

**FAMIG- FACULDADE MINAS GERAIS**

**LORRAN VINICIUS SANTOS DA CRUZ**

**PERFIL DOS CRIMES VIRTUAIS NO BRASIL**

Belo Horizonte  
2021

**LORRAN VINICIUS SANTOS DA CRUZ**

**PERFIL DOS CRIMES VIRTUAIS NO BRASIL**

Monografia apresentada à disciplina  
Trabalho de Conclusão da Faculdade  
Minas Gerais.

Orientadora: Camila Soares

**LORRAN VINICIUS SANTOS DA CRUZ**

**PERFIL DOS CRIMES VIRTUAIS NO BRASIL**

Monografia apresentada a Famig –  
Faculdade de Minas Gerais, como  
requisito parcial para obtenção do título  
de Bacharel em Direito.

**BANCA EXAMINADORA**

---

Professora Camila Soares  
Orientadora  
Famig–Faculdade Minas Gerais

---

Prof. Ms.  
Membro Famig–Faculdade Minas Gerais

---

Prof. Ms.  
Membro Famig-Faculdade Minas Gerais

Belo Horizonte, xx de xx de 2021

## RESUMO

Os crimes virtuais são crimes realizados por um dispositivo tecnológicos, dispositivos que fazem parte do cotidiano da população brasileira e que desempenha um papel importante na comunicação entre os indivíduos, as más condutas representam um problema social e legislativo de acordo com o aumento dos números de delitos virtuais. Em vista dessa problemática ocorreu o desenvolvimento dessa pesquisa, que tem como objetivo de identificar os crimes virtuais, avaliar políticas públicas desenvolvidas para combater os crimes e investigar as medidas de prevenção utilizadas pelos usuários do ambiente virtual. Aplicando um levantamento de dados por meio dos bancos DFNDR lab- Laboratório de Cibersegurança da PSafe, SAFERNET- Centro de Apoio Operacional das Promotorias da Criança e do Adolescente. e ANATEL- Agência Nacional de Telecomunicações, nos períodos de janeiro a dezembro do ano de 2006 a 2014 e no ano de 2018, de número e tipos de crimes virtuais, apurando a legislação presente e aplicada das seguintes punições e enriquecendo os resultados obtidos com revisões bibliográficas acerca do tema de estudo. Ao analisar os bancos de dados é notável o crescimento de novos crimes virtuais, como surgimento de propagandas enganosas, premiações falsas, cópias de aplicativos reais que realizam anúncios falsos, empréstimos e consócios, com os aparecimentos de novos delitos faz-se necessário a aplicação de punições mais severas, o desenvolvimento de e aprovações de leis e prevenção para o combate dos crimes virtuais.

**Palavras chaves:** Internet; Dispositivos tecnológicos; Crimes virtuais; Legislação; Informática.

## ABSTRACT

Virtual crimes are crimes carried out by a technological device, devices that are part of the daily life of the Brazilian population and that play an important role in the communication between individuals, misconduct represents a social and legislative problem according to the increase in the number of crimes virtual. In view of this problem, this research was developed, which aims to identify virtual crimes, evaluate public policies developed to combat crimes and investigate the preventive measures used by users of the virtual environment. Applying a data survey through the banks DFNDR lab- PSafe Cybersecurity Laboratory, SAFERNET- Operational Support Center for the Child and Adolescent Public Prosecutor's Office. and ANATEL- National Telecommunications Agency, in the periods from January to December 2006 to 2014 and 2018, of the number and types of virtual crimes, investigating the present and applied legislation of the following punishments and enriching the results obtained with bibliographic reviews on the subject of study. When analyzing the databases, the growth of new virtual crimes is notable, such as the appearance of misleading advertisements, false awards, copies of real applications that carry out false ads, loans and consortiums, with the appearance of new crimes it is necessary to apply stricter punishments, the development of and enactment of laws and prevention to combat cybercrime.

**Keywords:** Internet; Technological devices; Virtual crimes; Legislation; Computing

## SUMÁRIO

<b>1-INTRODUÇÃO.....</b>	<b>7</b>
<b>2-SURGIMENTO DA INTERNET E EVOLUÇÃO.....</b>	<b>10</b>
2.1- Internet no Brasil: índice de uso da tecnologia.....	11
2.2- Redes Sociais: um ambiente virtual usado para práticas de delitos.....	12
2.3- Aumento dos números de crimes virtuais no Brasil.....	13
2.4. Amparos das vítimas de crimes virtuais.....	14
<b>3-OS CRIMES CIBERNÉTICOS NO BRASIL.....</b>	<b>17</b>
3.1- Identificação e classificação dos tipos de crimes virtuais que sucedem no Brasil.....	17
3.2- Avaliação das leis que assegura as das vítimas de crimes virtuais no Brasil.....	20
3.3- Levantamento de dados no banco DFNDR lab., SAFERNET e ANATEL.....	25
3.3.1- Construção de gráficos e histogramas.....	27
<b>4-CENÁRIO ATUAL BRASILEIRO E PERSPECTIVAS DE MUDANÇAS.....</b>	<b>29</b>
4.1-Análise dos dados levantados de crimes virtuais.....	29
4.2- Análise dos números de denúncias de crimes virtuais no Brasil por meios dos gráficos.....	30
4.3- Levantamento de dados dos novos crimes virtuais no Brasil.....	32
4.4-Comparação do número de denúncias de crimes virtuais no mundo.....	34
4.5- Avaliação da legislação vigente de crimes virtuais no Brasil.....	35
4.6- Avaliação dos novos dispositivos legais de crimes virtuais no Brasil.....	37
<b>5-CONCLUSÃO.....</b>	<b>40</b>
<b>REFERÊNCIAS.....</b>	<b>42</b>

## 1- INTRODUÇÃO

A internet é considerada uma ferramenta essencial para a manutenção das estruturas sociais, proporcionando uma aproximação entre as pessoas de países diversos, armazenando e processando os dados com grande precisão e velocidade. Diante do cenário de muitas transformações tecnológicas, o desenvolvimento de mídias sociais se tornou uma febre que causa um grande impacto nas relações entre as pessoas e nas relações jurídicas.

As relações mantidas no ambiente virtual, também deve acatar os princípios constitucionais, em especial o princípio fundador do Estado Democrático de Direito Brasileiro e a dignidade da pessoa humana, assim como as demais, visando colocar os interesses existências como a principal prioridade.

A potencialidade global que a internet proporciona e a ausência de um único domínio sobre a plataforma, desperta uma visão mais crítica sobre os impactos que o mundo virtual trás para a vida dos seus usuários. Analisando essa vertente é evidente o conflito que existe na afirmação de que a internet é um meio livre e que existe a irrestrita circulação de informações, aonde pode a censura será vedada.

Por conta desses fatores o presente estudo se faz necessário, pois é um tema pouco discutido e explorado pela doutrina, mas que tem ganhando grande importância, por conta do aumento de denúncias de crimes que são cometidos em ambiente virtual, evidenciando que o Poder Judiciário deve se posicionar sobre essas práticas delituosas, pois os crimes práticos no ambiente virtual se diferem dos crimes considerados como convencionais. O Direito muitas vezes não consegue acompanhar as mudanças que ocorrem na sociedade, tendo em vista a necessidade de criar e alterar as normas do Poder Legislativo.

Para a realização desse trabalho a análise da legislação vigente e os projetos de leis existentes e a criação de novos projetos voltados para o amparo das vítimas de crimes virtuais, uma vez que não existe uma legislação específica. Foram realizadas pesquisas bibliográficas referentes ao tema, da mesma forma

com a doutrina, jurisprudência e as normas do sistema jurídico brasileiro, com o objetivo de construir uma base sólida do método indutivo e dedutivo.

Portanto os objetivos desse estudo é analisar os fenômenos da globalização, as inovações tecnológicas, identificar os tipos de crimes virtuais, leis que assegurem as vítimas de crimes virtuais e medidas de políticas públicas para a prevenção desses crimes e de como utilizar essa ferramenta de comunicação de maneira segura, através do desenvolvimento de uma pesquisa de método qualitativo e descritivo, analisando dessa forma os dados dos crimes virtuais por intermédio do banco de dados do laboratório especializado em crimes virtuais DFNDR lab- Laboratório de Cibersegurança da PSafe, SAFERNET- Centro de Apoio Operacional das Promotorias da Criança e do Adolescente. e ANATEL- Agência Nacional de Telecomunicações, nos períodos de janeiro a dezembro de 2006 a 2014 e 2018, pois a comunicação ainda é uma peça importante nesse processo, ademais comunicar-se de forma segura nunca foi tão importante para os usuários da internet.

O primeiro capítulo aborda como a tecnologia possui grande influência na sociedade e como ela é importante, como uma ferramenta de comunicação, tendo em vista que a comunicação sempre foi essencial para a humanidade e apresenta como o avanço da tecnologia otimiza e facilita a comunicação. O capítulo também retrata o processo de invenção da internet e dos dispositivos eletrônicos que fazem a ponta direta para a comunicação e transmissão de dados, com maior rapidez, o que diferencia esta ferramenta de comunicação das demais existentes.

O segundo capítulo aborda o aumento dos números de delitos no ambiente virtual e aponta com maior magnitude as práticas mais recorrentes, que já possuem uma tipificação no ordenamento jurídico brasileiro, além de expor a estrutura de amparo recebida pelas vítimas de crimes praticados no ambiente virtual, que sentem que os seus direitos não são assegurados pelo ordenamento jurídico brasileiro, pois ao realizar as denúncias dos crimes cometidos, o processo não tem um andamento, pois os criminosos não são identificados, sendo assim não há como punir a prática realizada, elucidando o problema central abordado pelo trabalho, que aponta o aumento dos crimes nos ambientes virtuais, as novas

modalidades de crimes, a tipificação dessas novas modalidades e a falta de amparo das vítimas de crimes virtuais. Posteriormente no mesmo capítulo é abordado as legislações específicas, como a Lei nº 12.737/2012, conhecida também como Lei Carolina Dieckman, que realizou algumas alterações no Código Penal Brasileiro, devido ao vazamento das suas fotos íntimas nas redes sociais e o Marco Civil na Internet, também conhecido pela Lei nº 12.965/14.

O terceiro capítulo elucida como está o cenário atual brasileiro em se tratando de crimes virtuais e como estes crimes acarretaram muitas mudanças na sociedade e no comportamento dos usuários da internet. Ao realizar o levantamento de dados dos crimes praticados no Brasil e no mundo, foram identificadas as seguintes modalidades já tipificadas, como, o racismo, preconceito, homofobia, pornografia infantil, apologia e incitação a crimes contra a vida e intolerância religiosa. Foram identificadas novas modalidades de crimes, como propagandas falsas, anúncios e premiações falsas, empréstimos e consórcios que fazem a população brasileira refém desses golpes diariamente. Em seguida é realizada uma comparação desses crimes em âmbito mundial, apontando quais são os países que possuem maiores números de denúncias de acordo com o tipo de crime descrito, posteriormente serão analisadas a legislação vigente de crimes virtuais no Brasil e a criação de novos dispositivos, com objetivo de reconhecer e tipificar as novas modalidades de crimes realizados no ambiente virtual.

## 2- SURGIMENTO DA INTERNET E EVOLUÇÃO

A internet é um sistema que envolve a conexão de uma rede de computadores de proporções mundiais, abrangendo mais de 150 países e reunindo cerca de 300 milhões de computadores, sendo mais de 400 milhões de usuários conectados (DIZARD, 2000, p. 24). Seja computadores individuais e pessoais ou em um sistema de redes em um escritório, eles se conectam a um provedor de acesso, que se ligam as redes regionais, que se ligam as nacionais que por sua vez se ligam as internacionais, esses provedores estão dispostos nos aparelhos conhecidos como roteadores, que são instalados para captar dos sinais das redes, que se encarregam na rota adequada.

A internet surgiu em meados de 1960, como ferramenta de comunicação entre os militares durante a guerra e que seria possível resistir a um conflito nuclear mundial. O Departamento de Defesa dos Estados Unidos reuniu um grupo de engenheiros eletrônicos e de programadores para desenvolverem uma rede sem controle central por onde as mensagens enviadas e recebidas eram fragmentadas e que recebeu o nome de pacotes, dessa forma as informações eram transmitidas com rapidez e sem erros para uma rede onde cada computador seria apenas um ponto que mesmo impossibilitados de funcionar, ele não interromperia a transmissão das informações passadas nas mensagens.

Em 1969, a parceria entre a Universidade da Califórnia e o centro de pesquisa de Stanford, desenvolveu uma operação que recebeu o nome de ARPAnet (Advanced Research Projects Agency Network), que começou conectando uma rede de quatro computadores e em seguida conectou em todos os computadores de outras universidades, formando um centro de pesquisa com objetivo de auxiliar os militares e indústrias bélicas.

Em 1980, surgiu o TCP/IP (Transmission Control Protocol/Internet Protocolii) como um protocolo para a realização das trocas de informações pela ARPAnet, que possibilitou a conexão entre redes diferentes e em grandes distâncias. Em 1990, ocorreu a transformação da ARPAnet em NSFnet (National Science Foundation's Network), que permitiu a conexão entre as redes fora dos

Estados Unidos, sendo assim ocasionando o surgimento da internet que começou a ser utilizada como ferramenta entre o meio acadêmico e para troca de informações entre os usuários.

Em 1995 por conta do aumento do número de usuários a internet foi transferida para a administração de empresas não governamentais, que se encarregaram de estabelecer padrões de infraestrutura, registros e conexão. As instituições nos Estados Unidos são conhecidas como Internet Society, que atua em todo o mundo, mas no Brasil a instituição tem o nome de Comitê Gestor da Internet.

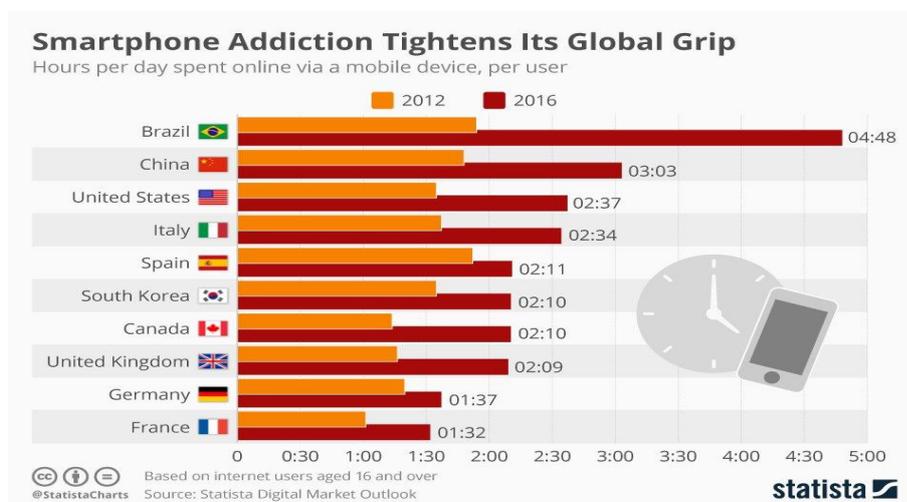
### **2.1- Internet no Brasil: índice de uso da tecnologia**

A chegada da internet no Brasil foi em 1995, através do governo federal com o objetivo de implantar a infraestrutura através de empresas privadas que fornecerá os serviços para os usuários que possuem interesse em ter a tecnologia como ferramenta de trabalho e troca de informações.

A internet é um avanço para a humanidade, além de possibilitar as relações interpessoais independente do espaço em que as os indivíduos se encontram, e só é possível por conta do ambiente virtual ou ciberespaço. Não é um espaço físico, real e concreto, é um ambiente criado especificamente para troca de informações, é um ambiente fácil e ágil (LEONARDI, 2005, p. 30.).

Desde então, o crescimento de usuários na internet no Brasil é estarrecedor, o (gráfico) é um demonstrativo no qual aponta que o Brasil em comparação aos países da China, Estados Unidos, Itália, Espanha, Coreia, Canadá, Alemanha e França, nos anos de 2012 e 2016 é o país que mais acessa e o que passa mais tempo na internet pelo smartphone (STATISTA, 2017, *online*).

**Gráfico 1-** Comparativo do tempo de uso de smartphone nos respectivos países



**Fonte:** Statista, 2017 (*online*)

## 2.2- Redes sociais: um ambiente virtual usado para práticas de delitos

Com a intensificação, a ampliação da internet e a globalização, a comunicação entre as pessoas aumentou gradualmente, impactando a vidas social e intelectual dos usuários através das trocas de informações.

Desta forma as tecnologias da informação desempenham um papel muito importante na sociedade da informação, pois trazem uma nova forma de comunicação, liberdade de expressão, trocas de informações, trocam de experiências culturais, como comidas, roupas e costumes, o que reflete na realidade jurídica da população. (FIORILLO, 2016, p. 30-40).

Diversos usuários desfrutam a ferramenta como benefício, e pela facilidade de comunicação com os demais usuários do mundo todo, a disseminação de informações e o compartilhamento de fotos, textos, vídeos e posicionamentos diante dos fatos ocorridos pelo mundo realizados em poucos segundos pelas redes sociais, como Facebook, Instagram, Whatsapp, Google, Youtube, Blogs, torna o ambiente da internet um local desagradável (MARTELETO, 2001, p.71-81).

Todavia esse espaço possibilita a criação de outros ambientes virtuais, e com isso surgiram diversos problemas originados da má utilização dessa ferramenta que permite o anonimato dos criadores, essa problemática se chama crimes virtuais ou cyber crimes, são crimes praticados por meio da internet. Crespo (2011, p.82) e Ferreira (2011, p. 55) classificam os delitos pelos seguintes meios: 1) crimes informáticos próprios, sendo um conjunto de ações realizado contra o sistema de informática utilizando o conhecimento de informática; 2) crimes informáticos impróprios, sendo tipificados os seguintes delitos, falsificação de documentos, violação de segredo, espionagem industrial, violação de serviços de utilidade pública, inserção de dados falsos em sistema de informações, estelionato, crimes contra a honra, pornografia infantil, ameaça, induzimento a suicídio, apologia de crime e racismo.

Com tudo muitos usuários utilizam as redes sociais para denegrir a imagem de outros usuários, compartilhando fotos íntimas, proferindo ofensas morais, interceptando comunicações, modificando dados, infligindo os direitos de autores, incitando ódio e discriminação, realizando chacota religiosa, transmitindo pornografia infantil, incitando terrorismo, entre outras formas, o que tem gerado vários casos na justiça, tornando o ambiente virtual um local para práticas de pequenos delitos, pois muitos usuários acessam a internet de forma anônima e com o auxílio de softwares, os mesmos inativam o IP dos dispositivos, o que dificulta o rastreamento dos criminosos (PINHEIRO, 2010 p. 297).

Sendo assim, os crimes virtuais tem apavorado a população que mesmo observando o avanço tecnológico da segurança pública, ainda não conseguem rastrear os criminosos, desta forma os criminosos saem impunes e as vítimas traumatizadas e muitas vezes sem suporte psicológico adequado, o que contribui para o aumento das inseguranças, crises de pânico, crise de ansiedade e até mesmo depressão.

### **2.3- Aumento dos números de crimes virtuais no Brasil**

Os delitos praticados na internet têm crescido exorbitantemente no Brasil, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

(Cert.BR), apontou um crescimento de cerca de 197% de crimes virtuais no ano de 2015, em 2014 a empresa mais prestigiada no mercado de TI, a Kaspersky Lab, efetuou o bloqueio de cerca de 6 bilhões de sites, computadores e smartphones denunciados por praticarem crimes virtuais.

O (gráfico 2) indica o crescimento de crimes praticados em ambiente virtuais entre os anos de 1999 e 2014, a tendência do aumento desses delitos se dá em consequência do tempo em que a população passa na internet, visto que os dispositivos fazem parte do cotidiano dos mesmos e desempenham um papel importante nas trocas de informações entre os usuários.

**Gráfico 2-** Qualitativo de crimes virtuais reportados ao Cert.BR entre os anos de 1999 a 2014



Fonte: 4SEC, 2015

## 2.4- Amparos das vítimas de crimes virtuais

Os crimes virtuais, são crimes praticados por meio da internet e na ausência de uma legislação específica, os infratores são julgados de acordo com Código Penal Brasileiro, pois o Brasil é um dos países que não possui uma legislação definida para julgar os crimes virtuais. E por conta do aumentos do números de ocorrências de crimes na internet, fez-se necessário a criação de algumas leis para punir os criminosos e resguardarem as vítimas, a Lei nº 12.737/2012 alterou o Código Penal Brasileiro, devido ao compartilhamento de fotos íntimas das atriz Carolina Dieckmann, as fotos foram divulgadas sem o conhecimento da atriz que procurou as autoridades da segurança pública para que pudessem identificar e

punir os autores, e removerem de todas as plataformas as fotos compartilhadas (BRASIL, 2012).

A tipificação dos delitos cometidos em ambientes virtuais é importante para as vítimas e nas prevenções de possíveis delitos, pois não promovem a impunidade para os praticantes e desmistificam a ideia de que a internet é um local onde os usuários não podem ser identificados e podem agir da forma que lhes convém e que lhes deixem confortáveis para realizar as demais práticas delituosas.

Conforme o artigo 154-A:

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena- detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL, 2012).

O Marco Civil na Internet, também conhecido pela Lei nº 12.965/14, que prevê as condutas para a utilização da internet, de acordo com o Art. 1º:

A Lei de nº 12.965/14 “estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria” (BRASIL, 2014).

As demais condutas são relacionadas a liberdade de expressão, proteção da privacidade e garantia de neutralidade da rede. Em vigor, a regra dispõe a garantia da privacidade dos usuários individuais e das empresas, as informações que são fornecidas para estas não poderão ser compartilhadas para terceiros, assegurando os dados e informações sigilosas, tornando possível a retirada de conteúdo divulgados que viole a privacidade dos demais. O Marco Civil da Internet sucedeu a obrigatoriedade dos registros de conexão dos usuários, que são salvos pelos provedores de acesso pelo período de um ano, sob total sigilo e em software seguro. Essas informações dizem respeito ao endereço de IP, com a data e hora inicial e final da conexão, garantindo a localização exata dos dispositivos e os seus respectivos donos (BRASIL, 2014).

A Polícia Civil do Distrito Federal desenvolveu diversas cartilhas com o objetivo de informar a população sobre os crimes virtuais de forma que o uso da internet e a navegação nas redes sociais seja consciente. As cartilhas preventivas são entregues nas ruas por Policiais Militares e disponibilizadas nos sites da Polícia Militar e Civil. A cartilha alerta os usuários sobre os delitos cometidos por estelionatários, como, propagandas enganosas, premiações falsas, cópias de aplicativos reais que realizam anúncios falsos, empréstimos, consócios, compartilhamento de fotos, vídeos sem a autorização dos proprietários, xingamentos e ofensas. Diante disso as vítimas recebem as devidas orientações cabíveis para denunciar as práticas cometidas pelos criminosos para que o poder Judiciário possa punir os indivíduos de forma justa e que a vítima seja reparada, acolhida e amparada.

### **3- OS CRIMES CIBERNÉTICOS NO BRASIL**

#### **3.1- Identificação e classificação dos tipos de crimes virtuais que sucedem no Brasil**

A nova sociedade informacional é movida pelo modelo cultural conhecido como a cibercultura, que tem como definição a cultura no qual a internet assume o papel de grande relevância na vida da população e nas relações sociais, dentro desse contexto da cibercultura, surge uma nova modalidade de crime, conhecido como crimes cibernéticos, mas que é conceituado pela doutrina como delitos de informática, crimes virtuais ou crimes digitais. Os crimes virtuais desafiam o direito, pois essa infração penal está na ordem do dia a dia e que ainda é uma novidade para o ordenamento jurídico, que vem encontrando dificuldades para combater esses crimes.

Os crimes virtuais podem ser tipificados em diversas condutas, como a calúnia, difamação, injúria, fraude, estelionato e até mesmo racismo. Apesar de serem classificados como crimes hodiernos, até então não existia uma legislação específica para a punição desses crimes, fazendo-se necessário a criação de novas leis e a utilização do ordenamento jurídico já existente.

Discute-se com frequência entre muitos pesquisadores a classificação dos delitos cometidos no ambiente virtual. Muitos classificam os delitos de acordo com as condutas exercidas pelos criminosos, podendo ser divididos entre Crimes Virtuais Impróprios e Próprios, sendo definido como os Crimes Virtuais Impróprios, como crimes que ocorrem através do sistema informático, que é apenas um meio para a execução do delito, sendo que o seu papel não é essencial para a existência dos crimes, pois podem ocorrer através de outros meios e são considerados crimes de ação livre que respalda na legislação pátria, mas que requerem de uma legislação penal específica (DE PAULA, 2012).

Por outro lado, os Crimes Virtuais Próprios são definidos, através das práticas de delitos voltadas para o próprio computador, enquanto elemento físico da denúncia, ou seja, as condutas ferem bens jurídicos inerentes à informática,

que consiste no acesso a dados e informações interligados a ele (CRESPO, 2011). Os delitos que tem o objetivo de enfraquecer o funcionamento de um sistema computacional, servidores, ambientes de rede, banco de dados e até mesmo websites, são considerados também como Crimes Virtuais Próprios (DE PAULA, 2012).

Pinheiro (2010, p. 27) classifica os Crimes Virtuais, como:

Os crimes eletrônicos ou cibernéticos têm modalidades distintas, dependendo do bem jurídico tutelado. Nesse sentido, podemos dar como exemplo o crime de interceptação de dados, que tem como bem jurídico tutelado os dados, ou seja, o que se quer é proteger a transmissão de dados e coibir o uso dessas informações para fins delituosos, como, por exemplo, captura de informações para envio de “e-mail bombing”, o “e-mail com vírus”, o “spam”. Esse tipo penal protege também a questão da inviolabilidade das correspondências eletrônicas (PINHEIRO, 2010, p. 27).

Do mesmo modo, Rossini (2002), denomina as duas classificações de crimes virtuais apontadas acima, como crimes virtuais puros e mistos. Sendo os crimes puros, as práticas delituosas que viola o sistema computacional, em que o criminoso tem como objetivo atingir os próprios dispositivos eletrônicos ou o banco de dados presente nesse dispositivo. Os crimes virtuais puros, são as práticas delituosas, no qual o computador atua como uma ponte para que o criminoso ofenda e viole os direitos de terceiros, podendo ser tipificados como estelionato, ameaça e crimes contra a honra.

Os sujeitos ativos dos crimes virtuais considerados puros, são conhecidos como, hackers e crackers. De acordo com Greco (2017), os hackers são pessoas no qual detém um conhecimento relevante de informática e que utilizam desse conhecimento para desenvolver habilidades para violar os mecanismos de segurança para invadir os dispositivos eletrônicos alheios. Por muitas vezes eles não praticam o delito com o intuito de praticar o crime, mas eles fazem para desafiar a si mesmo, chegando a gerar competições entre os grupos de hackers para ver quem consegue invadir mais páginas nas internet, elucidando o fato de que os usuários dessas páginas estão vulneráveis na rede mundial de computadores.

Os crackers, são conhecidos como indivíduos que utilizam a internet com a finalidade de cometer o crime, visando não apenas a invasão de um sistema, mas utilizando das suas habilidades para fins lucrativos ao realizar fraudes eletrônicas e bancárias, aplicando diversos golpes em pessoas físicas e jurídicas (GRECO, 2017).

O anonimato é um dos principais pontos discutidos quando se trata de crimes virtuais, tendo em vista que o criminoso cria diversos perfis falsos, o que dificulta a sua identificação. O rastreamento do número de IP (Internet Protocol) é uma das maneiras de chegar aos infratores, o IP é uma identificação do computador e que é usado durante o inquérito policial como uma evidência concreta da autoria dos delitos pelo responsável do computador. Malaquias (2015, p 12) entende que:

O Estado não pode estigmatizar o indivíduo alcançar pessoas abstratas com meras inferências. A perfeita identificação do autor e a correta delimitação da infração cometida são essenciais para se punir o criminoso virtual principalmente, quando se considera o ambiente virtual em que o crime foi praticado, caracterizado pela ausência da presença física do infrator (MALAQUIAS, Roberto Antônio Darós, 2015 p 12).

Em suma, a identidade virtual possui grande importância, entretanto, a ausência de normas específicas contribuiu com diversos precedentes e posicionamentos sobre o assunto por parte do ordenamento jurídico, cabendo ao Poder Legislativo tipificar e especificar uma legislação que puna as práticas delituosas, com o intuito de garantir que os direitos das vítimas desses crimes sejam resguardados e que a impunidade dessas práticas sejam sandas.

Ao regulamentar as infrações das práticas que envolve os crimes virtuais, a legislação brasileira discutiu a necessidade de tipificar a primeira modalidade de crimes virtuais puros, mas o ordenamento jurídico tem encontrado dificuldades para enfrentar esse novo modelo de criminalidade, principalmente quando se trata dos crimes, que não são possíveis identificar os criminosos, a fim de puni-los.

### **3.2- Avaliação as leis que assegura as das vítimas de crimes virtuais no Brasil**

A tipificação dos crimes virtuais conhecidos como puros no Brasil se deu a partir da criação da Lei de nº 12.737 de 30 de novembro de 2012, que inseriu os artigos 154-A e 154-B no Código Penal, sendo que o primeiro descreve a conduta típica e menciona a sua qualificação e as causas no aumento da pena estabelecida e o segundo, descreve a ação penal referente a espécie do delito.

Os dispositivos legais mencionados, dispõem:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. §1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. §2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. §3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. §4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. §5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime for 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. (BRASIL, 2012).

A Lei de nº 12.737 também é conhecida como a Lei da Carolina Dieckmann, pois a edição foi motivada pela divulgação das suas fotos íntimas em diversos sites e redes de computadores mundiais, após terem sido furtadas pelo seu computador pessoal. O crime teve grande repercussão nos veículos de mídia que fornece informações para a população e a partir dessa repercussão que surgiu a necessidade de regulamentar esses delitos que são cometidos no ambiente virtual.

De acordo com Nucci (2017, p. 546), “criou-se novel figura típica incriminadora, buscando punir quem viole não apenas a comunicação telemática, mas também os dispositivos informáticos, que mantêm dados relevantes do seu proprietário”.

Entende-se que o bem jurídico tutelado, de acordo com Cunha (2016), que a privacidade individual ou profissional é armazenada em um dispositivo informático, que em consonância com o direito, à intimidade e à vida privada da vítima é assegurada pelo 5º artigo, inciso X, da Constituição Federal. Sendo classificado como conduta punitiva, a invasão do dispositivo informático de terceiros, mediante a violação do dispositivo de segurança contrato pela vítima e da instalação de sistema que podem causa a vulnerabilidade do dispositivo, sendo que as formas de execução sejam voltadas para o furto dos dados e das informações disponíveis no dispositivo.

Em face a essa realidade, é importante frisar que o crime previsto no Art. 154-A do Código Penal, é um crime de menor potencial ofensivo, a partir das disposições da Lei de nº 9.099/95, sendo que o agente tem direito aos benefícios da transação penal e suspensão da condicional do processo, quando na sua forma qualificada (§3º), for majorado pela divulgação, comercialização ou transmissão a terceiro dos dados ou informações obtidas (§4º). Sendo que a ação penal no delito tutelado se torna pública e condicionada, quando a vítima faz a representação do crime, e terá como exceção, quando os crimes virtuais são cometidos contra a administração pública direta ou indireta de qualquer um dos Poderes da União, Dos Estado, Municípios e dos Distrito Federal, ou até mesmo de empresas que fazem a prestação de serviços públicos, e está inserido no Art. 154-B do diploma repressivo (CUNHA, 2016).

As práticas dos crimes considerados como mistos, no qual os dispositivos são utilizados como meio para realizar variadas práticas de infrações penais, são poucos mencionados pela legislação penal brasileira. Mas no geral, as infrações penais tidas como, ameaça, estelionato e a perturbação da paz, recebem o mesmo tratamento, quando são praticados no ambiente virtual, portanto não há nenhuma prescrição legal específica que enfrente as diversas práticas delituosas mencionadas. Ademais, a exceção é apenas para os crimes praticados contra a

honra, que apresenta um aumento na pena quando eles são praticados meios que possibilitam a sua dispersão e está disposto no Art. 141, inciso III, do Código Penal, in verbis:

“Art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido: [...] III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria”. (BRASIL, 1944).

Em 2004, o pesquisador John Suler, ao realizar um estudo sobre o comportamento humano no ambiente virtual, relata que esse meio é um ambiente seguro para a exposição e que os indivíduos se sentem encorajados a falar mais sobre a sua vida, falar sobre as suas alegrias, tristezas, angústias, fantasias e desejos, esse encorajamento se dá pelo anonimato que o ambiente virtual proporciona. De acordo com essa premissa, o pesquisador identificou o termo que ficou conhecido como, efeito desinibitivo online, que apresenta o comportamento real e virtual que acarreta as ações diferentes do mesmo indivíduo, no qual muitos desses comportamentos podem gerar condutas delituosas (SULER, 2004).

O pesquisador aponta que existem seis fatores que dão origem a essas condutas delituosas e a diapasão dos comportamentos do indivíduo, sendo o que primeiro, o anonimato dissociativo, que facilita a não identificação da verdadeira identidade dos usuários, está razão é uma das justificativas que o indivíduo realiza as práticas delituosas, pela sensação de impunidade dos atos praticados. O segundo fator, é a invisibilidade, por muitas vezes o ambiente virtual não possibilita que os demais usuários consigam ver o que configura a coragem do autor, pois certamente se fosse em um ambiente público e que tivesse a presença física, ele não cometeria o delito (SULER, 2004).

O terceiro fator é a assincronia, que se refere ao fato de que no ambiente virtual a interação entre os usuários nem sempre acontece em tempo real, tal como as publicações em redes sociais, o que faz com que alguns usuários se sintam mais seguros e encorajados ao enviar uma mensagem ofensiva que pode ser divulgada através de outros usuários, em virtude da impunidade e que em um curto

espaço de tempo, os usuários irão esquecer. O quarto fator citado pelo autor, é o que ele define como introjeção solipsista, que consiste em uma percepção criada no ambiente virtual, no qual os usuários fazem uma fusão da sua mente e do seu comportamento virtual, essa fusão pode proporcionar a quem faz a leitura das publicações desse indivíduo a audição da voz dentro da sua própria mente e introjetada em sua psique.

Para Lucena (2012), a introjeção solipsista tem relação com o fato de que a sua imaginação é segura e correta, desta forma os usuários se sentem livres para realizar as práticas delituosas que não fariam na realidade. Muitas das vezes as práticas desses delitos, apontam que a realidade é a imaginação do indivíduo. Sendo assim, o texto virtual pode se transformar em um mecanismo de trapaça psicológica, em que a mente do indivíduo tece papéis fantasiosos e usam desse mecanismo para realizar as práticas sem desinibição, essa conversa pode ser experienciada inconscientemente como se a pessoa estivesse falando com ela mesma, e falando com ela mesmo o usuário se sente à vontade para dizer tudo o que pensa e não diria normalmente (SULER, 2004).

O quinto fator é a imaginação dissociativa, em que o usuário a partir da introjeção solipsista para de se sentir como um personagem imaginário que ele criou em sua fantasia, no qual ele separa a sua responsabilidade, da moral da realidade em que vive, acreditando que quando ele se desvincular do seu dispositivo eletrônico, ele deixa o seu mundo imaginário e volta para a sua realidade concreta. E o sexto fator, Sulen (2014), define como efeito desinibitivo online, que se refere a minimização da autoridade, tendo em vista que o ambiente virtual os usuários tem o mesmo poder e voz, razão pela qual, no mundo real o indivíduo reluta em expor suas opiniões em face de uma figura de autoridade e no ambiente virtual ele se sente mais à vontade para manifestar de forma livre e ofensiva, uma vez que a autoridade é minimizada.

Pela observação dos aspectos analisados na obra de Suler (2014), o ambiente virtual conduz a dissociação entre o comportamento do usuário no mundo virtual e no mundo real, constituindo de fato, um meio em que a violência verbal e as práticas delituosas são facilitadas. E de acordo com Lucena (2012), os

usuários podem assumir diferentes papéis para não se comprometer diante do seu comportamento agressivo, e a ausência da identificação facilita também as agressões verbais, que são norteadas pela falta de ética. As identidades verdadeiras são difíceis de serem identificadas no ambiente virtual e a reputação não carrega o mesmo peso das que tem fisicamente.

No entanto, os delitos praticados no ambiente virtual são de difícil apuração e se torna um dos maiores desafios do direito para realizar a elucidação da autoria delitiva, conforme ressalva Delgado (apud GRECO, 2017, p. 585-586), [...] a dificuldade em atribuir a autoria do fato vem, em grande medida, determinada pela dificuldade probatória que rodeia a ilicitude informática. Isso se deve à própria dinâmica do processamento informático, que impede detectar uma determinada atividade ou processo posteriormente à sua realização, e em outras ocasiões, devido à facilidade para fazer desaparecer, de forma fraudulenta, por meio da manipulação de programa e dados, as atividades, operações, cálculos ou processos que foram realizados anteriormente.

A princípio, além da própria identificação da autoria delitiva, a investigação do dolo e da culpa é muito importante e esses elementos subjetivos são de difícil constatação de delimitação no ambiente virtual. Segundo Pinheiro (2010, p, 294):

“em computação forense as ‘testemunhas máquinas’ não conseguem diferenciar culpa de dolo. Ou seja, um computador não traz informações de contexto da situação, tampouco consegue dizer se foi ‘sem querer’, sem intenção” (PINHEIRO, 2010, P. 294).

Deste modo, em muitos casos a tarefa de identificar o agente delituoso agiu sem a intenção de provocar sentimentos de constrangimento da vítima. O autor aponta a existência de dois fatores que contribuem para a dificuldade de penalizar os crimes virtuais, sendo o primeiro, a falta de conhecimento dos usuários da rede de computadores, o que por muitas vezes não são passadas as autoridades as informações necessárias e o segundo fator são o despreparo da polícia no processo investigativo. Os principais problemas do enfretamento dos crimes virtuais são a falta de denúncia dos usuários e o despreparo dos profissionais da

segurança pública para apurar as informações cedidas pelas vítimas, para que a partir das práticas do agente delituoso possa ser identificado dentro dos requisitos que caracteriza uma infração penal.

Elucida, Castro e Pereira (2015, p. 451), sobre a questão pontuada acima, [...] não se pode permitir que a discussão sobre a necessidade de leis específicas soterre o necessário debate acerca das medidas governamentais de enfrentamento à criminalidade digital. É realmente notório que o Brasil ainda está gatinhando na criação e estruturação de departamentos de polícia especializados em crimes digitais, e os que existem sofrem com a falta de recursos humanos e tecnológicos.

Por conseguinte, outro aspecto que é relevante discussão quando se trata dos crimes virtuais, é a aplicação da lei penal no ambiente virtual, pois dentro do espaço virtual a troca de informações e divulgação da mesma ocorre muito rápido e de qualquer lugar do mundo, como elucida (CONTE; SANTOS, 2018, p. 14). Desta forma, o agente delituoso pode estar em qualquer país, e acessar a internet de forma anônima, sem precisar se identificar, e não descartando o fato de que ele invadir diversos sistemas de muitas empresas, o que pode gerar prejuízo que para o Estado-nação.

É inquestionável a necessidade da discussão sobre os crimes virtuais, tendo em vista que a problemática é muito recente, e é um dos principais problemas que permeia as conexões humanas através do sistema computacional. Entretanto é importante salientar que não são raras as vezes que as transgressões de normas jurídico-penais, se torna a produção da verdade no ambiente virtual, a partir do surgimento do conceito, chamado como pós verdade. Desta forma, deve ser apurado e separado do direito à liberdade de expressão e a informação que assegura as vítimas de crimes virtuais.

### **3.3- Levantamento de dados no banco DFNDR lab., SAFERNET e ANATEL**

A SaferNet Brasil, foi criada em 20 de dezembro de 2005, com o objetivo de promover a defesa dos Direitos Humanos na Internet no Brasil, em uma época no qual tinha uma necessidade de ter uma resposta mais eficientes para os graves problemas relacionados as práticas delituosas que utilizam a internet e o sistema computacional com o intuito de violar os Direitos Humanos dos usuários.

Com o aumento dos números de produção e divulgação de pornografia, abuso sexual de crianças, aliciamentos de menores, racismo, homofobia e intolerância religiosa a SaferNet Brasil começou a atuar como uma rede de notificação e denúncias das páginas que vinculavas as informações e que repassa as informações coletadas para o Ministério Público, que tem o discernimento de investigar e identificar os responsáveis pela página e das práticas criminosas.

A Anatel foi a primeira agencia reguladora a ser instalada no Brasil, em 5 de novembro de 1997 e que foi criada a partir da regulamentação da Lei Geral de Telecomunicações, Lei 9.472, de 16 de julho de 1997. Sendo conhecida como uma entidade integrante da Administração Pública Federal indireta, submetida a um regime autárquico especial vinculada ao Ministério das Comunicações, que adota as medidas necessárias para o atendimento ao público, mas possuem as seguintes determinações:

- I- compor administrativamente conflitos de interesses entre prestadoras de serviços de telecomunicações;
- II- expedir ou reconhecer a certificação de produtos, observados os padrões e as normas por ela estabelecidos;
- III- administrar o espectro de radiofrequências e o uso de órbitas, expedindo as respectivas normas;
- IV- reprimir infrações aos direitos dos usuários;
- V- exercer, relativamente às telecomunicações, as competências legais em matéria de controle, prevenção e repressão das infrações da ordem econômica, ressalvadas as pertencentes ao Conselho Administrativo de Defesa Econômica (Cade).

O DFNDR lab., é um laboratório que conta com uma tecnologia que detecta crimes virtuais, através de uma inteligência artificial. A criação desse laboratório é uma resposta do aumento do número de crimes virtuais no mundo. Diariamente milhares de pessoas sofrem golpes digitais e possuem os seus dados furtados do seu dispositivo eletrônico, e o laboratório além de identificar os sites no qual

ocorrem praticas delituosas, ele serve como um método de prevenção de crimes virtuais, pois a população pode enviar os links das páginas para o site, que faz uma busca e informa se há uma possível prática de crimes virtuais, esse serviço é oferecido para os usuários de forma gratuita. O laboratório também permite montar uma base de dados dos crimes virtuais que acontecem em todos os países, juntamente com a classificam dos tipos de crimes, de acordo com o ano escolhido, sendo disponibilizado do ano de 2000 a 2021.

O Brasil carece de políticas públicas e de campanhas de enfrentamento a esses crimes, tal como a conscientização da população, acerca de utilizar a internet de uma forma segura, o aumento dos estudos de crimes virtuais se torna relevante para mensurar a quantidade de denúncias já realizadas, o conhecimento da legislação vigente e a disseminação acerca da estrutura de amparo das vítimas.

### **3.3.1- Construção de gráficos e histogramas**

Entende-se que a representação gráfica dos dados estatísticos tem como objetivo apresentar dos dados analisados de forma rápida e consica, permitindo com o que o leitor chegue a um entendimento e esclarecimento dos resultados encontrados no estudo.

Tornando-se possível a representação gráfica dos dados, estabelecemos uma correspondência entre os termos da série de dados em uma determinada figura geométrica, de modo que cada elemento da série de dados seja representada por uma figura propocional escolhida.

A representação gráfica deve seguir os respectivos requisitos: a simplicidade, que é indispensável devido à necessidade de levar uma rápida compreensão dos dados dispostos da figura; a clareza, que possibilita uma interpretação correta dos dados dispostos na figura; e a veracidade, que é indispensável, pois apresenta a realidade dso dados dispostos na figura.

Os gráficos escolhidos para a construção dos resultados do presente estudo são, os gráficos de barras, que tem como finalidade comparar com grandeza os dados indicados na série, os gráficos em colunas, que tem como finalidade também comparar os dados indicados na série, mas oferece ao leitor uma legenda para uma maior interpretação dos dados indicados na série e o gráfico de setor, que é uma representação gráfica dos dados estatísticos em um círculo, que é dividido em setores, de acordo com os dados indicados na série que representará a figura.

A construção dos histogramas, é uma alternativa que facilita a compreensão do entendimento dos dados apresentados e dos resultados apontados ao longo do estudo, pois é uma construção gráfica realizada a partir de uma distribuição de frequência, que irá indicar os dados da série que irá compor a figura.

Em vista disso, a metodologia do presente estudo, estende-se de um método qualitativo e descritivo, pois dessa forma, serão analisados os crimes virtuais por intermédio do banco de dados do laboratório especializado em crimes virtuais DFNDR lab- Laboratório de Cibersegurança da PSafe, SAFERNET- Centro de Apoio Operacional das Promotorias da Criança e do Adolescente. e ANATEL- Agência Nacional de Telecomunicações, nos períodos de janeiro a dezembro de 2006 a 2014 e 2018.

Com a finalidade de levantar os seguintes dados dos crimes: racismo, preconceito, homofobia, pornografia infantil, apologia e incitação a crimes contra a vida e intolerância religiosa, baseados nos objetivos de identificar os crimes virtuais frequentes. Tendo com o objetivo o estudo dos dados de bancos DFNDR lab, SAFERNET e ANATEL que serão levantados e tabulados no Word e Excel para que os dados sejam analisados de forma correta e eficaz, em seguida os dados serão calculados para que sejam colocados nas tabelas de distribuição de frequência. A tabela de distribuição de frequência é uma ferramenta utilizada para a construção de gráficos e histogramas, que serão inseridos para a realização das análises e conclusões dos resultados obtidos no estudo.

## **4- CENÁRIO ATUAL BRASILEIRO E PERSPECTIVAS DE MUDANÇAS**

### **4.1- Análise dos dados levantados de crimes virtuais**

A coleta e análise de dados do presente estudo estende-se de um método qualitativo e descritivo, pois dessa forma serão analisados os crimes virtuais por intermédio do banco de dados do laboratório especializado em crimes virtuais DFNDR lab- Laboratório de Cibersegurança da PSafe, SAFERNET- Centro de Apoio Operacional das Promotorias da Criança e do Adolescente. e ANATEL- Agência Nacional de Telecomunicações, nos períodos de Janeiro a Dezembro de 2006 a 2014 e 2018.

Sendo assim, foram realizadas as coletas dos respectivos dados dos seguintes crimes: racismo, preconceito, homofobia, pornografia infantil, apologia e incitação a crimes contra a vida e intolerância religiosa, baseado no objetivo de identificar os crimes virtuais frequentes no Brasil.

Na primeira etapa do levantamento dos dados dos bancos DFNDR lab, SAFERNET e ANATEL os números de denúncias foram inseridos e tabulados no Word e Excel para que os dados fossem analisados de forma correta e eficaz, em seguida os dados foram calculados e inseridos nas tabelas de distribuição de frequência. A tabela de distribuição de frequência é uma ferramenta utilizada para a construção de gráficos e histogramas, que serão inseridos para as análises e compreensão dos resultados obtidos no presente estudo.

Posteriormente, na segunda etapa, foram investigados os novos crimes virtuais, com as maiores incidências no mundo e que não foram tipificados judicialmente. Os novos crimes foram listados e seus respectivos dados foram inseridos no Word e no Excel para a construção de gráficos comparativos entre os países do mundo e do Brasil.

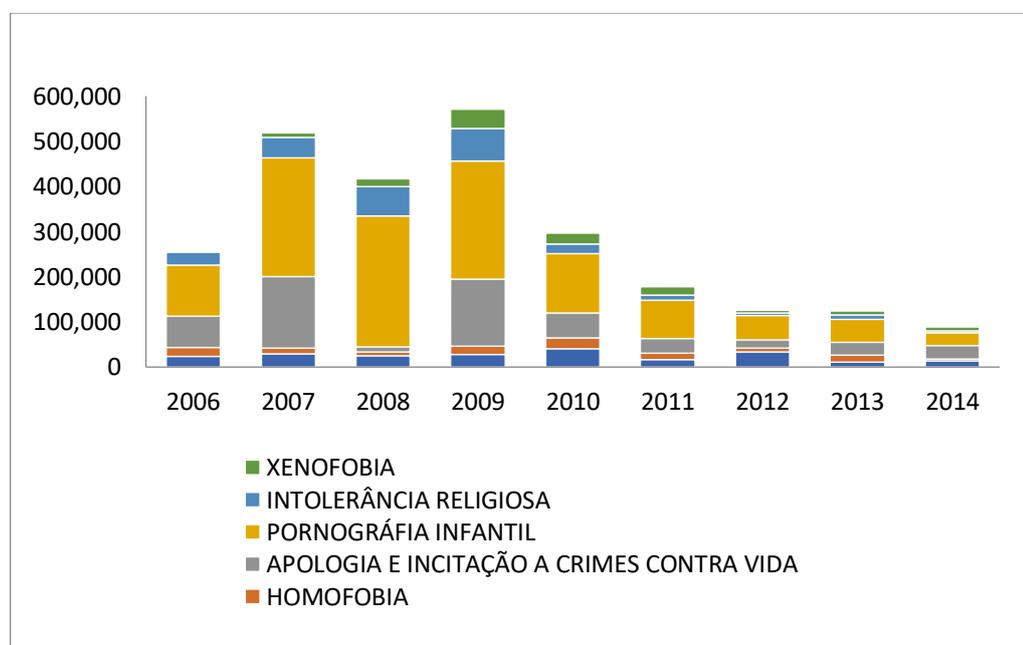
Por conseguinte, na terceira etapa da pesquisa tem como objetivo promover uma análise estatística entre banco de dados escolhidos DFNDR

lab, SAFERNET e ANATEL, os seguintes resultados encontrados foram descritos ao longo do estudo, tendo em vista que o propósito é de identificar e classificar os crimes virtuais existentes e os novos, avaliar as propostas de medidas de prevenção contras essa pratica de crime virtual e as leis que buscam aprovações para que os criminosos sejam punidos justamente, é necessário uma parceira e estudo de bibliografias e legislações vigentes, referente ao tema.

#### 4.2- Análise dos números de denúncias de crimes virtuais no Brasil por meios dos gráficos

O (gráfico 2), demonstra o número de denúncias realizadas no Brasil, nos seguintes períodos de 2006 a 2014 de acordo com os crimes virtuais tipificados e com punições prescritas no Código Penal Brasileiro, utilizando os seguintes bancos de dados: DFNDRIab, SAFERNET e ANATEL.

**Gráfico 3:** Número de denúncias de crimes virtuais realizadas no Brasil, nos respectivos períodos de 2006 a 2014



**Fonte:** Próprio autor

Ao analisar os dados levantados, de acordo com o (gráfico 2), os números de denúncias de pornografia infantil e de racismo tiveram um aumento

significativo entre os anos de 2006 a 2009. Esses crimes tiveram um aumento, pois a internet se torna um ambiente favorável para as práticas desses crimes, através das redes sociais, emails e chats, os crimes de discriminação racial são praticados de diversas formas, segundo Bulos (2003), “racismo é todo e qualquer tipo de tratamento discriminador da condição humana em que o agente dilacera a autoestima e o patrimônio moral de uma pessoa ou de um grupo de pessoas, tomando como critérios de raça ou cor da pele, sexo, condição econômica, origem, etc”. Visto que o crime de racismo agride a honra do indivíduo, a constituição Federativa do Brasil no seu artigo XLII cita que a “prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei”.

Levando-se em consideração os dados da SAFERNET, que possuiu parceria com Polícia Federal, Câmara, Senado, Secretaria de Direitos Humanos, Ministérios Públicos Federais de Minas Gerais e da Paraíba, a página reúne dados estatísticos de setes entidades que aceitam e reúnem denúncias anônimas de crimes contra direitos humanos e de animais, cerca de 50% das denúncias são de pornografia infantil sobre o domínio de 224,6 mil sites. Devido à ocorrência do aumento de denúncias de pornografia infantil e racismo, a Polícia Federal realizaram seis operações contra esses delitos, em 2012 foram apreendidos textos com ilustrações de mulheres e crianças sendo decapitadas por manterem relações sexuais com homens negros (BRAGA, BRAGA, ROVER, 2012).

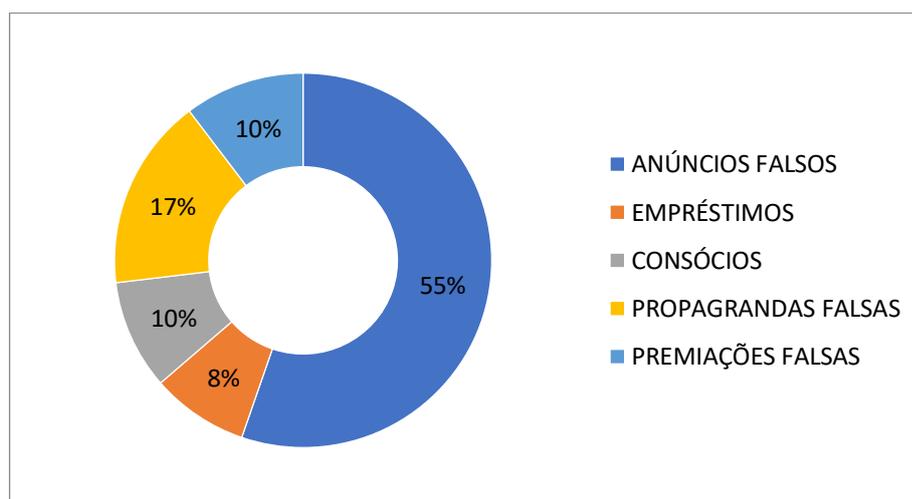
O Brasil ocupa o primeiro lugar no ranking de divulgação de pornografia infantil com mais de 1200 endereços confirmados que abastecem os mercados internacionais de pedofilia, normalmente os sites com conteúdos voltados para crianças possuem uma extensão direcionada para os conteúdos de cunho sexual e possuem salas de bate papos para os indivíduos conversarem entre si enquanto assistem os conteúdos disponíveis (ARAÚJO, COUTINHO, SANTOS, 2006). Essas extensões são abertas através de palavras chaves estrangeiras ou até mesmo desenhos que já são conhecidos entre os usuários desses conteúdos.

A senadora Marina Silva criou um projeto, conhecido por projeto de lei (n. 135/99) que foi discutido e aprovado pelo poder legislativo em 21/10/2001 que se trata de proteger legalmente crianças e adolescentes às mudanças sociais, especialmente contra crimes e abusos sexuais, que têm aumentado de proporção, porém em a lei altera o artigo 241 do ECA, mas essa alteração é positiva, pois trata de tipificar os crime de produção e divulgação de imagens de menores em cenas de sexo explícito.

#### 4.3- Levantamento de dados dos novos crimes virtuais no Brasil

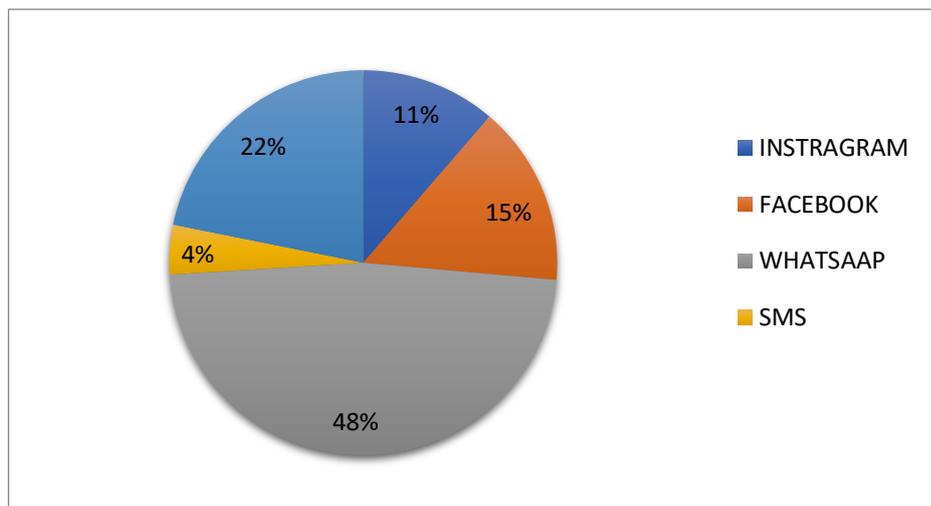
De acordo com o (gráfico 3) que corresponde a freqüência dos novos golpes ocorrida no período de 2018 no Brasil, e aponta que os números de anúncios e propagandas falsas correspondem a 72% dos casos de denúncias de crimes virtuais neste período, corroborando assim os dados do (gráficos 4) que aponta as plataformas com as maiores freqüências de golpes aplicados na população brasileira.

**Gráfico 4:** Freqüência dos novos de crimes virtuais realizados no Brasil, em 2018



**Fonte:** Próprio autor

**Gráfico 4:** Frequência dos novos de crimes virtuais realizados no Brasil, nas respectivas plataformas virtuais, em 2018



**Fonte:** Próprio autor

Entre os anos de 2011 e 2012, no Brasil o número de denúncias de crimes virtuais ocorridos no Facebook identificaram cerca de 11.305 endereços. Esses endereços foram denunciados para a CND- Central Nacional de Denúncias de Crimes Cibernéticos, que indica um crescimento de 264,50% comparados aos 39 do ano de 2011. No ano de 2014, a Polícia Federal e a Secretária de Direitos Humanos repassaram as denúncias apresentadas pelas CND para o Ministério Público, que removeram da internet cerca 2.400 sites com conteúdo ofensivos. Com o surgimento de novas redes sociais como o Snapchat, Twitter, Instagram e Whatsapp, os números de denúncias de crimes virtuais ocorridos no Facebook caíram deliberadamente e os números de crimes nas novas redes sociais assustaram e estamparam muitas reportagens em jornais alertando a população.

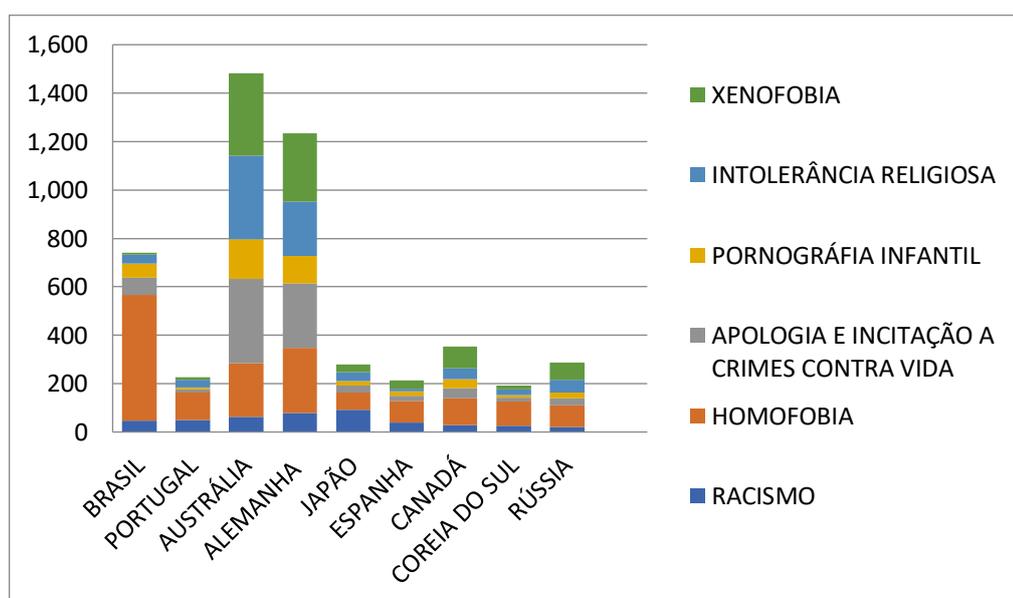
Dado o exposto aumento dos números de denúncias, elas apresentaram uma tendência negativa e preocupante para a população brasileira, pois a maioria dos golpistas tem como objetivo o roubo de dados dos usuários, como os emails, senhas, contas bancárias e fraudes de CPF. À vista disso, nos casos de abuso não autorizado da imagem de uma pessoa física, está pode requerer perante a justiça, a restituição do dano através de indenização, de acordo com a Súmula 403, “Independente de prova do prejuízo à indenização pela publicação não autorizada da imagem de pessoa com fins econômicos ou comerciais” (SCAPIM,

2012).

#### 4.4- Comparação do número de denúncias de crimes virtuais no mundo

De acordo com o (gráfico 5), que corresponde aos números de sites denunciados nos seguintes países, Brasil, Portugal, Austrália, Alemanha, Japão, Espanha, Canadá e Coreia do Sul de acordo com cada crime virtual tipificado no ano de 2018. Em comparação com a Austrália e Alemanha o crime que se faz mais presente em denúncias no Brasil é a homofobia, um crime que tem crescido muito e representa cerca de 70% dos números de assassinatos de LGBTQI+. A homofobia é um crime anoso e que só teve uma tipificação de crime na lei de racismo no Brasil, os ministros Celso de Mello, Edson Fachin, Alexandre de Moares, Luíz Roberto Barroso, Rosa Wber, Luiz Fux, Cármen Lúcia e Gilmar Mendes votaram pelo enquadramento da homofobia e transfobia como tipo penal definido na Lei do Racismo, Lei 7.716/1989, no dia 13, 2019, o que foi um marco na causa LGBTQIA+, tendo em vista que o Brasil é um dos países que mais mata mulheres e homens trans.

**Gráfico 5:** Número de sites denunciados por apresentarem crimes virtuais realizados nos respectivos países, em 2018



Fonte: Próprio autor

#### 4.5- Avaliação da legislação vigente de crimes virtuais no Brasil

A legislação brasileira que trata de crimes virtuais passou por um processo de reforma e melhoria para combater os crimes que ocorrem de forma virtual, em virtude da repercussão dos crimes nos veículos de disseminação de informações e em decorrência da repercussão a punição para os crimes que ocorrem na internet precisou ser avaliada.

Levando-se em consideração a legislação voltada para os crimes virtuais no Brasil é necessário ampliar e correlacionar os estudos entre a informática e o direito, por mais que pareça ser difícil, a ciência jurídica estuda a evolução tecnológica e a vertante do ordenamento jurídico, de acordo com Alan Moreira (2012, p. 20):

A confirmação dessa necessidade se dá na medida em que se observa um aumento constante nas condutas criminosas praticadas através de recursos informáticos. A busca de maior compreensão tecnológica objetiva oferecer ao usuário maior segurança, caso contrário existirá uma forte tendência ao caos, mas mesma velocidade da evolução tecnológica (2012, p. 20).

A Lei de nº 12.737/2012, já mencionada anteriormente no presente estudo e conhecida como a Lei Carolina Dieckmann, no qual a atriz teve suas fotos íntimas furtadas e divulgadas, incluiu no Código Penal os artigos 154-A e 154-B, que apresenta a origem do crime de invasão de dispositivo virtual e alterou os artigos 226 e 298 no Código Penal (CRESPO, 2013).

A alteração do artigo 154 do Código Penal, visa punir a conduta do hacker, visto que a conduta indicada no dispositivo 154-A tipifica a invasão dos dispositivos informáticos para obter e destruir as informações de terceiros ou até mesmo instalar software que possam causar vulnerabilidade com fim de obter certas vantagens (BRASIL, 1940).

O artigo 154-B afirma a representação penal tipifica a conduta do criminoso no artigo 154, se o crime for praticado contra a administração pública

direita ou indiretamente de quaisquer Poderes da União, Estados e Municípios. A alteração realizada no artigo 298 do Código Penal, visa inserir um parágrafo único voltado para a falsificação de cartão de crédito ou débito (BRASIL, 1940).

As Leis de nº Leis 12.735/2012 e 12.737/2012, entraram em vigor em Abril de 2013, que alterou o Código Penal no que se trata de crimes virtuais. Os projetos apresentaram como alternativa à Lei Azeredo que recebeu muitas críticas por conta da supressão da liberdade virtual dos usuários da internet e a sua promulgação preveu a obrigatoriedade dos órgãos do setor judiciário se estruturar e promover o combate das práticas delituosas no ambiente virtual.

Diantes das análises, o dispositivo que trata da responsabilidade dos provedores da internet seja duvidoso, e ao longo da sua tramitação foi reduzido a quatro artigos e foi reduzida por conta do veto na sanção da Presidência da República. Em Maio do ano de 2013, entrou em vigor o Decreto Federal a Lei de nº 7.962/13, que visa preencher as lacunas do Código de Defesa do Consumidor acerca dos crimes realizados em lojas virtuais, visto que não existe uma legislação específica de compra e venda pela internet. Sendo assim as novas normas determinou algumas regras para as empresas que possuem um comércio eletrônico (CASSANTI, 2014).

Em Maio do ano de 2016, o Marco Cível da Internet preve a aplicação da Lei Brasileira aos crimes praticados no ambiente virtual, que demanda certa atenção e preocupação com a aplicação do ordenamento jurídico para o enfrentamento das práticas delituosas no ambiente virtual e sanar as dificuldades encontradas pela Justiça Brasileira na obtenção das provas que serão apresentadas pelas vítimas durante o processo.

Após a promulgação do Marco Civil da Internet o posicionamento do Estado pela busca da regulamentação das práticas da sociedade civil no ambiente virtual apontou um avanço, no que se trata do combate e prevenção dos crimes virtuais ainda não tipificados, além do que o Marco Civil regulamenta a proteção de dados dos usuários da internet.

Compete ao Estado, o Poder Judiciário e Legislativo, combater os crimes de virtudes virtuais, fazendo-se necessário a atuação firme e severa do Poder Judiciário que por meio dos julgamentos e com o auxílio da Segurança Pública punir os usuários que cometem os delitos descritos ao longo da pesquisa, para que os usuários da internet possam continuar usando a ferramenta com segurança. O Poder legislativo juntamente com a Segurança Pública pode discutir projetos de leis que buscam proteger as vítimas desses crimes virtuais, assegurando os seus direitos como cidadão e empenharem-se para conscientizar os usuários através de cartilhas, charges, palestras, cursos, trocam de idéias, entre outros.

#### **4.6. Avaliação dos novos dispositivos legais de crimes vituais no Brasil**

A sociedade contemporânea podem ser caracterizadas pela inovação tecnológica e a interação social, os novos meios tecnológicos são capazes de desenvolver novos mecanimos de convivência e interação entre as pessoas e a consequência desta prática aponta a necessidade de avaliar e aprimorar os dispositivos legais.

Por conta dessa evolução, a população tenta alcançar novos objetivos que podem resultar em transformações nas áreas de conhecimento, principalmente a da ciência jurídica. Desta forma o direito sempre acompanhará as inovações presentes na sociedade.

O Direito Penal deve reformular as políticas de prevenção e combate a criminalidade através da aplicação de penas mais justas, apontando a necessidade de debater e analisar o conceito inerentes aos crimes, que não apenas um fenômeno social e sim um episódio que aconteceu com a vítima.

A promulgação das leis que regulamentam o direito as vítimas de crimes vituais deve provocar a jurisdição, com o objetivo de resolver os conflitos entre a população e o ambiente virtual. O Brasil é um dos países que mesmo

apresentando leis que estão em vigência, elas ainda não são apresentadas de forma clara e não abrangem todos os tipos de crimes virtuais que ocorrem diariamente (CRESPO,2013).

A proteção dos dados pessoais é necessária para manter a segurança dos usuários de dispositivos tecnológicos a fim de evitar abusos e furto dessas informações, sendo assim a Lei de nº 12.965/2014 regulamenta em seu artigo 7º:

Art. 7.º - O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei [...] (BRASIL, 2014).

O legislador buscou proteger os usuário de possíveis práticas delituosas, de acordo com o artigo 4º Lei de nº 12.527/2011, os dados informados pelo usuário não são detidos pelos sites que eles acessam, o site hospeda as informações pessoais e não possuiu qualquer direito sobre elas.

Essa lei prevê a indenização das vítimas a partir dos danos materiais ou morais em decorrência dessas práticas de violação da sua intimidade, de acordo com o Código Civil o artigo 927 garante a indenização aquele que: por ato ilícito, causar dano a outrem, fica obrigado a repará-lo. [...] Art. 944- A indenização mede-se pela extensão do dano (BRASIL, 2002).

A grande quantidade de dificuldades apresentadas quando se trata dos crimes virtuais aponta que o direito digital ainda é complexo e traz a tona a

necessidade da eficiência do ordenamento jurídico no combate aos crimes virtuais e a sua prevenção, de modo a proteger as vítimas e a população no geral, para que tenha mais cuidado e precaução ao utilizar um dispositivo tecnológico, portando a criação de novos dispositivos legais e projetos que leis que tenham como objetivo a proteção e prevenção dos crimes virtuais são essenciais diante da evolução dos dispositivos tecnológicos.

## 5- CONCLUSÃO

Conforme abordado no primeiro capítulo, um dos benefícios que a tecnologia trouxe, foi ter diminuído a distância entre os países e as pessoas. As transmissões de dados também são vistas como um facilitador, já que as transmissões desses dados são instantâneas e compartilhadas por todo o mundo. Por conta dessa facilidade de troca de informações e fornecimento de dados, muitos criminosos começaram a usar a internet como meio de praticar crimes, que na maioria das vezes a sua identificação não consegue ser rastreada.

Compreende-se que por mais que existem leis previstas para os crimes cometidos em ambientes virtuais, as mesmas apresentam uma fragilidade, tendo em vista que a demanda de processos são bem altas e muitas vítimas cobram um posicionamento eficaz das tipificações apresentadas nas leis criadas.

Posto isto, diante da temática abordada ao longo do segundo e do terceiro capítulo do estudo, é incontestável o aumento dos números de crimes virtuais no Brasil. Mas ao analisar os crimes identificados de acordo com os períodos estudados, ocorreu uma queda nos números de denúncias de pornografia infantil, devido à dedicação e serviço ostensivo da Segurança Pública que com o apoio da população que denunciou os sites, foi possível apreender os conteúdos que seriam disponibilizados nos endereços e os indivíduos que compartilhavam os mesmos.

Em contra partida os números de casos de homofobia e transfobia aumentaram de forma significativa, não somente de vias de fato virtuais mais como fisicamente, elevando o Brasil no Ranking de países que mais matam LGBTQIA++, ocupando o quarto lugar, tornando assim o México como o segundo país com o maior registro de assassinatos de LGBTQIA+ (ONU, 2020).

Foram identificadas novas modalidades de crimes, como propagando falsas, anúncios e premiações falsas, empréstimos e consócios que fazem a população brasileira alvo desses golpes diariamente, por serem divulgados em todas as redes sociais, e como o hábito diário de acompanhar as mensagens de WhatsApp e Instagram e de compartilhar para os amigos e familiares, a dispersão

desses golpes aumentam constantemente, portanto, a conscientização é uma ferramenta muito utilizada pela Segurança Pública e meio de compartilhamento de notícias como rádio e televisão, de modo com que vão informar a população sobre a importância de utilizar a internet e as redes sociais com responsabilidade e segurança e antes de compartilhar qualquer tipo de informação, seja notícia, vídeos e imagens, é de suma importância verificar a autenticidade das informações publicadas, para que ocorra uma diminuição de fake news e de golpes.

Desta forma, o Direito deve acompanhar a sociedade de forma que possa resguardar as vítimas dos crimes e punir sempre que forem necessárias as condutas praticadas pelos criminosos virtuais, previsto no Código Penal Brasileiro, em suma, mesmo com o conhecimento já existente das áreas e o empenho dos Poderes Judiciários e Legislativo, é importante que os investimentos em estudos nas áreas de tecnologia continuem para que possa haver uma diminuição dos números de crimes virtuais no Brasil e que a população possa desfrutar de maneira segura os dispositivos tecnológicos para o lazer, para o trabalho, para adquirir conhecimento e divulgar científica.

## REFERÊNCIAS

ARAÚJO, L. F. de; Coutinho, M. da P. de L.; Santos, M. de F. de S(2006). **O idoso nas instituições gerontológicas: um estudo na perspectiva das representações sociais**. Psicol. Soc., Porto Alegre, v. 18, n. 2, p. 89-98.

BRAGA, Diogo de Melo; BRAGA, Marcus de Melo; ROVER, Aires José.(2012) **Responsabilidade Civil das Redes Sociais no Direito Brasileiro**.

BRASIL. **Código Civil**. Disponível em <  
[http://www.planalto.gov.br/ccivil\\_03/Leis/2002/110406.htm](http://www.planalto.gov.br/ccivil_03/Leis/2002/110406.htm)>

BRASIL. **Código de Processo Penal**. Disponível em <  
[http://www.planalto.gov.br/ccivil\\_03/Decreto-Lei/Del3689Compilado.htm](http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689Compilado.htm)>

BRASIL. **Código Penal**. Disponível em <  
[http://www.planalto.gov.br/ccivil\\_03/decreto-lei/Del2848.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm)>

BRASIL. **Constituição Federal**. Disponível em <  
[http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)> 2

BRASIL, **Lei nº 10.866 de 26/03/2010**.

BRASIL. **Lei nº 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.

*BULOS*, Uadi Lammêgo (Autor). Edição: 11.ed ... Edição: 5ed; Ano do Fascículo: 0; Publicação: São Paulo: Saraiva , 2003;

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.

CONTE, Christiany Pegorari; SANTOS, Coriolano Aurélio de Almeida Camargo. **Desafios do direito penal no mundo globalizado: A aplicação da lei penal no espaço e os crimes informáticos**. 2018.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Editora Saraiva, 2011.  
Safernet Brasil.

CUNHA, Rogério Sanches. **Manual de Direito Penal: parte especial**. 8. ed. Salvador: Jus Podivm, 2016.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

GRECO, Rogério. **Curso de Direito Penal – Parte Geral**. 4. ed. Rio de Janeiro: Impetus. 2004.

\_\_\_\_\_. **Lei n. 9.099, de 26 de setembro de 1995**. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências.

\_\_\_\_\_. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece Princípios, Garantias, Direitos e Deveres para o Uso da Internet no Brasil. Disponível em: <  
[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm)>

\_\_\_\_\_. **Lei nº 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.

LEONARDI, Marcel. **Responsabilidade Civil Dos Provedores De Serviços De Internet**. Dissertação de Mestrado - Faculdade de Direito do Largo de São Francisco, São Paulo.

LOPES, Alan Moreira. **Crimes praticados por meio eletrônico**. 1ª Ed. Curitiba: Ag Book, 2012.

MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Provas - A investigação criminal em busca da verdade**. Curitiba: Editora Juruá, 2012.

MARTELETO, Regina Maria. (2001) **Análise de redes sociais: aplicação nos estudos de transferência da informação**. Ciência da Informação, Brasília, v. 30, n. 1, p. 71-81, jan./abr.

NUCCI, Guilherme de Souza, **O Valor da Confissão como meio de Prova no Processo Penal**, 2. ed., rev. E atual. São Paulo: Revista dos Tribunais, 1999.

NUCCI, Guilherme de Souza, **O Valor da Confissão como meio de Prova no Processo Penal**, 2. ed., rev. E atual. São Paulo: Revista dos Tribunais, 2015.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal**. Porto Alegre: PUCRS, 2006.

PINHEIRO, Patricia Peck. **Direito Digital**, 6ª edição. São Paulo: Saraiva, 2016.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SCAPIM, Eric. (2012) **Direitos da personalidade: direito à imagem**.

SAFERNET BRASIL. **Protegendo os Direitos Humanos na Sociedade da sociedade.**

SULER, John. **The Online Disinhibition Effect.** Mary Ann Liebert, v. 7, n.3, p. 321-326, 2004.

SYMANTEC. **Crimes virtuais geram mais prejuízo do que tráfico de drogas**  
Disponível em: <http://www.tecmundo.com.br/seguranca/13163-crimes-virtuais-geram-mais-prejuizo-doque- trafico-de-drogas.htm>, consultado em 18 – 10 – 2020.