CENTRO DE EDUCAÇÃO SUPERIOR REINALDO RAMOS/CESREI

FACULDADE REINALDO RAMOS/FARR

CURSO DE BACHARELADO EM DIREITO

TIAGO COSTA DA SILVA

CRIMES CIBERNÉTICOS EM RELAÇÃO AOS CRIMES CONTRA A HONRA

CAMPINA GRANDE – PB

2018

TIAGO COSTA DA SILVA

CRIMES CIBERNÉTICOS EM RELAÇÃO AOS CRIMES CONTRA A HONRA

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.

Orientador (a): prof. Ms: Ângela Paula Nunes Ferreira

CAMPINA GRANDE – PB

2018

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DA CESREI

S586c Silva, Tiago Costa da.
Crimes cibernéticos em relação aos crimes contra a honra / Tiago Costa da Silva. – Campina Grande, 2018.
31 f.

Monografia (Graduação em Direito) – Faculdade Reinaldo Ramos-FAAR, Centro de Educação Superior Reinaldo Ramos-CESREI, 2018.
"Orientação: Profa. Ma. Ângela Paula Nunes Ferreira".

1. Crimes Cibernéticos – Crimes contra a Honra – Brasil. 2. Crimes Virtuais – Legislação Brasileira. 3. Fake News - Crimes contra a Honra – Brasil. I. Ferreira, Ângela Paula Nunes. II. Título.

CDU 343.9:004.738.5(81)(094.5)(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

TIAGO COSTA DA SILVA

CRIMES CIBERNÉTICOS EM RELAÇÃO AOS CRIMES CONTRA A HONRA

Aprovada em: 11 de dezembro de 2018.

BANCA EXAMINADORA

Ângela Paula Nunes Ferreira

Profa. Ms. Ângela Paula Nunes Ferreira

Faculdade Reinaldo Ramos FARR/ CESREI

(Orientador)

Prof. Ms. Rodrigo Araújo Reul

Faculdade Reinaldo Ramos FARR/ CESREI

(1º Examinador)

André Gustavo Santos Lima Carvalho

Prof. Esp. André Gustavo Santos Lima Carvalho

Faculdade Reinaldo Ramos FARR/ CESREI

(2º Examinador)

Agradeço a Deus por ter me dado discernimento para a conclusão desse trabalho e por ter me ajudado em toda a minha jornada acadêmica.

AGRADECIMENTOS

Primeiramente a Deus que permitiu que tudo isso acontecesse, ao longo de minha vida, e não somente nestes anos como universitário, mais que em todos os momentos é o maior mestre que alguém pode conhecer. Agradeço em especial a meus pais Vera Lúcia e Ricardo Magno pelo apoio durante minha jornada e a Paula Freire que foi umas das pessoas que mais me ajudou na elaboração desse trabalho. A instituição e todo seu corpo docente em especial a minha orientadora Ms. Ângela Paula, que foi fundamental com toda sua paciência para a elaboração e total acompanhamento em meu trabalho. Por fim, e a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

RESUMO

Vivemos hoje em um mundo tecnológico em que o uso das mídias digitais se faz presente nas mais diversas situações do cotidiano. Dia após dia o uso das novas tecnologias vem ganhando mais força e em meio a todas as vantagens advindas do desenvolvimento da informática (internet), sua utilização vem sendo comprometida, pois uma grande onda de cyber crimes contra a honra se torna cada dia mais comum, já que é um dos crimes que atualmente quase nunca tem punição, pela dificuldade de identificação dos culpados.Assim, este trabalhoO trabalho tem com objetivo geral analisar o tratamento dos crimes cibernéticos no ordenamento jurídico brasileiro e a sua correlação com os crimes contra a honra previstos no Código Penal Brasileiro, fazendo uma breve análise a partir da Lei nº 12.737, de 30 de novembro de 2012.O Brasil está muito distante de ser uma potência mundial em relação a minimizar ataques virtuais, pelo contrário, está entre os 10 primeiros países com mais ataques virtuais do mundo.*Cyber* crimes nada mais é do que condutas típicas, ilícitas e culpáveis praticadas pela internet ou sistemas de informática.Os Crimes cibernéticos são classificados em três tipos: puros, mistos e comuns. No nosso Código Penal três classificações para crimes contra a honra, são elas, calúnia, difamação e injúria.No momento atual, um grande exemplo de crimes comum, o chamado “fakenews” quando é lançado um “viral”, uma espécie de nota publicada na rede “internet” noticias falsas de determinado assunto buscando na maioria das vezes denigrir a imagem da vítima com informações caluniosas e expondo a pessoa ao ridículo.Este estudo teve como base a identificação de um conjunto de termos que pertencem aos crimes cibernéticos e que há décadas que esse conjunto de crimes acontecem, mas ainda não temos uma forma concreta de combatê-lo.Concluímosque os crimes cibernéticos e crimes contra a honra praticamente não tem punibilidade visto que são temas muitos novos e o estado quase nunca consegue punir com rigidez por falta de uma legislação específica nova e eficaz, haja vista que a nossa legislação penal é muito antiga e omissa para esse tipo de crime. O Brasil ainda está em fase de desenvolvimento comparado a outros países que contam com diversos recursos e tecnologias para combater os crimes cibernéticos.

Palavras-chave: Legislação. Crimes cibernéticos. Fake News.

ABSTRACT

Nowadays, we live in a technological world in which the use of digital media is present in the most distinct situations of our everyday lives. Day after day, the use of new technologies is gaining strength and, among all the advantages coming from Informatics development (internet), its use is becoming compromised, because a great wave of cyber-crimes against honor is getting common, since it is one of the crimes that almost never is punished. This work intends to show to the reader some ways of preventing possible cyber-attacks behind hacked systems; Crackers can invade your privacy in unimaginable ways. Unfortunately, Brazil is far away of being a world power when it comes to minimizing virtual attacks; on the contrary, we are among the ten first countries with more virtual attacks around the world. Cyber-crimes are typical, illicit and culprit conducts practiced on the internet or informatics systems. Cybernetic crimes are classified into three types: pure, mixed and common. Our Penal Code brings three classifications for crimes against honor: calumny, defamation and insult. Now, a great example of common crimes, the so-called "FAKE NEWS", which releases a "viral", a kind of note published on the net, announcing fake news about a certain matter, mainly aiming to denigrate the victim's image using false information and exposing the person to ridicule. This study was based on the identification of a set of terms belonging to cybernetic crimes and that have been happening for decades, without a concrete form of be combated. Concluding that cyber-crimes and crimes against honor are practically non-punishable since they consist of new terms, the state almost never achieves a rigid punishment due to the lack of a new, specific and efficient legislation, considering that our current set of laws is ancient and omit in relation to this sort of crimes. We affirm that Brazil is still growing in comparison to other countries that count on several resources and technologies to fight against cybernetic crimes.

Key words: *Legislation. Cyber-crimes. Fake News*

SUMÁRIO

1 INTRODUÇÃO

Vivemos hoje em um mundo tecnológicoem que o uso das mídias digitais se faz presente nas mais diversas situações do cotidiano. Dia após dia o uso das novas tecnologiasvem ganhando mais força e em meio a todas as vantagens advindas do desenvolvimento da informática (internet), sua utilização vem tornando-secomprometido, pois uma grande onda de cyber crimes contra a honra se torna cada dia mais comum, pois é um dos crimes que atualmente quase nunca tem punição.

Nos dias de hoje temos várias redes sociais que representam as principais redes de relacionamento que conhecemosas que mais têm o maior numero desse tipo de crime, são: *Facebook, WhatsApp, Instagram*. A cada minuto, cerca de 50 pessoas no Brasil tem seus dados grampeados segundo o “G1noticias”, com isso, informações pessoais, sobre relacionamento, trabalho, família e dados bancários são monitorados.

> O *Cyber* crime atinge 1,5 milhão de vítimas todos os dias. Isso significa que, por segundo, 18 pessoas são atacadas por alguma forma de crime online - vírus, malware, phising, etc. No meio desse índice mundial, destacamos **28,3 milhões de brasileiros** que, anualmente, se transformam em vítimas de algum esquema virtual”. “DEPARTAMENTO DE CYBERSEGURANÇA DA SYMANTEC - 02/2018”

Os ataques principais são em cima de celulares, notebooks e *netbooks,* por se tratar de aparelho portátil de fácil acesso, através das redes *wifi* pública o usuário deixa o seu aparelho “livre” para um“hacker” amador conseguir invadir de forma que não se desconfia, com isso tem acesso a senhas de contas bancárias, fotos e vídeos íntimos, lista de contatos etc.

> O Brasil é o segundo país que mais sofre ataques pela internet, isso tudo devido ao grande número de smartphones adquiridos, tem cerca de 236 milhões de aparelhos em todo o país, com isso temos o aumento também de lojas online onde grande parte da população realiza compras pela internet utilizando se do cartão de crédito e sendo assim tendo seus dados clonados causando um enorme prejuízo na economia do país.NORTON, SECURITY, 360

Este trabalho visa mostrar para o leitor algumas formas de se precaver de possíveis ataques cibernéticos, atrás de sistemas pirateados, os Crakers invadem sua privacidade de forma essa que você nem imagina, iremos mostrar que nem toda

rede que se dizem “seguras”, realmente são, que sites, lojas virtuais, redes sociais, mesmo com toda segurança no seu aparelho pode ser quebrado, nesse contexto, faremos uma correlação aos crimes contra a honra praticados pela internet dos delitos que ofendem bens imateriais.

- Quais tipos de crimes os infratores estão cometendo no espaço virtual?
- Será que esses crimes na internet realmente tem uma lei específica, e ela é cumprida?
- O código penal prevê algum tipo de pena para tais crimes?
- A Lei é rígida para os crimes contra a honra praticados na internet?

Assim nossa pesquisa tem como objetivo geral analisar o tratamento dos crimes cibernéticos no ordenamento jurídico brasileiro e a sua correlação com os crimes contra a honra previstos no Código Penal Brasileiro, fazendo uma breve análise a partir da Lei nº 12.737, de 30 de novembro de 2012.

E como objetivos específicos, analisar quais os tipos de crimes os infratores estão cometendo no espaço virtual, esclarecer se há uma lei específica para os crimes praticados na internet e Analisar de que modouma cooperação rápida e eficaz, das forças policiais e do judiciário, pode ser eficaz no combate aos crimes cibernéticos.

O trabalho será desenvolvido de acordo com o método indutivo, de classificação bibliográfica, visto que o presente trabalho busca apresentar, análises de doutrinadores e diversos fatos levantados com base em dados extraídos de sites de segurança nacional e patrimonial e por fim conseguir com que o leitor opte pela posição adotada no presente trabalho.

Gil explica o método indutivo como:

> O método indutivo procede inversamente ao dedutivo: parte do particular e coloca a generalização como um produto posterior do trabalho de coleta de dados particulares.De acordo com o raciocínio indutivo, a generalização não deve ser buscada aprioristicamente, mas constatada a partir da observação de casos concretos suficientemente confirmadores dessa realidade. (GIL, 2008, p.19)

Contamos coma lei n°12.737 de 30 de novembro de 2.012, conhecida com Carolina Dieckmann, após ser sancionada pela então presidente Dilma Rousseff, com propósito de proteger todo e qualquer cidadão de ataques cibernéticos, mais tarde mais conhecida como Marco Civil da Internet, com garantias, deveres, princípios e direitos.

> […] Um delito típico de internet seria quando uma pessoa se utiliza de um computador acessando a rede, invade outro computador e obtém, destrói, ou altera um arquivo pertencente ao sistema, ainda que não houvesse qualquer obtenção de vantagem patrimonial, mas tão somente a obtenção, destruição ou alteração de dados daquele sistema restrito – circunstância esta que já caracterizaria o tipo penal específico (QUEIROZ, 2008, p.174).

Quanto à natureza da pesquisa, esta se desenvolve pelo método bibliográfico, e não possui aplicabilidade específica. Gil(2008, p.69) afirma que,“a pesquisabibliográfica é retirada em artigos, pesquisas cientificas e materiais já publicados na internet”.

A referida lei criou tipos penais e estabeleceu uma proteção a mais para o “internauta”, termo utilizado, visto que os ataques são mais pelo o uso da internet, alguns artigos foram adicionados ao Código Penal após o Marco Civil em 2014, trazendo uma alteração para maior segurança do usuário. Vale salientar que cada um que acesse a internet tenha a responsabilidade de se resguardar diante da rede de dados, pois a internet é um serviço descentralizado em todo o mundo.

2.CAPITULO I

2.1 DOS CRIMES CIBERNÉTICOS (CONCEITO E CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS E LEI N°12.737 DE 30 DE NOVEMBRO DE 2.012)

Cyber crimes nada mais é do que condutas típicas, ilícitas e culpáveis praticada pela internet ou sistemas de informática, (CAPEZ, 2003). Esses crimes são invasões de sistema por meio de vírus, com roubo de dados pessoais, falsidade ideológica, acesso a informações pessoais etc. Os *cyber* crimes são debatidos e combatidos desde os anos 90, contudo não é fácil localizar o criminoso devido ao grande número de computadores pessoais, onde qualquer pessoa pode praticar esse tipo de crime mesmo do outro lado do planeta sem sequer conhecer a sua vitima ou sair de casa para praticar tal delito.

> 65% dos internautas já foram vitimas de ataques pela internet de alguma forma e esses dados só tende a aumentar pois a maior dificuldade de combater esses crimes é a falta de leis para punir de forma eficiente, vários países estão na luta contra os ataques". (NORTOM, SECUTIRY)

A forma "mais segura" de navegar na internet é sempre mantendo o antivírus atualizado, existem também algumas ferramentas que podem ser utilizadas como segurança do computador, além disso, é importante sempre atualizar seu sistema operacional para ficar livre de ataques.

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2- O 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3- Assim, o 'Crime de Informática' pressupõe dos elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4- A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5- Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, entre outros. (ROSA, 2002 apud SCHMIDT, 2014).

Abrir e-mails suspeitos, links de sites de lojas com valor muito atrativo, links com premiações, também são as maiores armas dos Crackersao clicar no link automaticamente o seu endereço de IP "Internet Protocol", o IP é um numero de serie que seu computador, por exemplo, quando envia informações para outro computador é utilizada uma espécie de codificação eletrônica (carta), o mesmo é grampeado e é onde começa toda a varredura no seu computador, celular ou tablet, por isso especialistas salientam que sempre é bom ter bastante cuidado nesse tipo de conteúdo.

Maria Eugenia Gonçalves Mendes, ano 2016, classifica os *cyber* crimes em três categorias, Puro, Misto e Comum. Já o criminoso que pratica esse tipo de crime está classificado em duas nomenclaturas, Interno e Externo.

A lei n°12.737 de 30 de novembro de 2012, conhecida como“Lei Carolina Dieckmann”, foi um grande passo para a segurança da era digital, mesmo tendo sido sancionada às pressas em tempo recorde, pela presidente da república, devido a uma violação do computador de uma atriz global. Essa lei estabeleceu algumas garantias, princípios, direitos e deveres para utilização da internet no Brasil, contudo mesmo com a lei sancionada, na prática nada mudou, considerando-se que a pena a ser cumprida é muito pequena e na maioria das vezes é impossível localizar os criminosos, devido à utilização de IPs falsos, o criminoso consegue se esconder e acessar a rede de qualquer pessoa do outro lado do país. O Brasil infelizmente está muito distante de ser uma potência mundial em relação a minimizar ataques virtuais, pelo contrário, está entre os 10 primeiros países com mais ataques virtuais do mundo.

A “Lei Carolina Dieckmann” acrescenta o artigo 54-A ao Código Penal, eu dispõe:

> 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 (planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737)

O crime só é consumado se o dispositivo for alheio, violação indevida sem justa causa, exemplo você destruiu um celular e alguém encontra e consegue recuperar os dados e faz a exposição de sua imagem.

2.2 CLASSIFICAÇÃO

Os Crimes cibernéticos são classificados em três tipos, são eles, puros, mistos e comuns, na maioria das vezes uma pessoa que foi “atacada” por algum tipo de vírus utiliza logo a expressão que foi hackeada, não sabendo ela que para cada tipo de crime existe uma denominação correta, na maioria dos casos o crime “puro” é o mais utilizado pelos crakers, com a intenção apenas de capturar os dados da vítima para posteriormente divulgar, como por exemplo, imagens pessoais, ou

conversas comprometedoras dessa maneiraameaça-lo de alguma forma para reaver alguma vantagem que no geral é financeira.

Atualmente, os dados são facilmente capturados, basta apenas um simples clique que você já está na mira de criminosos e como a lei para esse tipo de crime é muito aberta isso se torna ainda mais “normal” de acontecer.Conforme (SCHMIDT 2014),É o caso do vírus Melissa, que em 1999 causou um prejuízo de mais de US$ 80.000.000,00 (oitenta milhões de dólares), e em 2011 houve o caso do furto de dados, nomes, endereços e possivelmente detalhes de cartões de crédito de 77 milhões de usuários da *Playstation Network* (mundial).

> Trata-se de crime comum (aquele que pode ser praticado por qualquer pessoa), plurissubsistente (costuma se realizar por meio de vários atos), comissivo (decorre de uma atividade positiva do agente: “invadir”, “instalar”) e, excepcionalmente, comissivo por omissão (quando o resultado deveria ser impedido pelos garantes – art. 13, § 2º, do CP), de forma vinculada(somente pode ser cometido pelos meios de execução descritos no tipo penal) ou de forma livre(pode ser cometido por qualquer meio de execução), conforme o caso, formal (se consuma sem a produção do resultado naturalístico, embora ele possa ocorrer), instantâneo(a consumação não se prolonga no tempo), monossubjetivo (pode ser praticado por um único agente), simples (atinge um único bem jurídico, a inviolabilidade da intimidade e da vida privada da vítima) (Vicente de Paula Rodrigues Maggio (2013, [n.p.])

Um dos crimes mais praticados é o crime “puro”, quando o criminoso tem uma conduta ilícita contra o software ou hardware de um computador, como, por exemplo, uma invasão de um sistema de uma empresa privada, um furto de um simples HD de um setor público para beneficio próprio.

Outro crime é o “misto”, é a conduta em que o agente se esconde atrás de uma rede de comunicação “internet” ou sistemas para praticar delitos, como por exemplo, compras com dados clonados, transações de dinheiro por IP clonado e etc.

Por último, temos o crime comum, que são aqueles que se utilizamda internet para enviar e-mails, links, pornografia infantil ou qualquer outro tipo de conteúdo proibido de acordo com o Código Penal.

No momento atual temos um grande exemplo de crimes comum, o chamado “FAKE NEWS” onde é lançado um “viral” uma espécie de nota jogada na rede “internet”, noticias falsas de determinado assunto buscando na maioria das vezes denigri a imagem da vitima com informações caluniosas e expondo a pessoa ao ridículo.

Como identificar as chamadas *Fake News*? Considere a fonte, verifique o autor, leia mais, se tem fontes de apoio, verifique a data, uma piada ou sátira, se é preconceito e por fim consulte especialistas.

Os maiores exemplos de *Fake News* são nas eleições, onde determinado grupo, quer implantar na cabeça de outras pessoas a “verdadeira face do candidato”, de acordo com o jornal estadão.

> Segundo levantamento do Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (Gpopai), da Universidade de São Paulo (USP), cerca de 12 milhões de pessoas compartilharam *fakenews* no Brasil em junho deste ano. O levantamento, que monitorou 500 páginas digitais de conteúdo político falso ou distorcido, indica que tais notícias têm potencial para alcançar grande parte da população brasileira se considerada a média de 200 seguidores por usuário. (JORNAL O ESTADÃO 2018)

A internet é uma espécie de arma como qualquer outra, como, por exemplo, uma faca ou arma de fogo, porém como as leis para os crimes cibernéticos não são tão eficazes, qualquer internauta fica desprotegido de tais crimes.É necessário que o estado, ou órgãos fiscalizadores tomem uma atitude afim de que esse tipo de crime seja de fato fiscalizado, pois a cada dia que passa mais pessoas, órgãos e até mesmo o próprio estado sofre com constantes ataques de organizações criminosas.

Outro termo bastante confuso é a identificação dos infratores conhecido nacionalmente com “hacker”, porém existem duas denominações para os infratores desse tipo de ataque, são eles, os hacker e crakers.

Os hackers são conhecidos como (chapéus brancos), eles são aqueles que atacam sistemas de segurança de empresas, quebram senhas e modificam software, tudo isso para tentar corrigir falhas para que os criminosos não consigam invadir. Já o crakers, (chapéus negros) é o oposto, eles invadem sistemas, modificam senhas, clonam cartões, para se beneficiar de tal ato, os mesmo são comparados inclusive com terroristas, eles são mais conhecidos com “hacker” no senso comum.

> Substantivo de agente do v. tohack, ‘dar golpes cortantes (para abrir caminho)’, anteriormente o aplicado a programadores que trabalhavam por tentativa e erro; S.2 g. Inform. 1. Individuo hábil em enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes, gerar a partir de uma conexão remota em uma rede de computadores; violar de um sistema de computação. (FERREIRA, 1999)

2.3CRIMES PRÓPRIOS E IMPRÓPRIOS

Os crimes próprios só podem ser cometidos por determinada pessoa ou categorias de pessoas. São aqueles que em que o sistema informático do agente é o objeto e o meio do crime. (CAPEZ, 2009; SCHMIDT, 2014)

Os crimes cibernéticos impróprios seriam aqueles que atingem um bem jurídico comum, como o patrimônio, e utilizam dos sistemas informáticos apenas como meio de execução. (CAPEZ, 2009; SCHMIDT, 2014)

2.4 DOS CRIMES CONTRA A HONRA

A Honra é um bem inviolável segundo a Constituição Federal de 1988, no artigo 5º, um conceito para a honra é que a construímos a vida toda e que te torna merecedora de apreço e convívio social e que aumenta sua autoestima. Crimes contra a honra são aqueles que te põem em perigo e que de uma forma ou de outra deixa você frágil, atinge sua integridade e/ou incolumidade.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (CF88, BRASIL).

Temos no nosso Código Penal três classificações para crimes contra a honra, são elas, calúnia, difamação e injuria.

Calunia, quando você imputa para alguém algo que você não tem provas ou não viu, narrando um fato como uma espécie de “história”, julgando lhe de uma forma que possa o constranger de uma forma ou de outra e colocando a publico tal situação.

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos.

> **Exceção da verdade**
> § 3º - Admite-se a prova da verdade, salvo:
> I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
> II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
> III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível. (Código Penal, BRASIL 1940).

Como por exemplo, a divulgação de capturas de telas “prints” através do *whatsapp*, de uma conversa onde essas conversas foram manipuladas por aplicativos de edição visual com conteúdo que tenha claramente a intenção de incriminar alguém.

Difamação, quando você expõe a vida ou uma informação pessoa que não necessariamente precisa ser falsa a público, não precisa citar detalhes da situação, apenas expor a dignidade da pessoa ao ridículo.

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> **Exceção da verdade**
> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções. (Código Penal, BRASIL 1940).

Exemplo, divulgação de uma conversa pessoal, conversa essa real e verdadeira e expor a mesma para uma rede de dados, apenas com o intuito de expor a imagem da pessoa.

Injuria, caracteriza apenas pelo ato de você falar mal, insultar, da uma opinião duvidosa da dignidade da pessoa, não precisa ter fatos precisos, apenas informações genéricas da pessoa em questão.

> Art. 140 - Injuriar alguém, ofendendo- lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - no caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes: Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

> § 3o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:
> Pena - reclusão de um a três anos e multa. (Código Penal, BRASIL 1940).

Caracterizado por exemplo o fato de você publicar algo em rede social mensagens com apelidos, palavrões ou até mesmo questionar o sexo do individuo, com o intuito de que varias pessoas tenha conhecimento de tal fato.

3CAPITULO II

3.1 DIREITO À PRIVACIDADE

O direito à privacidade é assegurado pela Constituição Federal de 1988, no art. 5º, inciso X; são invioláveis a **intimidade**, a **vidaprivada**, a **honra** e a **imagem** das pessoas, um morto também tem esse direito assegurado. A indenização é um direito pelo dano material ou moral decorrente de sua violação, porém esse direito não é absoluto, em algumas situações esse direito pode ser quebrado, mas para esse direito ser quebrado por alguma intervenção o motivo deverá ter uma justificativa muito maior para que o direito seja afastado,esse direto abrange para a inviolabilidade domiciliar, escuta telefônica, quebra de sigilo bancário, direito à honra e a imagem, entre outros, decreto 678de 1992 no artigo 11 do Pacto de San José da Costa Rica garantem o respeito a honra e a dignidade.

> Apesar de erroneamente o direito a privacidade ser considerado por alguns, em relação aos interesses sociais, um mero capricho, uma vontade extravagante, para proteger uma demanda individualista, ele tem caráter não só individual, mas também social, pois colabora para a manutenção dos limites de toda uma sociedade perante um individuo, como salienta (VIDAL, 2010)

O direito a privacidade, “vida íntima ou vida privada”, é a faculdade que cada pessoa tem de impedir a intromissão de pessoas da família ou estranhos de querer invadir sua privacidade, atualmente não temos muita privacidade devido às redes sociais, mesmo colocando senhas em nossas“contas”, a cada aplicativo que instalamos principalmente no celular, damos permissão para tal aplicativo acessar nossos dados ou até mesmo permitir que acesse o nosso IP, (número de serie da

nossa rede), com isso nosso “sigilo” não é mais privado e mesmo sabendo dessas situações não existe um sansão que proíba esse tipo de procedimento adotado por lojas de aplicativos.

Um bom exemplo que podemos aplicar são as famosas *“Fake News”,* quando alguém divulga uma noticia falsa ea mesma é espalhada em segundos. Um período que se aborda muito sobre o assunto *Fake News* é o período de campanha eleitoral, onde candidatos de lados opostos tentam a qualquer custo disseminar notícias falsas do seu adversário, esse ano se falou bastante nas eleições da “*fakenews*”, haja vista que inúmeras vezes os candidatos a presidência constantemente reclamavam sobre essas noticias vindas de lados opostos.

Vale salientar que sua vida íntima é protegida constitucionalmente, como por exemplo, uma foto armazenada no seu computador ou smartphone, já sua vida exposta em rede social e divulgada para inúmeras pessoas não entra nessa proteção definida pela constituição.

3.2 SIGILO DE DADOS E INVIOLABILIDADE DO DOMICÍLIO E COMUNICAÇÃO

Com base na no inciso XI e XII do artigo 5º da Constituição Federal, qualquer tipo de violação, seja ela domiciliar, de dados ou de comunicação, faz jus a ligação com a intimidade e espécie de privacidade. O Sigilo de dados é uma questão bem complexa, pois a legislação brasileira não contempla como direito absoluto, o mesmo individuo pode ter quebra de sigilo bancário, ou ter sua residência invadida durante o dia mediante autorização judicial.

Interceptação telefônica ou gravação clandestina sãomeios bastante utilizados para quebra de sigilo, a diferença entre elas é que na interceptação, nenhum dos interlocutores sabem, já a gravação apenas um sabe, porém as duas formas são ilícitas e sem valor jurídico, mas esse tipo de procedimento pode se tornar licito contendo uma autorização judicial.

> É possível afirmar que a intimidade corresponde ao conjunto de informações da vida pessoal do indivíduo, hábitos, vícios, segredos desconhecidos até mesmo da própria família, como por exemplo, as preferências sexuais, dentre outros. Por outro lado, a vida privada está assentada no que acontece nas relações familiares e com terneiros, como interferir em empréstimo feito junto aos seus familiares ou obter informações sobre o saldo bancário do

> empregado, devendo ser preservado no anonimato o que ali ocorre. Dito isto, constata – se que o direito à intimidade se situa em um círculo concêntrico menor que o direito à vida privada. (QUEIROS, 2009)

A inviolabilidade é garantida a qualquer pessoa, qualquer individuo pode se comunicar com quem quer que seja, contudo o conteúdo dessa conversa não pode ser divulgado sem nenhum consentimento, (FREGADOLLE, 1998, P. 87) “Afirma que existem certas manifestações de pessoa que se destinam a permanecer inacessíveis ao conhecimento alheio, ou acessível apenas para um grupo reduzido de pessoas, a quem o sujeito permita tal comunicação”.

> **Divulgação de segredo**
> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
>
> Pena - detenção, de um a seis meses, ou multa.
>
> **Violação do segredo profissional**
>
> Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
>
> Pena - detenção, de três meses a um ano, ou multa.
>
> **Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

3.3 INVESTIGAÇÕES DOS CRIMES CYBERNETICOS

O Ministério Público tem uma equipe especifica que trata apenas crimes cibernéticos, ela é centro de apoio a diversos órgãos do estado, que conta com policiais, analistas, investigadores e promotores.

Alguns sites inclusive fazendo um trabalhopreventivo junto a algumas escolas para orientar os alunos e os seus pais de como se prevenir contra ataques na internet e mantendo-se sempre em alerta, porque qualquer clique automaticamente você já está “grampeado” na rede de computadores.

Mesmo com várias formas se se prevenir temos uma grande dificuldade em localizar invasores, pois não existe legislação que obriga o provedor a fornecer as informações do autor de tal crime, sendo assim fica muito difícil que o MP trabalhe para combater essas irregularidades na rede mundial de computadores.

Recentemente, o MPSP e a Microsoft Brasil anunciaram uma parceria para combater os crimes praticados na internet, com isso os promotores passaram a ter um treinamento específico para trabalhar com ferramentas mais eficazes para combater tais crimes, a Microsoft se compromete em sempre encaminhar relatórios com “tendências” desse tipo de crime.

> A Microsoft elabora seus relatórios a partir de informações de segurança de 1 bilhão de dispositivos Windows atualizados mensalmente, que somam 200 bilhões de e-mails rastreados por ameaças virtuais, como phishing e malware, e 300 bilhões de acessos mensais a serviços. (MICROSOFT BRASIL)

4CAPÍTULO III

4.1 CRIMES CONTRA A HONRA COMETIDOS NO ESPAÇO VIRTUAL QUE TIVERAM GRANDE REPERCUSSÃO NA MÍDIA BRASILEIRA

Nos dias atuais, as redes sociais, o ambiente virtual se tornou um ambiente de propagação de *fakenews* e práticas de outra condutas, que em determinados casos, podem configurar a prática de crime contra a honra.

Alguns desses casos ganham bastante notoriedade, principalmente quando envolvem políticos, artistas, atletas famosos etc. Neste capítulo, vamos apresentar e discutir como os crimes contra a honra se configuram em fatos que tiveram grande repercussão midiática.

4.1.1CASO MARIELLE FRANCO

Marielle Franco era vereadora do Rio de Janeiro, (PSOL), Socióloga com mestrado em Administração Pública, foi eleita Vereadora da Câmara do Rio de Janeiro pelo PSOL, com 46.502 votos, foi também Presidente da Comissão da Mulher da Câmara, no dia 14/03/2018 foi assassinada em um atentado ao carro onde estava morta a tiros no centro da cidade, o motorista do carro Anderson Pedro, também morreu, a policia suspeita de execução como principal hipótese.

A vereadora Marielle foi assassinada após sair de um debate promovido pelo Psol por volta das 21h, quando um carro Cobalt a segue, um outro carro também se uniu na perseguição, por voltas das 21h30minh ela é atingida por 13 disparos, sendo que 9 atingi a lataria e 4 o vidro. Marielle e o motorista são baleados e morrem, a arma do crime foi uma pistola 9 mm, com munições de um lote vendido a Policia Federal DF em 2006, segundo o ministro de segurança essas munições foram roubadas de uma agência do correios da Paraíba.

A polícia afirma que os assassinos observaram onde a vereadora estava exatamente, visto que ela estava no banco de trás, algo raro, e os vidros do carro revestidos, os criminosos agiram sem levar nada.

A irmã e a viúva de Marielle pedem na justiça, indenização de R$ 1milhão por notícias falsas publicadas no *Youtube*, ação movida contra o Google que é a quem pertence o canal, porém o juiz que determina o valor da multa. As autoras alegam que enxurradas de notícias falsas foram espalhadas na rede de internet, mensagens essas com discursos de ódio e calúnia contra Marielle. Segundo os familiares, mais de 20 milhões de pessoas foram alcançadas com essas publicações. Logo no início da petição, utilizam a frase usada por Joseph Goebbels, ministro da propaganda de

Hitler; "Uma mentira repetida mil vezes torna-se verdade", com isso mostra a aflição das autoras para que todas as publicações sejam retiradas do ar.

A mensagem que mais gerou repercussão foi a do Deputado Federal Aberto Fraga (DEM). De acordo com o G1 o deputado Alberto Fraga diz:

> “Conheçam o novo mito da esquerda, Marielle Franco. Engravidou aos 16 anos, ex esposa do Marcinho VP, usuária de maconha, defensora de facção rival e eleita pelo Comando Vermelho, exonerou recentemente 6 funcionários, mas quem a matou foi a PM.” (ALBERTO FRAGA, G1 2018)

Nesta declaração, percebemos que houve a configuração da calúnia, por imputar a Marielle práticas criminosas, bem como difamação, ao associar a vereadora a práticas ofensivas a sua reputação.

Marilia Castro Neves, desembargadora do Rio de Janeiro, também publicou no *facebook*que Mariele foi eleito pelo comando vermelho (facção criminosa do RJ)

> Mensagem: “A questão é que a tal da Marielle não era apenas uma "lutadora"; ela estava engajada com bandidos! Foi eleita pelo Comando Vermelho e descumpriu "compromissos" assumidos com seus apoiadores. Ela, mais do que qualquer outra pessoa "longe da favela" sabe como são cobradas as dívidas pelos grupos entre os quais ela transacionava. Até nós sabemos disso. A verdade é que jamais saberemos ao certo o que determinou a morte da vereadora mas temos certeza de que seu comportamento, ditado por seu engajamento político, foi determinante para seu trágico fim. Qualquer outra coisa diversa é mimimi da esquerda tentando agregar valor a um cadáver tão comum quanto qualquer outro. (MARILIA CASTRO NEVES)

O réu do processo (GOOGLE BRASIL LTDA) se defendeu utilizando o argumento de que, se for retirada todas as publicações da plataforma, estará tirando o direito de liberdade de expressão das pessoas, mesmo assim foi retirado 40 vídeos intitulados com o nome da vitima, e se ausentou de qualquer material postado internacionalmente.

Lei nº 12.965/14, Marco Civil na Internet, estabelece que:

> "Art. 19. 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.

No mesmo caso ocorreram também representações contra o Deputado Federam Alberto Fraga e a Desembargadora Marilia Castro, ambos acusados pelo crime de calúnia art. 138, difamação art. 139 e injúria art. 140 do código penal, por postarem *fakenews* em suas redes sociais, o processo contra o deputado já se encontra arquivado.

Mesmo que haja constitucionalmente o direito de expressão não é permitido difamar, injuriar ou ofender pessoas nas redes sociais, mas o pedido de indenização deve a ver um valor que condiz com o fato narrado seguindo o passo de apenas tirar uma captura da tela e levar a um cartório mais próximo para realização de ata notarial para servir como prova.

4.1.2 CASO WESLEY SAFADÃO E THYANNE DANTAS

O cantor “Wesley Safadão” há alguns anos se tornou um dos cantores mais famosos do Brasil na atualidade. No seu caso,a polêmica começou depois que o cantor pediu revisão da pensão que pagava ao filho, Yhudi. Na época, ele pagava 9 salários mínimos de pensão. Após o processo foi definido o aumento para 40 salários, sua ex esposa MileideMihaile começou a dar uma série de entrevistas, ocasião em que falava abertamente que na época em que estava casada com o cantor foi traída. A partir disto começou uma série de ataques sobre o cantor e sua atual esposa Thyane Dantas.

Um grupo no aplicativo *Whastsap* foi criado por algumas mulheres com a intenção de denegrir a imagem do cantor e principalmente de sua atual esposa Thyane, com o propósito, segundo relatos de algumas delas, apenas de ver o sofrimento do casal. Diante dos fatos, Thyane e Wesley iniciaram uma busca aos Haters(os que odeiam) nomenclaturas utilizadas para definir pessoas que fazem *bullying* virtual, passaram a tirar capturas de telas, armazenar áudios de conversas vazadas e áudios manipulados com as vozes das vítimas. A ex-esposa do cantor afirma não ter nada a ver com os grupos e nem com os ataques, porém uma das envolvidas com o nome de Katyelle afirma que Mileide passava informações sobre o caso e com total intuito de manchar a reputação do casal.

Wesley e Thyane já tem 4 ações judiciais em curso, com 50 depoimentos, várias pericias em contas de *Icloud, WhatsApp, Facebook*e *Instagram*. Quebra de sigilo telefônico e cerca de 78 contas no *instagram*identificadas, mais de 60 horas de áudio em conversas recuperadas e todos os inquéritos estão em curso.

Sabemos que não existe uma legislação específica para quem produziu as notícias, mas existem alguns meio de tirar as noticias do ar por meio de autorização judicial, com base na lei do Marco Civil na internet no artigo 19.

> O provedor de aplicações só será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial especifica, não tomar as providencias 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.

No caso acima citado, algumas pessoasestão sendo processadas com ação criminal por calúnia, injúria e difamação, a pena para esse tipo de crime varia de 3 meses a 3 anos e dependendo do caso pode ser trocado por serviço comunitário e pagamento de indenização.

4.1.3 CASO ELEIÇÕES 2018(JAIR BOLSONARO X FERNANDO HADDAD)

O maior tema da eleição 2018 não foram os projetos dos candidatos, rivalidade entre os partidos e sim, as*Fake News* que a todo momento eram citados de um lado e de outro, o candidato Fernando Haddad afirmou ser alvo de Fake News “comprada” pelo presidente eleito Jair Bolsonaro. Haddad afirma que Bolsonaro teria pactuado com empresários para comprar e disparar mensagem no W*hatsApp* difamando a sua idoneidade e espalhando boatos e informações negativas tanto suas, quanto do seu partido, essa prática inclusive se enquadraria como caixa dois por serem doações não declaradas a Justiça Eleitoral, esse caso específico foi o assunto mais comentado nos últimos dias que em fração de segundos após a noticia publicada praticamente todo o brasil ficou sabendo de tal fato.

> Não tem prova de nada, é a *Folha* jogando nesse time do Haddad. Nós não precisamos de fakenews para combater o Haddad, as

> verdades são mais que suficientes. Todos se lembram de 13 anos do PT, aí sim: caixa dois, corrupção generalizada, assalto a estatais, quebra de fundos de pensão, doação de dinheiro do BNDES a ditaduras. Esse é o PT, nós não precisamos fazer fakenews contra eles", (declarou Jair Bolsonaro em vídeo no Instagram).

Nesse caso em questão, se o presidente eleito "Bolsonaro", fosse condenado, este teria sua candidatura impugnada, iria responder pelos crimes de caixa dois art. 350 do código eleitoral, organização criminosa art. 1º lei nº 12.850/2013 e por fim calúnia, difamação e injúria que estão dispostos nos respectivos artigos, 138, 139 e 140 do código penal.

O Partido dos trabalhadores (PT), também acionou a Justiça Eleitoral para que fosse retirado do ar cerca de 200 conteúdos apontados como *fake News* das redes sociais.

5CONCLUSÃO

Este estudo teve com base a identificação de um conjunto de termos que pertencem aos crimes cibernéticos e que há décadas que esse conjunto de crimes acontecem, mas ainda não temos uma forma concreta de combatê-lo.

Esse estudo serve como base para que usuários da web tenha como apoio para se prevenir de possíveis invasores, que sirva como um norte para novos estudos de estudantes e pesquisadores, haja vista que é um tema promissor para novos estudos técnicos.

É de suma importância que o combate dos crimes contra a honra no espaço virtual, a partir de "*Fake News*" que são divulgadas com a intenção apenas de expor e/ou enganar uma terceira pessoa afim de que a mesma venha a mídia ridicularizada causando sérios transtornos a ela e até mesmo a família, vimos que o provedor de internet só pode retirar a publicação do ar através de medida judicial, porém leva bastante tempo e a notícia já se tem espalhado e gerado dano a honra da vítima.

Foram identificados os tipos de crimes, tipos de invasores e leis vigentes no país, afim de que o leitor possa saber identificar qual tipo de ataque ele está recebendo e qual melhor opção do mesmo se defender.

Os crimes cibernéticos são uma conduta humana que através de sistemas informatizados, pratica atos ilícitos para atingir, defraudar, expor a dignidade, bem como difamar, caluniar ou injuriar uma terceira pessoa um alvo e que infelizmente ainda não contamos com uma rigorosa legislação para tratar desse crime. Temos algumas leis, mas, como visto a cima é muito difícil localizar o infrator, pois os provedores não são obrigados a revelar o endereço e a identidade do criminoso e a cada dia que passa através de meios tecnológicos os infratores se escondem ainda mais atrás de máquina e assim podem navegar anonimamente dificultando cada vez mais o trabalho de investigação.

É necessário urgentemente uma lei mais rígida para uma pena mais segura para os infratores visto que a pena é ainda pequena para um crime de expressão tão grande.

Ainda vimos que os crimes cibernéticos e crimes contra a honra quase não tem punibilidade visto que são temas muitos novos e o estado quase nunca consegue punir com rigidez por falta de uma legislação específica nova e eficaz, haja vista que a nossa atual legislação é muito antiga e omissa para esse tipo de crime. O Brasil ainda está em fase de crescimento comparado a outros países que contam com diversos recursos e tecnologias para combater os crimes cibernéticos.

6 REFERÊNCIAS

ACS., **Direito à Intimidade e Privacidade - Andréa Neves Gonzaga Marques** 18 de abril de 2010. Disponível em: <http://www.tjdft.jus.br/institucional/imprensa/artigos/2010/direito-a-intimidade-e-privacidade-andrea-neves-gonzaga-marques> acesso em: 15 de outubro de 2018.

CAPEZ, Fernando.,**Curso de Direito Penal.** 13. ed. São Paulo: Saraiva, 2009. v. 1.

Código Penal, BRASIL 1940

CONSTITUIÇÃO FEDERAL.,1988, BRASIL.

DIGITAL, C., **Wesley Safadão abre o jogo e diz que traiu Thyane com Mileide**26 de novembro de 2018. Disponível em:<https://caras.uol.com.br/tv/wesley-safadao-abre-o-jogo-com-leo-dias-com-polemica-e-diz-que-traiu-thyane-dantas-com-mileide-mihaile.phtml>. acesso em: 28 de novembro de 2018.

DUARTE, Adrien Carlos, **Marco Civil da Internet: O que é e o que Muda na Sua Vida.** [2016]. Disponível em: <https://www.oficinadanet.com.br/post/12558-o-marco-civil-da-internet-foi-aprovado-entenda-o-que-e-e-o-que-muda-na-sua-vida>. Acesso em 25 de novembro de 2018.

FBI. G., **Cyber Crime,**Disponível em:**<**https://www.fbi.gov/investigate/cyber>, acesso em: 07 de outubro de 2018.

FERREIRA, M. C.,**Lições de Direito ..Manual de Direito *Penal*: parte geral, vol. 1. 6.ª Ed,** São Paulo Saraiva, 1999/2000.

FREGADOLLE, L.., **O Direito À Intimidade e a Prova Ilícita** 1998, P. 87.

G1., **Assassinato de Marielle Franco: o que se sabe sobre o crime 15 de março de 2018.**Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/assassinato-da-vereadora-marielle-o-que-se-sabe-sobre-o-crime.ghtml. acesso em: 16 de novembro de 2018.

G1.,**Marielle engravidou aos 16? Foi casada com o traficante Marcinho VP? Ignorava as mortes de policiais? Não é verdade! 1**9 de março de 2018. Disponível em? https://g1.globo.com/e-ou-nao-e/noticia/marielle-engravidou-aos-16-foi-casada-com-o-traficante-marcinho-vp-ignorava-as-mortes-de-policiais-nao-e-verdade.ghtml acesso em: 16 de novembro de 2018.

G1**., Conselho arquiva processo de deputado que divulgou fakenews sobre** Marielle 29 de maio de 2018.Disponível em: <https://g1.globo.com/politica/noticia/conselho-arquiva-processo-de-deputado-que-divulgou-fake-news-sobre-marielle-franco.ghtml>. acesso em: 17 de novembro de 2018.

GIL, A.C., **Metodos e Tecnicas de Pesquisa Social,** 2008, p.19.

GIL, A.C.,**Metodos e Tecnicas de Pesquisa Social,** 2008, p.69.

HAJE, L. NOTICIAS, C. **Brasil está atrasado em estratégias de combate a crimes cibernético.**15 de março de 2013.Disponível em: <*http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/437788-BRASIL-ESTA-ATRASADO-EM-ESTRATEGIAS-DE-COMBATE-A-CRIMES-CIBERNETICOS.html*>.acesso em: 08 de novembro de 2018.

KLEINA, N., **7 maneiras de ser hackeado facilmente,** 19 de dezembro de 2011. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/16814-7-maneiras-de-ser-hackeado-facilmente.htm>.Acesso em: 07 de outubro de 2018.

LENZI, R., **Aplicação da cyber inteligência no combate aos crimes cibernéticos.** feveireiro de 2018. Disponível em:<https://jus.com.br/artigos/64207/aplicacao-da-cyber-inteligencia-no-combate-aos-crimes-ciberneticos> Acesso em: 06 de novembro de 2018.

MAGGIO, V. P. R.,**Infanticídio e a morte,** 2013.

MAZZILLI. E.R.A**., CRIMES CONTRA A HONRA NO CÓDIGO PENAL BRASILEIRO.** Disponível em:**<**https://docplayer.com.br/1849661-Crimes-contra-a-honra-no-codigo-penal-brasileiro.html#> Acessado em: 02 de novembro de 2018.

MORETTI**, I., A metodologia de pesquisa deve ser apresentada com propósito, tipo de abordagem e procedimentos.** 26 de julho de 2018. Disponível em: <https://viacarreira.com/metodologia-de-pesquisa-do-tcc-110040/>Acesso em 09 de novembro de 2018.

MENDES, M. E. G., VIEIRA, N. B., **Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Especifica.** [200-?]. Disponível em: http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2., Acesso em 01 de novembro de 2018.

MONNERAT, A., RIGA, M., RAMOS, P., **Fakenews devem causar impacto em eleições de 2018.**Disponível em: <http://infograficos.estadao.com.br/focas/politico-em-construcao/materia/fake-news-devem-causar-impacto-em-eleicoes-de-2018>Acesso em: 15 de novembro de 2018.

NONN A.,**RESUMO OAB – Penal – Crimes contra a Honra**Disponível em: <https://amandanonn.wordpress.com/2015/08/18/resumo-oab-penal-crimes-contra-a-honra/>Acesso em: 9 de outubro de 2018.

planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737

Presidência da República Casa Civil. Disponível em:**<**http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>,Acesso em 1 de novembro de 2018.

QUEIROZ, A., **Curso de Direito Penal** (Teoria Geral), 2008, p.174.

REDAÇÃO., **O que é crime cibernético** ?.Disponível em: <https://canaltech.com.br/seguranca/O-que-e-cibercrime/> Acesso em: 08 de outubro de 2018

RESUMO DE DIREITO PENAL IV- CRIMES CONTRA A HONRA. Disponível em: <https://www.passeidireto.com/arquivo/10866669/resumo-de-direito-penal-iv--crimes-contra-a-honra> Acesso em: 7 de outrubro de 2018

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002.

SCHMIDT, Guilherme. **Crimes cibernéticos. Jus Brasil,** 2014. Disponível em: <http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos/> Acesso em: 01 outubro. 2018.

SIGNIFICADOS., **Significado de Fake News,**26 de abril de 2018.Disponível em: <https://www.significados.com.br/fake-news/> aceso em: 09 de novembro de 2018.

SOUZA. H. T., FERREIRA F.G.C O., **Direito Penal e os crimes cibernéticos.** Outubro de 2014.Disponível em: <https://jus.com.br/artigos/32681/o-direito-penal-e-os-crimes-ciberneticos> Acesso em: 9 de outrubro de 2018

VEIGA, F., **10 tipos de vírus de computador – Quais são os tipos de vírus de PC,** 10 fevereiro de 2013.Disponível em: http://www.vejaisso.com/10-tipos-de-virus-de-computador-sintomas-do-pc-com-virus-e-malwares/ acesso em: 7 de outro de 2018.

VEJA., **Não precisamos de fakenews para combater Haddad', diz Bolsonaro**.,18 de outubro de 2018.Disponível em:<https://veja.abril.com.br/politica/nao-precisamos-de-fake-news-para-combater-haddad-diz-bolsonaro/> 30 de novembro de 2018.

VIDAL, G R. **Regulação do direito à privacidade na internet: o papel da arquitetura. Jus Navigandi, Teresina**, ano 15, n 2688 10 de novembro de 2010.Disponível em: <http://jus.com.br/revista/texto/17798>. Acesso em: 05 Outubro 2018.

VICIOUS, S., **Ministério Público do Estado de São Paulo e Microsoft Brasil anunciam parceria para combate ao cibercrime,.**28 de fevereiro de 2018.Disponível em: <https://www.baboo.com.br/seguranca/ministerio-publico-do-estado-de-sao-paulo-e-microsoft-brasil-anunciam-parceria-para-combate-ao-

cibercrime/?doing_wp_cron=1542300150.9835960865020751953125> Acesso em 07 de outubro de 2018.