003).

Em 1969, a agência Americana *ARPA (Advanced Research and Projects Agency),* órgão responsável pelo desenvolvimento de pesquisas científicas e tecnológicas para fins militares, concedeu uma rede que interligava computadores, por cabos subterrâneos, com o objetivo de interconectar as bases militares e os departamentos de pesquisas do governo norte – americano. (CASTELLS, 2003, p. 13-14).

O funcionamento ocorreu pela primeira vez em 1972, interligando os computadores de quatro universidades. Onde a Universidade da Califórnia em Los Angeles - UCLA enviou a seguinte mensagem de texto: “Você está recebendo isto?”. Tendo recebido a mensagem, as demais universidades responderam enviando a palavra afirmativa “SIM”, mostrando que a conexão tinha dado um resultado positivo. Com o passar dos anos, a internet foi ganhando formas para se adequar às necessidades, se tornando privada e saindo assim dos campos de pesquisas científicas e ganhando as casas dos futuros usuários seu texto aqui.

A internet no Brasil

O ano da internet no Brasil foi em 1988, tendo o seu desenvolvimento da mesma forma do surgimento da internet em um ambiente acadêmico científico. No mesmo ano, a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), junto com a Secretaria Estadual de Ciência do Estado de São Paulo, realizou a primeira conexão. O interesse maior era a construção de uma infraestrutura de rede nacional nos ambientes acadêmicos. Com isso veio à instalação de pontos específicos nas principais capitais do país interligando as redes das universidades. Em 1994, os ministérios de Ciência e Tecnologia e das Comunicações, a RNP e a Embratel, em uma ação conjunta, trouxeram em larga escala a internet para dentro dos lares dos usuários brasileiros. (VIEIRA, 2003, p.8).

Proteção de dados

A Lei nº 13.709 que se refere a Lei Geral de Proteção de Dados Pessoais foi sancionada no dia 14 de agosto de 2018, tendo com a sua principal inclusão uma lei específica para a proteção de dados e privacidades dos cidadãos Brasileiros. O Trâmite no Congresso Nacional desta Lei teve duração de dois anos entre Câmara e Senado, contou com duas consultas públicas, mais de duas mil e quinhentas contribuições entre pessoas naturais e jurídicas de vários setores da sociedade, nacionais e internacionais, além de inúmeros eventos. (MONTEIRO, 2018).

Vale ressaltar que a Lei se aplica a qualquer operação realizada por pessoa física ou jurídica de direito público ou privado, tendo a independência da localização do país onde se encontram os dados.

Sobre os fundamentos estão elencados no artigo 2 da Lei n°13.709, o respeito à privacidade, à autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre-iniciativa a livre concorrência e a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (MARINELI, 2019).

O inciso I, do artigo 6º da referida Lei, diz:

> As atividades de tratamento de dados pessoais deverão observar a boa fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informando o titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Este princípio tem uma atenção especial, pois trata-se da relação direta com a proteção da privacidade, vinculando os dados pessoais que poderá ser avaliado regularmente. Logo, os dados que são coletados só poderão ser utilizados para as finalidades que foram autorizadas pelo usuário, sendo possível ainda impedir que continue a transferência de dados a terceiros através de uma segurança onde irá detectar possíveis abusos que vão além da autorização do uso de dados.

Crimes cibernéticos

Diante dos dias que estamos vivendo, é cada vez mais preferível estar conectado a aparelhos que proporcionam acesso ao mundo virtual. A facilidade de interação de duas ou um

grupo de pessoas é extraordinário, até mesmo inovador em meio ao distanciamento social. O ato de navegar na internet, expressão que se dá a pessoa que passeia na internet, vem sendo costumeiro, com os aplicativos de relacionamentos. Porém, existem criminosos capazes de apenas estarem através de uma tela de computador cometer crimes virtuais, utilizando um dispositivo conhecido como *Malware* (aplicativo que adentra um sistema, com a intenção de roubar dados de terceiros, ou até mesmo danificar os dispositivos elétricos).

Uma simples interação social, trocas de e-mail, mensagens e ato de visitar sites contendo este vírus, os criminosos roubam os dados pessoais das vítimas, ou seja, o *malware* é o principal responsável por roubar os dados das vítimas, dando origem aos cibercrimes. Contudo os criminosos utilizam-se da internet, para a prática de outros cibercrimes, como assédio, injúria, calúnia, difamação, pedofilia, apologia ao crime e até mesmo o ato de terrorismo. O número crescente de cibercrimes cada vez torna-se comum, devido à falsa sensação de impunidade do ato praticado por acharem que não há como deixar rastros de identificação.

Tipificação dos crimes cibernéticos

Na linha de pensamentos de muitos usuários da internet os crimes ali praticados estão impunes definido o fato de não deixaram rastros, porém existe a tipificação e quando identificados recebem a sanção penal. Segue alguns crimes comuns previstos no Código Penal Brasileiro (CPB).

Assédio sexual, previsto no artigo 216-A do CPB:

> Constranger alguém com o intuito de obter vantagem ou favorecimento sexual, prevalecendo-se o agente da sua condição de superior hierárquico ou ascendência inerentes ao exercício de emprego, cargo ou função. Pena de detenção, de 1 (um) a 2 (dois) anos.

Segundo o artigo supracitado, o assédio sexual é um crime que consiste em constranger alguém na intenção de obter favorecimento de cunho sexual, através de poder hierárquico. As atitudes vão de uma tentativa de um beijo roubado, gestos que causam constrangimentos ou o ato que viole a liberdade sexual.

Pornografia infantil, previsto no artigo 240 e 241 do Estatuto da Criança e do Adolescente (ECA), onde diz no art. 240 “Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou

adolescente. Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa", e no artigo 241, dispõe sobre a venda "Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa."

Dentre as denúncias mais recorrentes de crimes virtuais, estão em grande escala a fraudes e pornografia infantil. Sendo o Brasil, ocupando o 4• lugar, no ranking mundial em material disponível na internet sobre a pedofilia e a pornografia infantil, com uma estrutura de combater tal crime, alinhados com as polícias para desintegrar e achar quem os comercializam através de fotos e vídeos com teor pornográfico envolvendo menores de idade. (G1, 2008)

Conforme Guilherme de Souza Nucci:

> A maneira pela qual o autor do crime adquire, possui ou armazena o material é livre, valendo-se o tipo da expressão "por qualquer meio" Comumente, com o avanço da tecnologia e da difusão dos computadores pessoais, dá-se a obtenção de extenso número de fotos e vídeos pela Internet, guardando-se o material no disco rígido do computador, em disquetes, DVDs, CDs, pen drives, entre outros. (2018, p. 849)

De acordo com os artigos 240 e 241 do Estatuto da Criança e do Adolescente, produzir, comercializar, publicar foto ou vídeo de criança e adolescente, através da internet, tipifica conduta criminosa com apologia à pedofilia. Mesmo os que guardam esse tipo de conteúdo em sites e em seus aparelhos pessoais, praticam o mesmo delito.

Calúnia, difamação, injúria, crimes estes relacionados à honra da pessoa tipificados nos artigos 138 "Caluniar alguém, imputando-lhe falsamente fato definido como crime", artigo 139 "Difamar alguém, imputando-lhe fato ofensivo à sua reputação" e artigo 140 "Injuriar alguém, ofendendo-lhe a dignidade ou o decoro".

A calúnia geralmente acontece na falsa existência de acusação de um crime a determinada pessoa. Ou seja, mesmo sabendo que o crime é falso, torna-o público ou divulga, trazendo um contexto virtual, muito direcionado às *Fakes News*, com compartilhamento do ato nas redes sociais.

Difamação nada mais é que a ofensa praticada contra a reputação de alguém, levando ao conhecimento de terceiros, na forma de falar mal de outrem em redes sociais.

A injúria é a ofensa praticada contra a dignidade da pessoa, não haverá necessidade do conhecimento de terceiros. Basta a pessoa sentir-se ofendida, sendo qualificados na forma de

ofensas relacionadas, a raça, cor, etnia, religião, idade e pessoa com deficiência. Com a coleta de provas, através do registo da ocorrência (boletim de ocorrência), em delegacias especializadas, será dado o andamento de uma investigação, no qual haverá a determinação de busca e apreensão informática e a quebra do sigilo informático.

O crime cibernético puro tende a ser atos de comportamentos ilícitos, o principal objetivo é invadir o sistema computacional, seja o *hadware* ou o *software*, abrangendo os dados dos sistemas. Com essa modalidade, o foco dos criminosos é o equipamento, junto com as informações nos bancos de dados.

Legislação Pertinente

A lei exerce um papel de suma importância, no meio do ordenamento jurídico. Sendo relevante em trazer objetivos, que será de grande valia, no direcionamento na vida em sociedade, independente de qual ente surgiu à sua criação. Neste sentido, faz-se necessário explanar a Lei nº 12.737/2012, conhecida como a Lei Carolina Dieckmann, sendo sancionada em novembro de 2012. Tendo o seu surgindo, após um episódio onde envolvia a atriz Carolina Dieckmann, em que por meio da invasão de sua privacidade, em seu aparelho ligado à internet, teve fotos íntimas divulgadas, em uma exposição de proporção imensa, até sofrendo do crime de extorsão. Por esse, episódio, houve-se um debate na referida lei, que teve a alteração nos textos do Código Penal Brasileiro.

De acordo com Uchôa, “para ser legítima a tutela penal é necessária que o bem seja ‘digno’ dessa proteção, e que sua lesão ou ameaça efetivamente mereça uma sanção penal” (2009, online)

Com o episódio citado, envolvendo a atriz Carolina Dieckmann, a problemática teve um desfecho, pois diante dos fatos ocorrido não existia uma tipificação legal, que amparasse as vítimas, dos crimes cometido no ciberespaço. No Código penal, foram acrescidos os artigos 154-A e 154-B, sendo tipificado as condutas criminosas de invasão de dispositivos de informática, em que o sujeito ativo (criminoso), tende a cometer tal violação indevida de obter dados ou informações, sem a autorização do sujeito passivo (vítima).

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou

> de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
> 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 concessionarias de serviços públicos. (Incluído pela Lei nº 12.737, de 2012) Vigência

Por fim, o Projeto de Lei (PL) 4.554/2020, do senador Izalci Lucas (PSDB-DF), foi aprovado em 28/05/2021. Com o preceito de alterar o Código Penal (Decreto-Lei 2.848, de 1940), para o agravamento das penas dos crimes como invasão de dispositivos, furto qualificado e estelionato ocorrido no ciberespaço, conectado ou não à internet. Consoante a nova redação do Código Penal, o crime de invasão de dispositivos informáticos passará a ter a punição de reclusão, de um a quatro anos, e multa, aumentando-se a pena de um terço a dois terços, caso a invasão resultar em um prejuízo ao bem econômico da vítima. Anteriormente a pena era mais branda, com a aplicação de detenção de três meses a um ano e multa.

Com a invasão provocada por meio de obter conteúdo de comunicações privadas, dados sigilosos de indústrias e comerciais, sem a prévia autorização do dispositivo invadido, a pena é de reclusão de dois a cinco anos multa. O que no passado a pena não passava de seis meses a dois anos e multa. O Regime de reclusão do cumprimento da pena, poderá ser fechado. Diante do fato, a reclusão torna-se uma aplicação branda, não admitindo o início do cumprimento em regime fechado. Conforme as palavras proferidas por Cunha “A atual orientação jurisprudencial acaba por estabelecer o império da impunidade em relação a essas fraudes, com grave prejuízo à administração da justiça e à sociedade em geral”. (Fonte: Agência Senado).

CONSIDERAÇÕES FINAIS

A presente pesquisa foi de grande relevância, abordando os principais aspectos dos crimes virtuais, narrando o tratamento legal e as restrições no combate ao *cibercrime*. Como a tecnologia vem se aperfeiçoando com o tempo, os cibercriminosos acompanha essa tendência, praticando delitos de roubo de informações bancárias, extorsão, ameaças, difamação e crimes com apologia à pedofilia infantil, sendo constante o aumento desses crimes no meio virtual. Por mais que o ambiente virtual da aquela sensação de liberdade, nas práticas dos crimes, a nossa Constituição Federal de 1988, veda o anonimato, tendo isso uma característica inicial dos crimes virtuais. Bem como, o Direito de privacidade, assegurando a proteção da vida privada e a intimidade de todos, sendo uma das principais linhas na defesa dos direitos, no âmbito virtual.

Além disso, vale ressaltar os princípios básicos da legalidade, tendo vários atos ilícitos que têm a sua previsão na legislação penal, sendo punidos independentemente do local praticado (mundo real ou virtual).

Em compensação, houve a criação de outras legislações, com o intuito de tratar e punir tais crimes virtuais. Dentre elas, a Lei nº 12.737 de 2012, especifica o crime de invasão por meio de dispositivos ligados a internet, alterando os artigos do código penal, adequando-os a realidade cibernética. Vale ressaltar a importância do Marco Civil da internet, teve a sugestão de regulamentar, estabelecendo direitos, deveres, princípios e garantia no espaço virtual.

Já no âmbito judicial, há uma limitação em conseguir provas, por conta do anonimato dos indivíduos, bem como os métodos investigativos, tem a sua deficiência em apontar de fato, o autor do delito no meio virtual.

Por fim, as tecnologias veem modificando e tendo certa influência na sociedade. Sendo uma forma facilitadora de buscar tudo que há de se aprender, a rede social se torna poderosa ferramenta, desvalorizando a privacidade e trazendo uma vulnerabilidade para os seus usuários, por práticas criminosas de cibercriminosos.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSUNÇÃO, Ayume da Silva, **A Tipicidade dos Crimes Cibernéticos no direito Penal Brasileiro: um estudo sobre o impacto da Lei n° 12.737/2012 e a (des) construção de uma dogmática penal dos crimes cibernéticos**, Guanambi, Bahia, 2021.

BRASIL. **Lei 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 12 de novembro de 2022.

BRITO, Auriney Uchoa de. **O bem jurídico-penal dos delitos informáticos. Boletim IBCCrim**. n. 199, 2009.. https://www.ibccrim.org.br/noticias/exibir/4800/, Acessado 14 de novembro de 2022.

CUNHA, Rodrigo; BAPTISTA, Rodrigo; **Lei com penas mais duras contra crimes cibernéticos é sancionada Fonte: Agência Senado, 2021.** https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada Acesso 15 de novembro de 2022
CRUZ, Diego; RODRIGUES, Juliana. **Crimes Cibernéticos e a Falsa Sensação de Impunidade.** Revista Científica Eletrônica do Curso de Direito, 2018.

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social**. São Paulo: Atlas, 2006.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de Metodologia Científica**. São Paulo: Atlas, 2007.

MARINELI, Marcelo Romão. **Privacidade e Redes Sociais Virtuais**. Revista dos Tribunais, São Paulo: ABDR, 2019.

MATSUYAMA, Keniche Guimarães; LIMA, JAA. **Crimes cibernéticos: atipicidade dos delitos**. 2017.

NUCCI, Guilherme de Souza. **Estatuto da criança e do adolescente comentado. 4a ed. rev., atual. e ampl. – Rio de Janeiro:** Forense, 2018

SANTOS, Gabrielly Daianne Alves ; **CRIMES VIRTUAIS: tratamento legal e limitações no combate aos crimes cibernéticos**, 2021.