CENTRO DE EDUCAÇÃO SUPERIOR REINALDO RAMOS - CESREI
FACULDADE REINALDO RAMOS – FARR
CURSO DE BACHARELADO EM DIREITO

SELINEIDE DE SOUSA

CRIMES CIBERNÉTICOS: UMA ANÁLISE DAS ATUAIS LEGISLAÇÕES VIGENTES QUE TRATAM CRIMES DIGITAIS

CAMPINA GRANDE – PB
2021

SELINEIDE DE SOUSA

CRIMES CIBERNÉTICOS: UMA ANÁLISE DAS ATUAIS LEGISLAÇÕES VIGENTES QUE TRATAM CRIMES DIGITAIS

Trabalho Monográfico apresentado à coordenação do Curso de Direito da Faculdade Reinaldo Ramos – FARR, como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientadora: Prof. Esp. Ranalisson Santos Ferreira.

CAMPINA GRANDE – PB
2021

SELINEIDE DE SOUSA

CRIMES CIBERNÉTICOS: UMA ANÁLISE DAS ATUAIS LEGISLAÇÕES VIGENTES QUE TRATAM CRIMES DIGITAIS

Aprovado em 14 de Dezembro de 2021.

BANCA EXAMINADORA:

_____

Prof. Esp. Ronalisson Santos Ferreira
Faculdade Reinaldo Ramos - FARR
Orientador

_____

Prof. Me. Rodrigo Araújo Reul
Faculdade Reinaldo Ramos - FARR
1º Examinador

_____

Profa. Me. Diego Coutinho Araújo
Faculdade Reinaldo Ramos - FARR
2° Examinador

S725c Sousa, Selineide de.
Crimes cibernéticos: uma análise das atuais legislações vigentes que tratam crimes digitais / Selineide de Sousa. – Campina Grande, 2021.
35 f.
Monografia (Bacharelado em Direito) – Faculdade Reinaldo Ramos FAAR, Centro de Educação Superior Reinaldo Ramos-CESREI, 2021.
"Orientação: Prof. Esp. Ronalisson Santos Ferreira".

1. Crimes Digitais. 2. Fake News. 3. Crimes de Ódio – Redes Sociais. 4. Internet – Crimes Cibernéticos. 5. Legislação. I. Ferreira, Ronalisson Santos. II. Título.

CDU 343.63:004.738.5(043)
FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

AGRADECIMENTOS

Faço aqui meus agradecimentos primeiramente ao meu orientador, professor Ronalisson, por ser a primeira pessoa a depositar confiança e estímulo no meu trabalho de conclusão de curso nesta graduação. Aproveito a oportunidade e expresso minha gratidão a minha família, pelo apoio incondicional, todas as honras. Aos professores, colegas e funcionários faculdade Cesrei, pela convivência agradável e pela colaboração prestada;

E a todos que, citados ou não, sabendo ou não, querendo ou não, longe ou perto, diretos ou indiretamente, de uma forma ou de outra, contribuíram para a concretização deste trabalho e realização de mais um sonho. Há todos meus muito obrigados.

RESUMO

Este trabalho trata-se de um estudo descritivo que tem como objetivo principal analisar os crimes digitais sobre o olhar da legislação vigente no país, apresentando dessa forma as principais leis existentes em relação a essa temática, utilizando para tanto uma abordagem bibliográfica, também chamada de descritiva. Conceituando os crimes digitais ou crimes cibernéticos que são fatos típicos e antijurídicos cometidos por meio ou contra a tecnologia informação, ou seja, um ato ilegal, cometido através da informática em geral. Citando as principais normas como a lei 12.837 de 2012, Lei Carolina Dieckmann, Lei 12.965 de 23 de abril de 2014, Marco Civil da Internet e também a de grande importância que é a Lei nº 13.709/18, lei Geral de Proteção de Dados Pessoais, todas inseridas no nosso ordenamento jurídico, as quais vem a definir, comportamentos de usuários e provedores com o trato de dados e atividades realizados por esses no país que possam ser caracterizados como atos ilícitos, prejudiciais tanto ao patrimônio como honra dos indivíduos como as *fake news* e os crimes de ódio, e a as dificuldades sofrida nas apurações dos ilícitos cometidos por esses criminosos através da internet.

Palavras chave: Crimes digitais, legislação, *fake news* e crimes de ódio, internet.

ABSTRACT

The main objective of this paper is to analyze digital crimes from the perspective of the current legislation in our country, using a bibliographic approach. Conceptualizing digital crimes or cybercrimes that, according to the authors Jesus and Milagres (2016), are typical and unlawful facts committed through or against information technology, i.e., a typical and unlawful act committed through information technology in general. Citing the main norms as the law 12.837 of 2012, Carolina Dieckmann Law, Law 12.965 of April 23, 2014, Marco Civil da Internet and last and of great importance, was the Law no. 13. 709/18, the General Law of Personal Data Protection, all inserted in our legal system, which defines the behavior of users and providers with regard to the treatment of data and activities performed by them in the country that can be characterized as illegal acts, harmful both to the property and honor of individuals such as fake news and hate crimes, and the difficulties suffered in the investigation of crimes committed by these criminals over the Internet.

KeyWords: Digital crimes, legislation, fake new, hate crimes, internet.

SUMÁRIO

INTRODUÇÃO 8

CAPÍTULO I CRIMES CIBERNÉTICOS 4
1.1 EVOLUÇÕES LEGISLATIVAS 11
1.2 O MARCO CIVIL DA INTERNET 13

CAPÍTULO II TIPOS DE CRIMES CIBERNÉTICOS 17
2.1 CRIMES DE MAIORES INCIDÊNCIAS CONTRA O PATRIMÔNIO NO PAÍS 18
2.2 AS FAKES NEWS NO AMBIENTE DIGITAL 21

CAPÍTULO III DISCURSO DE ÓDIO NAS REDES SOCIAIS 23
3.1 POSICIONAMENTOS JURISPRUDENCIAIS EM RELAÇÃO AOS CRIMES CONTRA HONRA 26
3.2 AS DIVERSIDADES DE PROVAS DIGITAIS 28

CONSIDERAÇÕES FINAIS 30

REFERÊNCIAS 32

INTRODUÇÃO

Na atualidade é notável que o mundo de maneira geral que está altamente interligado a partir dos meios tecnológicos e a internet, o que faz com que todos sejam bombardeados diariamente com inúmeras informações de diferentes países em tempo de certa forma instantâneo, o que acarreta reações diversas na sociedade (ROCHA, 1996).

Essas modificações facilitaram alguns serviços que anteriormente demoravam a ser executado, bem como em um banco que costumava-se passar horas em longas filas para realizar serviços como transferência e pagamentos de fatura, esses que agora podem ser realizados por meio de aparelhos digitais com acesso à internet, já que são ofertadas essas operações em aplicativos disponíveis para download. O compartilhamento de informações como notícias que antes eram expostos apenas em telejornais da televisão ou no rádio é facilitado através da utilização dos sites e principalmente das redes sociais (PINHEIRO, 2011).

Como sabe-se infelizmente com a facilidade não surgem apenas vantagens para o cidadão, afinal evidenciaram a partir dessas modalidades um aumento considerável de crimes cibernéticos esses que ocorrem por meio do ambiente virtual, os indivíduos que se beneficiam através do pouco conhecimento de algumas pessoas sobre o novo, e que por vezes atraem suas vítimas para agir de forma criminosa, seja roubando seus dados pessoais, ameaçando-os ou até mesmo clonando suas informações e furtando seus bens, por essa razão os consumidores destes serviços devem procurar ter conhecimento a respeito dos crimes de inúmeras vertentes causados virtualmente como *Fake News* e os crimes de ódio, estelionato, entre outros (BARRETO, 2020).

Surgindo com isso, uma inquietação em observar como a legislação atua nesses casos, as leis que existiam ou que foram criadas para autuar criminosos que cometem esses delitos no mundo digital, será que os crimes cometidos presenciais

ganham formato digital? Para que seja possível responder esse questionamento, o presente estudo tem como principal objetivo analisar os crimes digitais existentes e a atuação da legislação vigente em no país, trazendo como objetivos específicos, observar como se dá os crimes cibernéticos, conceituando o mesmo, ressaltar como se deu o surgimento de algumas leis na área e sua importância, por fim, expor alguns casos sobre a temática para facilitar a compreensão da mesma e dessa forma, apresentar as razões por ter se tornado necessário elaboração de leis que visem autuar as práticas ilegais no universo digital para assim amenizar os impactos que a modernidade acarreta na vida das pessoas, buscando pela segurança de todos.

Portanto, para isso, utilizando metodologicamente uma abordagem bibliográfica e descritiva se enquadrando em uma pesquisa qualitativa, esse tipo de estudo também chamado em alguns momentos de análise documental, é utilizado para um melhor entendimento do conteúdo. Como pontua Boccato: Esse tipo de pesquisa trará subsídios para o conhecimento sobre o que foi pesquisado, como e sob que enfoque e/ou perspectivas foi tratado o assunto apresentado na literatura científica. Para tanto, é de suma importância que o pesquisador realize um planejamento sistemático do processo de pesquisa, compreendendo desde a definição temática, passando pela construção lógica do trabalho até a decisão da sua forma de comunicação e divulgação (BOCCATO, 2006, p. 266).

Sendo assim, foram analisados e descritos dados disponíveis em fontes secundárias, materiais impressos e eletrônicos tais como livros, artigos dissertações e monografias, procurando conhecer as definições do corpus abordado. Do ponto de vista metodológico este estudo classifica-se dentro de uma abordagem qualitativa com isso, “[...] o cientista é ao mesmo tempo é o sujeito e o objeto de suas pesquisas. O conhecimento do pesquisador é parcial e limitado” (GERHARDT; SILVEIRA, 2009, p. 32).

Em relação à organização estrutural do trabalho, o mesmo divide-se em três capítulos, o primeiro aborda acerca da conceituação dos crimes cibernéticos a evolução da legislação nesses casos é o marco civil da internet, o segundo capítulo traz os tipos de crimes e os mais comuns contra a sociedade, abrangendo também sobre *fake News*, já nos preparando para o último capítulo que vem com a questão dos discursos de ódio que são expostos e os *ciberbullying*, discutindo a temática e logo após teremos as considerações finais.

CAPÍTULO I

1 CRIMES CIBERNÉTICOS

Com o fenômeno da globalização, avanços tecnológicos, nas últimas décadas da internet, a sociedade está cada vez mais conectada, fazendo a utilização de meios tecnológicos para realizar tarefas que muitas vezes demandava tempo e muita paciência, como por exemplo, ir ao banco realizar serviços bancários, marcar consultas médicas, fazer compras no supermercado, fazer solicitação de serviços em geral, tudo isso na atualidade pode ser realizados com apenas alguns toques na tela dos aparelhos de informática.

Ao ter em mãos um aparelho celular, computador, *table*t ou qualquer que seja a ferramenta de informática ligada à rede de internet, consegue-se realizar diversas tarefas em questão de segundos. Essas transformações tecnológicas trouxeram novos questionamentos, surgiram problemas sociais e principalmente as recentes modalidades de crimes, que até então somente eram realizados no mundo real, e que passaram a ser encontradas com maior intensidade no universo virtual, causando um dano bem maior às suas vítimas, pela capacidade dimensional do espaço da internet e a proporção que os mesmos podem tomar.

Segundo Blatt (2020):

> Os serviços oferecidos estão se ampliando e se popularizando, o comércio eletrônico vem crescendo em volume de vendas, os sites de bancos oferecem tantas facilidades para o cliente que acabam se tornando raras as vezes em que é necessário ir até uma agência bancária para pagar uma conta (BLATT, 2020, p. 69*).*

Com o crescimento e criação de ferramentas tecnológicas para dinamizar os serviços de instituições financeiras, foi perceptível a vulnerabilidade que essas ferramentas trouxeram para o nosso cotidiano de seus usuários. Conforme afirma Brito (2013),

A internet, a telemática e a informática, além de serem ferramentas de comodidade e consideradas poderosos fatores de desenvolvimento econômico, vulnerabilizaram um novo campo de exploração criminosa, em que crimes já conhecidos ganharam um novo meio de execução e o surgimento de novas condutas provocou o questionamento sobre a relevância de bens ainda não tutelados pelo direito penal (BRITO, 2013 p.09).

Os crimes cibernéticos, também conhecidos por crimes “virtuais”, “digitais”, “crimes de informática”, segundo os autores Jesus e Milagres (2016, p.9) “são fatos típicos e antijurídicos cometidos por meio da, ou contra a tecnologia informação, ou seja, um ato típico e antijurídico, cometido através da informática em geral”. Esses fatos não exigem dos usuários um grande conhecimento de informática, sendo somente necessária a utilização de um aparelho celular conectado à rede mundial de computadores para realizar uma grande operação criminosa. Sobretudo, tem-se crimes que levam tempo e necessitam de “profissionais do crime” com uma capacidade intelectual sobre o assunto para realizar alguns deles.

Ainda reforça Rocha (2017, p.13 apud AZEVEDO; CARDOSO, 2021, p. 5) “os crimes cibernéticos tratam-se de condutas ilícitas realizadas por algum tipo de dispositivo tecnológico [...], assim por entender que as condutas são dadas em ambientes virtuais”. Assim, entendemos que a conduta somente se realiza com o resultado.

Pelo princípio da legalidade do nosso ordenamento jurídico “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Ninguém pode ser

responsabilizado por fato que a lei desconsidera como de relevância penal” (JESUS; MILAGRES, 2016, p.12) o mesmo ressalta que,

Em 1998, em julgado que se tornou histórico, no HC 76.689/PB, relatado pelo Ministro Sepúlveda. Pertence, o Supremo Tribunal Federal já enfrentava um caso envolvendo pornografia infantil nas antigas BBS (Bulleting Board System/Internet). À época, poderia alguém já imaginar que haveria necessidade de lei específica para responder a tais delitos. Mas não! O Ministro deu aula ao explicar que nem todos os delitos cibernéticos necessitavam de nova tipificação, eis que em muitos a tecnologia era só um novo meio utilizado para concretização de delitos conhecidos (JESUS; MILAGRES, 2016, p 29).

Portanto, como são notáveis os crimes cibernéticos seriam somente crimes praticados através de novos meios, aqui referindo à tecnologia, de modo virtual fazendo uso da internet, e como esses crimes já existem no mundo real não eram necessária uma nova nomeação, podendo apenas ser identificados e explicados os locais de realização para aplicar a lei igual a se ocorressem no mundo real presencial.

EVOLUÇÃO LEGISLATIVA

O termo crimes cibernéticos surgiu pela primeira vez em uma reunião do G8 na França em 1990, onde foi discutida a prática de crimes cometidos através de aparelhos eletrônicos e a disseminação de informações pela internet, de acordo com Brito (2013),

O termo Cybercrime surgiu aproximadamente na década de 1990 em Lyon, na França, na reunião de um grupo das nações do G8 que discutia a prática de crimes através de aparelhos eletrônicos e a disseminação de informações pela internet. “Outra significativa participação do Brasil em acordos internacionais foi ratificada O Pacto Internacional de Direitos Civis e Políticos – 1992”, ficou

determinado que toda pessoa tenhamos a liberdade de procurar, receber e difundir informações e ideias de qualquer natureza independentemente de considerações de fronteiras, verbalmente ou por escrito, de forma impressa ou artística, ou por qualquer meio de sua escolha (BRITO, 2013, p. 25).

No Brasil os crimes cibernéticos foram integrados no nosso ordenamento jurídico pela Lei 12.737, ano de 2012, batizada de Lei Carolina Dieckmann, por se tratar de um caso de grande repercussão na mídia brasileira, o caso referido a atriz teve o seu computador pessoal invadido e seus arquivos pessoais roubados, causando a publicação de fotos íntimas na internet, por meio das redes sociais. A atriz vitimada abraçou a causa e cedeu seu nome à nova lei. Esta lei alterou o Código Penal Brasileiro tipificando a conduta criminalmente de invadir dispositivo de informática conectado ou não a internet:

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: § 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 (BRASIL, 2012, N.P)

Esses dispositivos trouxeram um grande avanço na legislação brasileira segundo Jesus e Milagres,

[...] 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 tramitam no Congresso Nacional (JESUS; MILAGRES, 2016, p. 49)

Porém com avanço na legislação posteriormente trouxe outras mudanças no Código Penal a atualização dos artigos 266 e 298 pela lei 12.737 de 2012, versam respectivamente sobre interrupção ou perturbação informático ou de informação de

utilidade de serviço telegráfico, telefônico informático, telemático de informação de utilidade pública e Falsificação de documento particular, para que em relação ao primeiro passasse a constar a conduta equiparada a tipo penal assim descrita, incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento e em relação ao segundo fosse equiparado o cartão de crédito e de débito ao documento particular mencionado no artigo (BRASIL, 2012).

Mesmo com avanços da lei 12.737 de 2012, a legislação existente no país, porém não existia uma regularização de formas de utilização da internet no Brasil, e o ciberespaço parecia uma “terra sem lei”. Surgiu assim a necessidade de uma legislação que normatize a instalação, funcionamento, uso, de futuras responsabilidades de provedores e usuários da rede mundial de computadores. Para Castells (2005, p. 27) “O que a sociedade em rede é atualmente não pode ser decidido fora da observação empírica da organização social e das práticas que dão corpo à lógica da rede”.

Lógica e comportamentos que muitas vezes vem causando danos a sociedade cada vez mais dependente da rede. Diante de uma lógica de comportamentos em rede e uma sociedade cada vez mais conectada vem aumentado substancialmente “crimes de internet” através de rede sociais, sendo as mais utilizadas “*Instagram*” e “*whatsapp*”, com a facilidade de se criar uma conta nos aplicativos citados e rapidez no envio e recebimentos de mensagens de texto, fotos, áudios e vídeos todos instantâneos, essa rapidez traz um dinamismo nos discursos de ódio, uma propagação imediata dos cibercrimes.

Surge neste contexto uma necessidade maior de criações de leis que normatizam serviços de instalação, fornecimento e distribuição da internet, como também os chame a responsabilidade de provedores e usuários na esfera civil e penal, quando danos causar a clientes e usuários, o Marco Civil da Internet veio com a proposta de sanar essa lacuna legislativa.

1.2 O MARCO CIVIL DA INTERNET

Mesmo com as mudanças surgidas no Artigo 154-A do Código Penal brasileiro com a Lei 12.737 de 12, ainda assim existiam lacunas em relação a utilização da internet no país, principalmente quando esta ferramenta passou ser utilizada para cometimentos de ilícitos penais e dificultando as investigações por não existir um responsável direto para fornecer informações sobre o *Internet Procotol* – Ips (protocolos de rede), conectados na rede, faltava assim uma norma que desencorajasse os criminosos utilizar a internet como ferramenta para expor vida de terceiros ou ludibriar os indivíduos para vantagens patrimonial.

Neste contexto, foi elaborado o Marco Civil da Internet Lei 12.965 de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil bem como diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios nesta matéria (BRASIL, 2014).

A partir desta lei provedores e usuário serão responsabilizados por crimes cometidos através desta ferramenta sendo necessários para isso a responsabilização, tanto penal como civil, que a partir da entrada da lei em vigência os dados de provedores e usuários, dos quais sejam solicitados pela justiça serão quebrados e deverão ser entregues às autoridades solicitantes somente com autorização judicial, para assim manter-se as garantias de segurança jurídica encontrada na Constituição Federal, que traz a internet como um direito fundamental de todas as pessoas e no artigo 7º da lei 12.965 de 23 de abril de 2014, mostra um rol de direitos:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - Inviolabilidade e sigilo do fluxo de suas comunicações pela internet,

salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; IV - Não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V - Manutenção da qualidade contratada da conexão à internet; VI - Informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade (BRASIL, 2014).

Mesmo que a lei garanta direitos de Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, esse direito deverá ser relativizado quando a rede mundial de computadores está sendo utilizada por pessoa má intencionada para cometer ilícitos penais, violando a vida privada ou utilizando o meio para ludibriar e retirar o patrimônio de Pessoas Físicas e causando prejuízos financeiros às pessoas Jurídicas. O artigo 19º da Lei 12.965 demonstra quando se aplica a responsabilidade civil pela violação da privacidade,

Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário (BRASIL, 2014).

Muitas vezes a violação da privacidade de terceiros é cometida pela confiança do falso anonimato dos indivíduos que utilizam o espaço virtual para cometer crimes achando que não irão ser responsabilizados, pelas dificuldades nas investigações.

Outra lei que veio a somar no âmbito jurídico brasileiro, foi a Lei nº 13.709/18 - Lei Gerais Proteção Dados Pessoais (LGPD), esta tem como principal objetivo proteger

a tutela de dados tanto de pessoas físicas como jurídicas, alterando também a lei 12.965/14.

No artigo 1º da lei 13.709 de 2014, da Lei Geral Proteção de Dados tem como objetivos “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2014, N.P) pessoa natural entende-se pessoa física com nome sobrenome, sexo, idade, produtos que pesquisa, tudo que pode individualizar uma pessoa, que a todo o momento está fornecendo informações através de aparelhos celulares conectados a rede de internet. Segundo Roque (2019),

> Os dados pessoais, na sociedade contemporânea, assumem importância estratégica cada vez maior. Podem ser utilizados em inúmeras aplicações, como o direcionamento de propagandas e anúncios específicos para o perfil de determinado consumidor, a partir das páginas que este visita na internet, ou a identificação da preferência ideológica ou mesmo sexual mediante análise dos gastos realizados pelo cartão de crédito, ou a investigação de doenças com maior probabilidade de se manifestarem durante a vida de determinado indivíduo, por meio da análise de seu material genético (ROQUE, 2019, p. 2).

Informações individuais colhidas de formas indiscriminadas e sem um tratamento adequado mesmo que sejam fornecidas pelos próprios usuários sem nenhum tratamento poderão como relatado anteriormente ser cruzadas com outras informações dos indivíduos em outro momento e de certa forma venham a ter problemas com esses dados fornecidos e que podem ser passados e discriminadas muitas vezes sem o consentimento do titular das informações. Assim, na sua análise Roque (2019):

> Diante de todos esses riscos significativos, que vão muito além da violação à privacidade, representando ameaça a diversos outros direitos da personalidade,

decorre a necessidade de controle na coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, armazenamento e eliminação dos dados pessoais, o que se busca no Brasil por meio da LGPD, que entrará em vigor em agosto de 2020 (ROQUE, 2019, p.3).

Mesmo diante do esforço legislativo dos nossos parlamentares, é visível na nossa sociedade contemporânea o aumento de crimes cometidos através de aplicativos conectado à internet principalmente crimes contra o patrimônio, a honra, as *fake News*, inclusive os crimes de ódio (cyberbully*)*.

CAPÍTULO II

2 TIPOS DE CRIMES CIBERNÉTICOS

A partir de agora iremos apresentar uma discussão sobre os principais crimes virtuais cometidos por usuários criminosos *hacker* utilizando a rede mundial de computadores. Aqui se fará necessário uma distinção nos conceitos de hackers. De acordo com Nunes e Madrid (2019, p. 5 apud PAESANI 2000, p. 22) existem dois tipos de *hackers*: o "ético e o não ético".

> [...] São especialistas, os denominados hackers éticos, que invadem sistemas, corrigem falhas de segurança e instalam uma porta única e controlada, com o propósito de garantir a exclusividade no acesso. Alguns arriscam falar sobre suas proezas, mas a maioria prefere a segurança do anonimato. Normalmente, um hacker entra num computador e sai sem ser percebido. Nem sempre está mal-intencionado, mas utiliza seus conhecimentos, para obter mais conhecimentos e avisa que ainda vai demorar muito até que as transações eletrônicas sejam totalmente seguras. Cita como exemplo uma companhia cujo site recebe pedidos por meio de uma conexão criptografada na Internet e então os envia para seu centro de processamento via e-mail. A primeira etapa é segura. A segunda, não. As mensagens eletrônicas corporativas são uma das primeiras coisas que um invasor procura. A maior preocupação do chamado hacker ético é com a implantação do sistema de segurança e sua tarefa é a de tentar invadir os sistemas das companhias com o objetivo de detectar os pontos vulneráveis à ação de outros hackers. Trabalha para gigantes do ramo dos computadores e para empresas que precisam defender informações confidenciais de seus clientes (NUNES, MADRID, 2019, p.5 *apud* PAESANI, 2000, p 22).

Conforme entendimento do autor os hackers éticos são técnicos especialistas em testar a vulnerabilidades da segurança de acesso de usuários e clientes, mantendo o sigilo das informações obtidas através desta prática de invasão, melhorando sistemas de acesso através de portas únicas evitando que pessoas mal intencionadas tenham acesso. Para autores hackers não éticos são:

O Hacker não ético: O hacker não ético (cracker) é o invasor destrutivo que tenta invadir na surdina os portões de entrada dos servidores Internet, que são a melhor forma de disseminar informações. É forçoso admitir que até o momento são os grandes vitoriosos nessa batalha informática. No Brasil, um exemplo de invasão agressiva ocorreu no dia 6 de junho de 1999, quando as páginas da Presidência na Internet foram invadidas por hackers e os textos com ataques ao governo também ocuparam o site do Supremo Tribunal Federal. No mesmo dia, houve uma tentativa frustrada de entrar no site da Secretaria da Receita Federal. Conforme comunicado do Computer Security Institute (CSI), os prejuízos financeiros atribuídos a crimes de computador podem ultrapassar US$ 10 bilhões por ano, em parte por causa da crescente expansão da Internet. Especialistas dizem que os crimes de computador ocorrem o tempo todo. A causa deve-se ao fato de os hackers terem desenvolvido programas automatizados que investigam os alvos a serem atingidos, como computadores conectados a uma rede pública, em busca de pontos vulneráveis. A proliferação de conexões de alta velocidade à Internet, por linhas telefônicas ou modems a cabo permanentemente conectados, aumentou muito o número de alvos disponíveis. Portanto, qualquer PC que não tenha um sistema de segurança, como o firewall, corretamente configurado será acessível a hackers sempre que o computador estiver ligado. O rápido desenvolvimento de novas tecnologias para a Internet também abre canais para o cibercrime, e é impossível para qualquer grupo corporativo de segurança manter-se atualizado em relação a essas mudanças, com possibilidade de até 75% dos servidores da Web se tornarem vulneráveis a ataques por hackers (NUNES; MADRID, 2019, p.5 *apud* PAESANI, 2000, p. 23).

Os hackers não éticos utilizam seus amplos conhecimentos de informática com o objetivo de causar mal aos usuários da rede, vender dados pessoais, expor imagens, causar prejuízos financeiros através de desvio de dinheiro, estelionatos, além de espalhar notícias falsas com objetivo de causar mal à sociedade. No tópico seguinte iremos tratar dos crimes mais cometidos por hacker no Brasil utilizando a rede mundial de computadores.

2.1 CRIMES DE MAIORES INCIDÊNCIAS CONTRA O PATRIMONIO NO PAÍS

Como os avanços tecnológicos e as comodidades fornecidas por ela, é muito comum os clientes utilizarem - se de aplicativos de bancos instalados no celular para realizar transações bancárias, além de parecer seguro. Segundo Jesus e Milagres (2016, p. 25), “pesquisas sempre revelaram que o Brasil está na rota dos crimes cibernéticos”.

De acordo com a Polícia Federal, em uma reportagem no ano de 2004, de cada dez hackers ativos no mundo, oito vivem no Brasil, a Federação de Bancos Brasileiros (FEBRABAN), durante os anos de 2020 e 2021, em período de pandemia os golpes financeiros cresceram 365%, isso demonstram o aumento desenfreados de crimes financeiros realizados por meio digitais.

Em um artigo publicado na revista Espacios por Scarpioni, et. al, (2016), afirmam que “Fraude na internet é um problema crescente. As vítimas deste crime muitas vezes experimentam um duplo golpe: além de perderem dinheiro, são psicologicamente afetadas”, por um sentimento de incapacidade diante da fraude, sem saber lidar a situação real, as vítimas destas fraudes sentem - se incapacitadas com um sentimento de vulnerabilidade, pois se tivesse tomando um pouco de precaução e as cautelas precisas não cairiam no golpe.

Esses criminosos realizam golpes com poucos investimentos financeiros e obtém grande retorno, conseguem aplicar vultosos valores com fraudes financeiras,

utilizando somente um computador e aparelhos celulares com chip pré-pagos. Segundo Mbaziira, Abozinadah e James (2015), às ocorrências de crimes organizados pela internet estão subindo porque os criminosos estão conseguindo grandes recompensas financeiras, com pequenos custos para cometer o crime.

No site da FEBRABAN (2021) existem campanhas de alerta para os golpes mais comuns contra o patrimônio, e como se proteger, o nome dado campanha publicitária consiste em “Pare&pense, pode ser golpe”, com a intenção de conscientização das pessoas a respeito da importância de refletir antes de determinadas propostas, duvidando de suas índoles e evitando assim cair em determinados golpe.

Primeiro alerta vai para o golpe da falsa central de atendimento, consiste O fraudador entra em contato com a vítima se passando por um falso funcionário do banco ou empresa com a qual ela tem um relacionamento ativo. Informa que sua conta foi invadida, clonada ou outro problema e, a partir daí, solicita os dados pessoais e financeiros da vítima.

O segundo falso motoboy, o golpe começa quando o cliente recebe uma ligação do golpista que se passa por funcionário do banco, dizendo que o cartão foi roubado. O falso funcionário solicita a senha e pede que o cartão seja cortado, mas que o chip não seja danificado. Em seguida, diz que o cartão será retirado na casa do cliente. O outro golpista aparece onde a vítima está e retira o cartão. Mesmo com o cartão cortado, o chip está intacto e os fraudadores podem utilizá-lo para fazer transações e roubar o dinheiro da vítima (SCARPIONI, et, al., 2016).

No golpe do falso leilão os golpistas criam sites falsos de leilão, anunciando todo tipo de produto por preços bem abaixo do mercado. Depois pedem transferências, depósitos e até dinheiro via Pix para assegurar a compra. Geralmente apelam para a urgência em fechar o negócio, dizendo que você pode perder os descontos. Mas nunca entregam as mercadorias pagas. Além disso, os fraudadores podem se aproveitar para roubar informações importantes como CPF e número de conta das vítimas;

O golpe do *WhatsApp* os golpistas descobrem o número do celular e o nome da vítima de quem pretendem clonar a conta de *WhatsApp*. Com essas informações em mãos, os criminosos tentam cadastrar o *WhatsApp* da vítima nos aparelhos deles. Para concluir a operação, é preciso inserir o código de segurança que o aplicativo envia por SMS sempre que é instalado em um novo dispositivo. Os fraudadores enviam uma mensagem pelo *Whatsapp* fingindo ser do Serviço de Atendimento ao Cliente do site de vendas ou da empresa em que a vítima tem cadastro (FREBANBAN, 2021).

Eles solicitam o código de segurança, que já foi enviado por SMS pelo aplicativo, afirmando se tratar de uma atualização, manutenção ou confirmação de cadastro. Com o código, os bandidos conseguem replicar a conta de WhatsApp em outro celular, tendo acesso a todo o histórico de conversas e contatos. A partir daí, os criminosos enviam mensagens para os contatos, passando-se pela pessoa, pedindo dinheiro emprestado.

O golpe da troca de Cartão consiste em os golpistas que trabalham como vendedores prestam atenção quando você digita sua senha na máquina de compra e depois trocam o cartão na hora de devolvê-la. Com seu cartão e senha, fazem compras usando o seu dinheiro. O mesmo pode acontecer com desconhecidos oferecendo ajuda no caixa eletrônico, Conforme o Cert (2012),

Os golpistas têm se intensificado a cada dia na exploração das fragilidades dos usuários, utilizando-se de técnicas de engenharia social com diferentes meios e discursos tentando enganar e persuadir as vítimas induzindo-as a fornecer informações sensíveis ou a realizarem ações, como acessar páginas falsas ou executar códigos maliciosos (CERT, 2012, p.5).

Se aproveitam de alguma dificuldade sua no terminal eletrônico para pegar rapidamente o seu cartão e depois devolver um que não é seu, ao mesmo tempo em que espiam sua senha. Cuidado com as Senhas, Golpistas só conseguem entrar em sua conta bancária usando sua senha e seus dados.

E eles podem conseguir essas informações de várias formas: fingindo ser um funcionário do banco, olhando você digitar a senha no caixa eletrônico, enviando falsos portadores ou durante uma compra presencial e até roubando seu celular para procurar senhas anotadas e os dados da sua conta ou cartão de crédito guardados em bloco de notas, arquivos ou em históricos de conversas no WhatsApp ou no e-mail.

E por último e não menos importante Golpe do link Falso, esse golpe em que normalmente ofertas muito atrativas chegam por e-mail ou redes sociais como iscas para que os usuários informem seus dados como número de CPF, conta cartões e senhas. Essas mensagens também podem instalar vírus e aplicativos que roubam seus dados por meio de links maliciosos, permitindo os golpistas acessarem todas as suas contas.

Além de explicar os golpes mais comuns e como evitar, a mesma página publicitária, faz uma alerta através de dicas de como se proteger desses oportunistas golpistas chamado de'' #10DICAS ANTI-GOLPES", cuidar de senhas, cartão, conferir cartão após uma compra, ativar duplo fator de autenticação, atenção com ligações, prestar atenção ao receber mensagens com sites, devendo nunca clicar em l*inks* desconhecido ou suspeitos, cuidado com compra online, cuidado operações bancárias, não fotografar ou filmar tela do caixa eletrônico usá-lo e cuidado com o que compartilha nas redes sociais.

São recomendações básicas, mas que dificultam que os criminosos façam usos de informações pessoais e bancárias de terceiros para ilícitos contra o patrimônio através de meios virtuais. Não podemos deixar de falar dos crimes de estelionatos, furtos, além dos crimes contra honra as "chamadas vinganças digitais", *fake News* que tem uma grande incidência no país.

2.2 AS FAKE NEWS NO AMBIENTE DIGITAL

Em ambientes digitais informações são propagadas com uma velocidade e intensidade muito grande, não conseguindo dimensionar a proporcionalidade deste ciberespaço. Essas informações muitas vezes inverídicas, não verdadeiras, são *fake* News, são capazes de tomar proporções imensuráveis causando prejuízos em diversas áreas como política, saúde, educação, principalmente psicológica e sensorial. Segundo O livro Educação digital e cibercidadania - prevenção de crimes cibernéticos, coordenado por Higor Vinicius Nogueira Jorge, assevera que,

As *fake news* costumam ser elaboradas como o emprego dos mesmos recursos psico-sensoriais inerentes à pós-verdade, tais sejam, emoção e crenças pessoais. Por via desses, os sujeitos passivos das feke News são levados a crer no conteúdo fictício que receberam e a divulgá-lo de maneira mecânica (JORGE, 2021, p.160).

Os sujeitos que recebem as informações toma aquilo como verdade, não busca checar as fontes se são coesas ou não e saem repassando sem nenhum critério de análise crítica. Causando muitas vezes as desinformações, levando os sujeitos a acreditarem em mentiras, principalmente virtuais que tem como função a "intensificar a fragilidade interpretativa humana no trato com informações virtuais" (JORGE, 2021, p. 160). Com a pouca cultura de pesquisar fontes confiáveis e falta de conhecimento para verificar o ambiente que surgiram as informações, podem ser identificadas como uma das causas dessa fragilidade interpretativa de informações, levando os usuários propagarem teorias falsas e danosas à sociedade.

Para Jorge (2021, p. 162) "À visão de mundo e as expectativas interiores de cada um dão às *fake* News o seu poder e intensidade e de forjar verdades aparentes", a vítima acredita veracidade da informação recebida por meio digital, pelo simples motivo de estar na rede mundial de computadores, acreditada como verdade pelo o recebedor. Portanto, viver na era digital está cada vez mais

conectado e basta um click, um *enter* para que tenha fotos, vídeo, principalmente sua opinião exposta na internet, necessitando de uma conscientização para que sejam evitados grandes prejuízos ao próximo.

CAPÍTULO III

3 DISCURSO DE ÓDIO NAS REDES SOCIAIS

Em uma sociedade cada vez mais conectada digitalmente a internet tanto produz como recebe informações a todo instante, os "internautas", usuários conectados à rede através de um aparelho informático, criam perfis *fakes* nas redes sociais, e através destes encontram-se no direito de dar a sua opinião em fotos, vídeos e postagem de outro usuário ou seguidores, muitas vezes com palavras agressivas, incitando a injúria racial ao racismo, homofobia, criando um ambiente de descriminação e ódio (TEFFÉ, 2017).

Esses seguidores expõem suas opiniões sem fazer nenhum senso de valor ou sem medir as consequências dessas palavras, causando em seus receptores danos irreparáveis, pois a internet é o meio mais rápido conhecido de propagação de informações. Segundo a autora Daniela Osvald Ramos Simpson define discurso de ódio como:

[...] um termo do estado da arte na teoria jurídica e política que é usado para se referir à conduta verbal – e outra ação simbólica e comunicativa – que voluntariamente expressa intensa antipatia em relação a algum grupo ou a um indivíduo com base na participação deste em algum grupo, e os grupos em questão são geralmente aqueles que se distinguem por etnia, religião ou orientação sexual. O discurso de ódio inclui abuso e assédio preconceituosos, certos usos de insultos e epítetos, algum discurso político e religioso extremista (por exemplo, declarações de que todos os muçulmanos são terroristas, ou que gays são seres humanos de segunda classe), e certas exibições de “símbolos de ódio’’ (RAMOS, 2019, p. 21).

A expressa e intensa antipatia em relação aos outros sujeitos, ou a um certo grupo social em especial, com base em uma etnia, religião, opção sexual, insultos preconceituosos que levam muitas vezes as pessoas cometerem atos contra suas próprias vidas, como o suicídio.

Para José Ruan Moreso o discurso de ódio se compõe dois elementos básicos: discriminação e externalidade (2011) a discriminação não externada não passaria de mero pensamento, não existe enquadramento jurisdicionas, bem como afirma em suas palavras Jeremy Waldron (2010, p. 1601 *apud* Moreso 2011, p. 3) “o problema se instaura quando o pensamento ultrapassa esses limites dando lugar à duradoura presença da palavra publicada”. A externalidade é a vontade do sujeito de expor suas opiniões agressivas, violentas.

É uma manifestação segregacionista baseada na dicotomia superior (emissor) e inferior (atingido) e, como manifestação que é, passa a existir quando é dada a conhecer por outrem que não o próprio autor. A fim de formar um conceito satisfatório, devem ser aprofundados esses dois a começando pela externalidade (MORESO, 2011, p. 3).

A necessidade que alguns sujeitos sentem de internalizam suas opiniões, de forma agressiva violenta e intencional nas redes sociais como *Instagram* e *Facebook*, muitas vezes utilizando de um perfil *fake*, causado a falsa impressão de anonimato, que não serão descobertos passam a propagar ofensas, discursos de ódio contra grupos ou pessoas específicas, como foram caso de injúria racial e de racismo propagado contra a jornalista da Rede Globo Maria Júlia Coutinho (Maju Coutinho), apresentadora do Jornal Hoje da Rede Globo em 2014. (RODRIGUES; LARA, 2020).

Os criminosos criaram perfis falsos e escreviam comentários racistas na página do Globo nas redes sociais: “Negros são uma raça maldita. Merecem morrer. Não era para ter acabado com escravidão Negra desgraças merecem o Chicote” (RIBEIRO; FERRARI, 2016). Dois homens foram condenados a seis anos de

reclusão e 30 dias-multa, e o segundo, cinco anos reclusão e 24 dias multas. Ambos cumprirão pena em regime semiaberto, mas ainda poderão recorrer da decisão.
Decisão proferida do TJSP (Tribunal de Justiça de São Paulo 5ª Vara Criminal da Capital, e publicada no dia 09/03/2020). Esse fato nos apresenta duas características importantes do poder de punir do estado, a demora no julgamento dos fatos de quase sete anos, e depois pena muito branda tratando-se dos regimes semiabertos e multas (RODRIGUES; LARA, 2020).

Verificamos que mesmo perante crime todos os arcabouços juntados pela investigação e comprovada pelo poder judiciário, as punições são todas em regimes semiabertos e abertos. Nenhum deles leva os criminosos à prisão, o que possivelmente não deixa as vítimas satisfeitas com essas penas, depois de sofrer violência gratuita (MONTE; MOURA; GUIMARÃES, 2021).

Um caso que nos faz refletir a respeito destas questões anteriormente mencionadas e como as pessoas que passam por esses problemas foi o ocorrido recentemente no estado da Paraíba, em que um jovem ao publicar em uma rede social vídeo com simples gesto de carinho com seu amigo por meio de brincadeiras, sofreu ataques extremos através de comentários em rede sociais, a ponto de que o mesmo não conseguiu superar a situação chegando a cometer suicídio (PORTAL G1, 2021).

O caso que repercutiu nacionalmente nas redes sociais, refere-se ao filho de uma cantora paraibana a Walkyria Santos, que ao receber comentários homofóbOicos em sua publicação sentiu-se muito incapaz, chegando a explicar o vídeo que era apenas brincadeira, sobretudo a grande repercussão, o mesmo se viu desnorteado com aquela situação, que infelizmente chegou a tirar a própria vida, o que demonstra total desespero com a situação na qual foi exposta.
Com isso, sua mãe expos o caso recomendando aos pais que observassem o que seus filhos e os comentários ofensivos que muitos deles recebem, para que não chegassem ao mesmo fim. Dessa forma, fica claro à proporção que o cyberbullyng pode exercer na vida de quem o sofre e tamanho sofrimento pode ocorrer na vida

não apenas da pessoa que está vivenciando, mas as consequências à vida de toda família, amigos e sociedade em geral que se identifica com a situação.

Em alusão ao filho da cantora surgiu o Projeto de Lei Lucas Santos, a mesma foi aprovada pela Assembleia Legislativa da Paraíba, no dia 10 de agosto de 2021, o projeto de lei nº 3057/2021o projeto cria o Dia Estadual de Combate ao Cyberbulling e monitoramento de ofensa na internet, propondo ações educativas em instituições para orientar e evitar práticas de violência na internet, ensinando as formas de agir diante de ataques virtuais (PORTAL G1, 2021).

Portanto, é de extrema importância que na atualidade exista leis voltadas as essas questões dos crimes cometidos na web, principalmente com punições mais rígidas, pois é perceptível a todos que as leis, normas jurídicas brasileiras são muito brandas em relação a punir crimes que ferem a dignidade das pessoas, seja de modo real que abranja um ambiente controlado, um espaço menor, ou na internet, ciberespaço impossível de medir as dimensões espaço e cada dia os tribunais vem se manifestando a favor das vítimas desses crimes, mesmo que ainda as penas aplicadas sejam ainda brandas por se tratar de um crime tão danosos para os sujeitos que sofrem gratuitamente a violência.

3.1 POSICIONAMENTOS JURISPRUDENCIAIS EM RELAÇÃO AOS CRIMES CONTRA HONRA

Aqui se faz necessário uma especificação entre injúria racial qualificada art.140 § 3 do Decreto Lei 2.848 de 1940, Código Penal Brasileiro, neste o crime se caracteriza se por,

Injuriar alguém, ofendendo lhe a dignidade ou o decoro: (...) § 3º se a injúria consiste na utilização de elementos referente à raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência." (BRASIL, 1940, N.P).

Portanto o sujeito tem a vontade de ofender a honra subjetiva de outras pessoas, o agente profere palavras de cunho racista somente direcionado a determinada vítima. O crime de racismo art. 20 da lei 7.716 de 1989: Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional (REDAÇÃO DADA PELA LEI Nº 9.459, de 15 -05-97).
Aqui se pretende atingir o bem jurídico tutelado, a cor, a religião, a etnia, ou procedência nacional, se comporta atingir um todo, não somente a certa pessoa, mas uma coletividade que se identifica culturalmente. Nos últimos anos os tribunais vêm se posicionando em relação a esses crimes, o Supremo Tribunal Federal (STF) no último dia 28 de outubro,

Entende que casos de injúria - onde a ofensa é direcionada a um indivíduo - podem sim ser enquadrados criminalmente como racismo ofensa direcionados ao coletivo e por isso, imprescritíveis pela Constituição, não havendo, portanto, prazo específico para o Estado punir o acusado (AGENCIA BRASIL, 2021, N.P).

A partir desta data todos os crimes de injúria racial passam a ser imprescritíveis como crime de racismo sem prazo determinado para o acusado ser punido pelo estado. Na última década os tribunais estão se manifestando de forma favorável às vítimas, condenando seus algozes da internet a penas consideradas brandas, que se levarem em conta toda a exposição vexatória que esses indivíduos tendem a sobre quando viram alvos de indivíduos inescrupulosos, não consegue ser comparado deixando marcas maiores do que com quem os cometeu, que pagará pelo crime, mas não carregará o fardo da situação e o medo de vivenciar novamente (COSTA, 2010).

Em uma sociedade cada vez mais conectada digitalmente a internet, em que todo momento está tanto produzido como recebendo informações os "internautas", usuários conectados através de um aparelho celular, tendo um perfil na rede social, encontram-se no direito de dar a sua opinião em fotos, vídeos e postagem de outros usuários ou seguidor do seu perfil, muitas das vezes sem medir as consequências

dessas palavras em um meio de propagação tão rápido como internet. Segundo a autora Daniela Osvald Ramos Simpson define discurso de ódio como:

Um termo do estado da arte na teoria jurídica e política que é usado para se referir à conduta verbal – e outra ação simbólica e comunicativa – que voluntariamente expressa intensa antipatia em relação a algum grupo ou a um indivíduo com base na participação deste em algum grupo, e os grupos em questão são geralmente aqueles que se distinguem por etnia, religião ou orientação sexual. O discurso de ódio inclui abuso e assédio preconceituosos, certos usos de insultos e epítetos, algum discurso político e religioso extremista (por exemplo, declarações de que todos os muçulmanos são terroristas, ou que gays são seres humanos de segunda classe), e certas exibições de “símbolos de ódio’’ (RAMOS, 2019, p. 21).

As expressões utilizadas em redes sociais que denigrem a imagem das pessoas ameaçam as mesmas, muitas vezes acarreta em problemas psicológicos de quem é submetido a esses discursos que menosprezam alguém pelo fato de ter opiniões divergente a de outras, ser de classe social menos favorecida financeiramente, religião diversas, entre outros pontos tão simples que infelizmente acabam sendo razões para sofrer ataques de ódio na rede.

Verificamos que mesmo perante crime perante todo o arcabouço juntado pela investigação e comprovada pelo poder judiciário, as punições são todas em regimes semiabertos e abertos. Nenhum deles leva os criminosos à prisão. Será que as vítimas estão satisfeitas com essa pena? Depois de sofrer violência gratuita? Portanto, é perceptível a todo que as leis as normas jurídicas brasileiras são muito brandas em relação a punir crimes que fere a dignidade das pessoas seja no mundo real ou virtual.

Devendo as autoridades buscar mecanismos cada vez mais eficazes para investigação como os meios de provas destes delitos cometidos por meio da internet (BRASIL, 2020).

3.2 AS DIVERSIDADES DE PROVAS DIGITAIS

No meio digital os vestígios, evidências que serão utilizadas como provas em um processo, podem ser diversas maneiras, vídeos, áudio, imagens, documentos, planilhas, textos etc, todos podendo ser retirados, manipulados e apagados permanentemente.

Este fato, exige das Autoridades uma agilidade nos tratos com essas informações, aqui surgi a primeira dificuldades em todas as investigações para qualquer acesso equipamentos guarde ou armazene informações, será necessário uma ordem judicial para acesso assevera Araújo (2018),

Nesse tipo de crime as evidências apresentam características diversas, possuindo diversos formatos, pois podem se tratar de imagens, vídeo, áudio, planilhas, documentos, sejam de forma isolada ou em conjunto. Essas evidências, por serem facilmente destruídas ou alteradas, devem ser de pronto preservadas. Elas estão misturadas a outros dados, obrigando os investigadores e técnicos a fazer uma análise mais apurada durante a sua obtenção (ARAÚJO, 2018.p. 101).

Faz-se necessário assim uma análise técnica para apurar a obtenção dessas evidências, sendo, portanto, submetidas ao contraditório legal para se tornarem provas em qualquer processo, levando a defesa contestar qualquer laudo apresentado pela investigação, assim como apontado na Cartilha Roteiro de Atuação Sobre crimes Cibernéticos (2013):

O exercício do contraditório possibilita que a defesa conteste a legitimidade dos procedimentos de investigação ou mesmo a consistência de um laudo pericial, tornando usual a necessidade de novas aquisições, análises e apresentação das informações durante o andamento do processo (ROTEIRO DE ATUAÇÃO MPF, 2013, p.166).

Cada documento, imagem, planilha vai exigir um tratamento individual para acesso aos dados exigindo uma capacitação e ferramentas para cada indício específico na investigação segundo Araújo (2018),

Na apuração desses crimes, cada área tem seus procedimentos específicos, por exemplo: análise dos dados registrados nos servidores; análise dos pacotes de dados contidos na transferência de informações dentro da rede; quanto à investigação relacionada a websites, é necessária a guarda de todos os seus componentes, e para isso existem programas específicos como: HTTrack, Express WebPictures, Grab-a-Site, Web bLooper e WebReaper (ARAÚJO,2018, p. 103).

Mesmo que os crimes cibernéticos deixam rastro, os criminosos tentam ficar ao máximo no anonimato utilizando-se de Software, para driblar as autoridades. Faz-se necessário ferramentas de inteligências e servidores capacitados para monitoramento rastreio e coletas de dados que por diversas vezes estão em provedores armazenados em outros países, e aí esbarramos em legislações diversas que dificultam a colaboração internacional a autoridades locais para conseguir os indiciamentos dos criminosos e punição devida ao mal causado.

CONSIDERAÇÕES FINAIS

A partir dos pontos abordados neste trabalho tornou-se possível identificar as inúmeras ações existentes que visam por melhorias em relação às penalidades aos crimes cometidos pela web. Sobretudo é importante que tenhamos consciência dos perigos que corremos, pois apesar de termos na atualidade uma facilidade imensa de resolver problemas que antigamente apenas eram tratados por meio presencial e agora podem ser resolvidos em cliques na web, como é o caso de pagamentos e transferências bancárias que tudo pode ser realizado através do aparelho celular com acesso a internet, sobretudo isso gera riscos com essa exposição, essas que são muito visadas atualmente.

Com a desenvolver dos estudos ficou aclarado informações que tínhamos coo objetivos de identificar o caso de como ocorre os crimes, e assim as leis que surgiram em alusão a crimes que antigamente eram cometidos apenas no meio presencial real e que agora é realizado através do digital, assim conseguimos apresentar satisfatoriamente informações relevantes a respeito desta temática que merece destaque, já que a cada dia o crescimento do mesmo é maior.

Dessa forma, foi um desafio encontrar informações seguras sobre as leis os processos para que compreender a grandeza desses crimes e as consequências na sociedade em geral, assim como também estão se voltando leis rígidas na área, pois é observado que os criminosos agem de uma forma tão peculiar que dificulta ainda mais o processo de investigação dos atos, mas sim a dificuldade do judiciário de punir, começando pela proteção constitucional dos direitos fundamentais a investigação para identificar a materialidade e a autoria como ocorre muitas vezes em casos de espionagem, material pornográfico envolvendo pessoas famosas e informações privadas de agentes governamentais, comprovando assim que qualquer pessoa pode passar por essa situação incômoda.

Um ponto importante que merece nossa atenção é que ao contrário do que muitas pessoas imaginam existe leis especializadas para assegurar os direitos dos usuários, mas devido o ordenamento jurídico brasileiro mesmo que não vincular a palavra internet aos crimes, não ficam impunes utilizando de outras denominações.

A diversidade de crimes existentes no mundo digital é inúmera e além de crimes temos o cyberbullyng que na atualidade vem sendo alvo de muitas discussões, pois se trata de uma prática de comentários maldosos nas publicações alheias que como citado em exemplo no trabalho gera um desconforto imenso causando desequilíbrios emocionais podendo levar a prática do desespero e até mesmo suicídio como no caso citado no desenvolvimento.

REFERÊNCIAS

AGENCIA BRASIL, **STF decide que crime de injúria racial não prescreve.** Revista Isto é dinheiro. Edição Nº 1251. Disponível em: https://www.istoedinheiro.com.br/stf-decide-que-crime-de-injuria-racial-nao-prescreve/. Acesso em: 03 de nov. 2021.

BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**, Editora Jus Podivm, 2020. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2020;001163495 . Acesso em 21 nov. 2021.

BRASIL. Tribunal Regional Federal da 3ª Região. **Escola de Magistrados Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017.

BOCCATO, V. R. C. Metodologia da pesquisa bibliográfica na área odontológica e o artigo científico como forma de comunicação. Rev. Odontol. Univ. Cidade São Paulo, São Paulo, v. 18, n. 3, p. 265-274, 2006.

COMISSÃO EUROPEIA. **Combater a desinformação em linha**: uma estratégia europeia. Comunicação da Comissão ao parlamento europeu, ao conselho, ao comité económico e social europeu e ao comité das regiões. Bruxelas, 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0236. Acesso em: 24 out. 2021.

COSTA; Cleber Lazaro Julião. Crimes de racismo analisados nos tribunais brasileiros: o que as características das partes e os interesses corporativos da

magistratura podem dizer sobre o resultado desses processos. Revista de Estudos Empíricos em Direito v. 6, 2019. Disponível em: https://reedrevista.org/reed/article/view/409. Acesso em 11 de out. 2021.

DELMAZO, Caroline; VALENTE, Jonas CL**. Fake news nas redes sociais online**: propagação e reações à desinformação em busca de cliques. Media & Jornalismo, v. 18, n. 32, 2018.

FREBANBAN. **Pare&pense, pode ser golpe.** FREBANBAN – Federação Brasileira de Bancos. São Paulo, 2021. Disponível em: https://antifraudes.febraban.org.br/?gclid=Cj0KCQiAnaeNBhCUARIsABEee8WF30PydeyY18dBa08afIA77IeOlgInSqkhjnr-bk4rS19uq58gmj4aAqkeEALw_wcB#golpes-comuns. Acesso em: 30 nov. 2021.

FERNANDES; Ricardo Vieira De Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gamba Prata de. **TECNOLOGIA JURÍDICA E DIREITO DIGITAL I**. Congresso Internacional De Direito E Tecnologia. Belo Horizonte, 2017.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. (Orgs.). **Métodos de pesquisa**. Porto Alegre: Editora da UFRGS, 2009.

JORGE, Higor Vinicius Nogueira. **Manual da educação Digital e Cibercidadania**: Um guia para jovens, adultos instituições, empresas e autoridades. Editora JusPodivm, São Paulo, 2021.

MONTE, Franciela Felix de carvalho; MOURA, Maria Aline Rodrigues de; GUIMARÃES, Pâmela Rocha Bagano. **Efeitos do discurso de ódio sobre o desenvolvimento sociomoral:** ensaio teórico. REVASF, Petrolina. Brasil, vol. 11, n.25, 2021 ISSN: 2177-8183

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

PORTAL G1, Após morte do filho, Walkyria Santos encampa luta para criação de lei que torna crime comentários de ódio na internet. Portal G1, Rio Grande do Norte, 2021.

RIBEIRO, Aline; FERRARI, Bruno. **No submundo das gangues virtuais**. Revista ÉPOCA, 2016. Disponível em: https://epoca.oglobo.globo.com/vida/experiencias-digitais/noticia/2016/01/no-submundo-das-gangues-virtuais.html. Acesso em: 23 de nov. 2021.

ROCHA, Fernando Antônio Nogueira Galvão da. **Criminalidade do Computador**. Revista Jurídica do Ministério Público, Belo Horizonte, a. 27, v. 19, p. 75-98, 1996.

RODRIGUES, Rodrigo; LARA, Walace. Justiça condena dois homens por racismo e injúria racial contra a jornalista Maju Coutinho. G1, São Paulo, 2020. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/03/09/tj-de-sp-condena-dois-homens-por-racismo-e-injuria-racial-contra-a-jornalista-maju-coutinho.ghtml, acessado 12 de nov. 2021.

ROQUE, A. (2019). A tutela coletiva dos dados pessoais na lei geral de proteção de dados pessoais (LGPD). *Revista Eletrônica de Direito Processual*, *20*(2). Disponível em:
https://antifraudes.febraban.org.br/#golpes-comuns. Acesso em 24 de out. 2021.

ROTEIRO DE ATUAÇÃO: **Crimes Cibernéticos.** 2. ed. rev. - Brasília: MPF/2aCCR, 2013.

RUARO, R. L; RODRIGUEZ, D. P.; FINGER, B. **O direito à proteção de dados pessoais e a privacidade**. Revista da Faculdade de Direito UFPR, 53. 2011.

SCARPIONI; Agesandro; BONINI, Luci Mendes de Melo; BISPO, Roberto Marins Ferreira; PADLIPSKAS, Salvio; JÚNIOR, Luiz Teruo Kawamoto. **Desenvolvimento de ambiente virtual para treinamento de idosos para evitar golpes pela Internet.** Revista Espacio. Vol. 37, 2016. Disponível em: https://www.revistaespacios.com/a16v37n09/16370913.html. Acesso em 20 de nov. 2021.

TEFFÉ, C. S; MORAES, M. C. B. **Redes sociais virtuais:** privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. *Pensar-Revista de Ciências Jurídicas*, 2017.

TOMAS, Evicius Eduardo. **Marco Civil da Internet:** uma lei sem conteúdo normativo. Estudos Avançados, v. 30, 2016.