UNIVERSIDADE FEDERAL DE ALAGOAS

INSTITUTO DE COMPUTAÇÃO

CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

EUDIANE SILVA DE ALMEIDA
MARCOS VALÉRIO DA SILVA

CRIMES INFORMÁTICOS: UM BREVE ESTUDO ACERCA DA LEGISLAÇÃO BRASILEIRA ATUAL

30 de julho de 2020
Maragogi – AL
2020

EUDIANE SILVA DE ALMEIDA
MARCOS VALÉRIO DA SILVA

CRIMES INFORMÁTICOS: UM BREVE ESTUDO ACERCA DA LEGISLAÇÃO BRASILEIRA ATUAL

Trabalho de Conclusão de Curso submetido ao curso de Sistemas de Informação do Instituto de Computação da Universidade Federal de Alagoas como requisito parcial para a obtenção do Grau de Bacharel em Sistemas de Informação.

Orientador: Prof.º Me. Petrúcio Antônio Medeiros Barros

Co-orientadora: Prof.ª MSc. Regina Maria Ferreira da Silva Lima

30 de julho de 2020
Maragogi – AL
2020

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecária: Taciana Sousa dos Santos – CRB-4 – 2062

A447c Almeida, Eudiane Silva de.
Crimes informáticos: um breve estudo acerca da legislação brasileira atual / Eudiane Silva de Almeida, Marcos Valério da Silva. – 2020.
67 f.

Orientador: Petrúcio Antônio Medeiros Barros.
Coorientadora: Regina Maria Ferreira da Silva Lima.
Monografia (Trabalho de Conclusão de Curso em Sistemas de Informação: Bacharelado) – Universidade Federal de Alagoas. Instituto de Computação. Universidade Aberta do Brasil. Maragogi, 2020.

Bibliografia: f. 59-67.

1. Crimes cibernéticos. 2. Segurança cibernética. 3. Legislação processual penal brasileira. I. Silva, Marcos Valério da. II. Título.

CDU: 007: 34

EUDIANE SILVA DE ALMEIDA
MARCOS VALÉRIO DA SILVA

CRIMES INFORMÁTICOS: UM BREVE ESTUDO ACERCA DA LEGISLAÇÃO BRASILEIRA ATUAL

Trabalho de Conclusão de Curso (TCC) foi julgado adequado para obtenção do Título de Bacharel em Sistemas de Informação e aprovado em sua forma final pelo Instituto de Computação da Universidade Federal de Alagoas.
Maceió, ___ de _____ de 2020.

Banca Examinadora:

Prof. Regina Maria Ferreira da Silva Lima MSc.
Co-Orientadora - UFAL

Prof. Petrúcio Antônio Medeiros Barros, Me.
Orientador - UFAL

Prof. Almir Pereira Guimarães, Dr.
UFAL

Prof. Marcus de Melo Braga, Dr.
UFAL

DEDICATÓRIA

Primeiramente sou grato ao meu Criador YHWH (YAUH), por ter me permitido chegar até momento importante de minha jornada, á meus pais, à minha esposa, Jéssica Nogueira, que me apoiaram ao máximo, do início ao fim do curso, dedico este trabalho.

DEDICATÓRIA

Em primeiro lugar ao Eterno que me iluminou durante esta caminhada. Minha mãe Elzenite, seu cuidado e dedicação foi que me deram, em alguns momentos, a esperança para seguir meu pai Moisés, sua presença significou segurança nessa caminhada.

A vocês dedico este trabalho.

AGRADECIMENTOS

Primeiramente ao Criador que permitiu que tudo isso acontecesse, não somente nos anos acadêmicos, mas em todos os momentos. É o maior mestre que alguém pode conhecer.

À Universidade Federal de Alagoas, seu corpo docente, direção e administração pela oportunidade de fazer o curso.

Ao professor Petrucio Antônio Medeiros Barros, pela orientação, seu tempo, apoio e confiança.

A nossa tutora online e co-orientadora Regina Maria Ferreira da Silva Lima, pelo suporte, disponibilidade, correções e incentivo.

Por fim, a todos que direta o indiretamente fizeram parte de nossa formação, o nosso muito obrigado.

RESUMO

O presente trabalho tem como escopo verificar se existe proteção adequada para as vítimas de crimes cibernéticos. Trata-se de uma pesquisa de natureza essencialmente bibliográfica, realizada através de literaturas publicadas em livros, artigos de revistas impressas e/ou eletrônicas, bem como de natureza qualitativa, consistente na interpretação e análise crítica da temática proposta, capaz de atender os objetivos da pesquisa. O estudo evidenciou que o Brasil tem uma lei que trata da Política Cibernética de Defesa no âmbito nacional, além de uma série de normas legais que visam amparar as vítimas de crimes cibernéticos. Para além das sanções no âmbito penal, existem medidas sancionatórias cabíveis na esfera jurídica civil, normalmente consistentes em pagamento de indenizações por danos morais e/ou materiais suportados pela vítima, assim como a obrigatoriedade dos provedores de internet de retirar da rede as páginas ou notícias ensejadoras de situações vexatórias e de consequentes danos morais. Porém, há necessidade de uma melhor aplicação da legislação, para melhor sucesso na autuação e punição de casos cometidos.

Palavras-chave: Crimes cibernéticos, Proteção, Danos; Legislação Brasileira.

ABSTRACT

This current work has as its objective identify whether there's adequares protection for victims of cybernetic crimes. This work is essentially bibliographic, done through research from literatures published in books, articles from magazines and/or electronic magazines, as well as qualitative, based on interpreting and critically analysing the proposed theme, capable of meeting the requirements of the research. The study showed that Brazil has a law that deals with Cyber Defense Policy at the national level, in addition to a series of legal rules that aim to protect victims of cybercrimes. In addition to the penalties in the criminal sanctions, there are sanctioning measures applicable in the legal sphere, usually consisting of the payment of indemnities for moral/material damage, as well as the internet providers responsibility of taking down the pages of unwanted news and consequent moral damage. However, there's need of a better application of the legislation, for success in assessment and punishment of committed crimes.

Keywords: Cybercrimes, Protection, Damage; Brazilian legislation.

SUMÁRIO

1. INTRODUÇÃO

O mundo está passando por transformações significativas nesta era da informação, que sofre alterações constantes em todas as áreas do conhecimento humano, inclusive no âmbito jurídico, em relação aos direitos e deveres.

A revolução digital consentiu para que países como o Brasil fossem integrados ao mundo globalizado, trazendo muitos benefícios para a sociedade Brasileira, mas junto com o advento da internet e com a imensa quantidade de informações disponíveis, algumas pessoas tornaram-se alvos de criminosos que se apoderam dessas facilidades e cometem os chamados crimes cibernéticos ou crimes informáticos (TRUZZI, DAOUN 2015).

Segundo Wendt e Nogueira (2013), os termos crimes cibernéticos, crimes virtuais, crimes de alta tecnologia, cibercrimes, crimes digitais, crimes de informática dentre outros termos, são modalidades de crimes cometidos por meios eletrônicos.

O termo crime cibernético (cybercrime) surgiu no final da década de 1990, em Lyon, na França, depois de uma reunião do subgrupo G8 das nações que analisaram e discutiram sobre os crimes promovidos por meios eletrônicos ou mediante a disseminação de informações pela internet (MORAES PEREIRA, 2010).

No Brasil, os Tribunais Superiores e o Poder Judiciário como um todo têm recebido demandas constantes acerca de casos em que há a reivindicação de indenizações em virtude da prática dos crimes cibernéticos, o que requer dos julgadores estudo, uma maior atenção e eficiência para apreciar e resolver tais conflitos.

Estudiosos da área jurídica também vêm se debruçando sobre a temática da responsabilização civil dos autores de crimes cometidos via web, ao ponto de haver instruções no site oficial do Conselho Nacional de Justiça acerca do reconhecimento, tipificação legal e denúncia dos citados crimes (CNJ, 2018), assim como já existem varas judiciais especializadas em crimes cibernéticos, a exemplo de uma vara federal especializada em crimes cibernéticos, existente em Minas Gerais desde 2018 (CONSULTOR JURÍDICO², 2018).

Essa responsabilização se dá por meio do dever de indenizar, nos termos do art. 927, cumulado com o art. 186 do Código Civil de 2002, transcritos abaixo, como uma reparação dos danos sofridos ou suportados pela vítima dos delitos. Além da sanção penal, é possível sim imputar a responsabilidade civil ou patrimonial aos sujeitos infratores, pois, uma vez causado dano a alguém, o legislador afirma que há a prática de ato ilícito, *in verbis*: “Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito” (BRASIL[1], 2020, p. 17). E, em havendo a prática do ato ilícito, eis que emerge o dever de indenizar para o autor do dano, nos termos da Lei: “Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo” (BRASIL[1], 2020, p. 67).

O motivo para que fossem tipificados os crimes cibernéticos foi justamente a necessidade de se proteger os cidadãos, dando lugar à defesa dos direitos da personalidade na web, direitos estes que são inerentes ao homem, à vida de cada ser humano. Os direitos da personalidade humana surgiram para proteger e resguardar os cidadãos contra o poder estatal, sendo fruto de muitas lutas e reivindicações sociais em contraposição aos atos desumanos, tornando estes independentes de positivação, pois são direitos humanos indisponíveis. “A sua fonte primordial é o jus-naturalismo, do qual acredita que o direito, a moral e a justiça são mandamentos dados por Deus e não pelo Estado” (GONZAGA, 2017).

Atualmente temos resultados positivos no que se refere às Cartas internacionais de Direitos Humanos, nas Constituições de todos os países e nas leis infraconstitucionais. No Brasil, por exemplo, temos o Código Civil, o qual traz entre os artigos 11 e 21 os citados direitos da personalidade que visa zelar pela preservação do individuo de uma maneira que ele possa viver com uma melhor qualidade de vida e possa recorrer á justiça por todo tipo de difamação, calúnia, todo tipo de bullying e preconceitos (JUS, 2017).

Diversos acontecimentos da história mundial contribuíram para que hoje o Direito Privado tutelasse a pessoa humana acima do patrimônio. Existem diversas teorias do nascimento de tais direitos, a primeira foi no Código de Hamurabi, o qual se podia observar que o homem já era protegido juntamente com o código de conduta ou Torah (Lei) que de acordo com os judeus foi dada por YHWH (YAUH)

á Moisés e escrita no Livro de SHEMÔT (ÊXODO, Cap.: 20 vers. 1-17), onde está registrado um conjunto de leis, com o intuito de proteger os indivíduos.

Ademais, no âmbito internacional, pode-se vislumbrar a proteção aos direitos da personalidade em vários documentos normativos, a exemplo da Declaração dos Direitos do Homem e do Cidadão, de 1789, proclamada durante a Revolução Francesa; a Declaração Universal dos Direitos do Homem, de 1948, proclamada no período posterior à segunda Grande Guerra Mundial; a Convenção Europeia dos Direitos Humanos, datada de 1950, dentre outras cartas internacionais (AMARAL, 2004).

De acordo com Delgado (2005, p.6), “os direitos da personalidade são direitos atinentes à tutela da pessoa humana, considerados essenciais à sua dignidade e integridade”. Por sua vez, França (1981, p. 5), os define como sendo “as faculdades jurídicas cujo objeto são os diversos aspectos da própria pessoa do sujeito, bem assim seus prolongamentos e projeções”. Nesse sentido, pode-se afirmar, na concepção de Delgado (2005, p.6), que:

> “Os direitos da personalidade são direitos inerentes e essenciais à pessoa humana, decorrentes de sua exclusiva humanidade, e que protegem todas as suas projeções, nos planos físico ou espiritual, possibilitando, assim, ao ser humano, a defesa daquilo que lhe é próprio (honra, vida, liberdade, intimidade, privacidade, etc.)”.

Ressalte-se que os direitos da personalidade mais ofendidos por meio dos crimes praticados na internet são: a honra, a boa fama, a respeitabilidade, o direito à privacidade ou a intimidade.

O que se propõe estudar neste trabalho é justamente sobre os crimes cibernéticos, que prejudicam milhares de pessoas todos os dias e de várias formas.

O trabalho foi dividido em duas partes: 1) a fundamentação teórica que trata sobre os crimes informáticos numa perspectiva que conceitua os crimes cibernéticos; 2) Soluções sobre o tema discutido inerente á Legislação Brasileira atual que compõe a nossa sociedade.

Assim, no segundo capítulo será realizada uma revisão de literatura sobre a responsabilidade ou punição dos infratores na web e sobre as leis vigentes no país; no terceiro capítulo será explanado acerca da sociedade em rede e do confronto entre a liberdade de expressão e o direito à privacidade nas redes sociais; no quarto capítulo, será explanada, em linhas gerais, a responsabilidade civil, para fins de se compreender como se dá a responsabilização no âmbito cível para os autores dos citados crimes, assim como será explanado acerca dos direitos de personalidade; no quinto capítulo, será realizado um breve esboço histórico dos crimes cibernéticos e as suas várias espécies; no capítulo sexto, serão abordados os aspectos jurídico-penais relacionados aos crimes informáticos.

Trata-se de uma pesquisa de natureza essencialmente bibliográfica, realizada através de literaturas publicadas em livros, artigos de revistas impressas e/ou eletrônicas, bem como de natureza qualitativa, consistente na interpretação e análise crítica da temática proposta, capaz de atender os objetivos da pesquisa.

1.1 JUSTIFICATIVA

Em 2018 o Brasil registrou um aumento de 109,5% em denúncias de crimes informáticos. Segundo a informação divulgada pela Safernet Brasil em 2019. A Safernet é uma associação civil de direito privado. Estes dados foram levantados em parceria com o Ministério Público Federal. Foram 133.732 queixas em 2018, de ante 63.698 de 2017 (PODER 360, 2019).

Diante de tantos crimes virtuais fez-se necessário este trabalho, com objetivo de fazer um estudo acerca da legislação brasileira e verificar se existem punições adequadas para as vítimas de crimes informáticos.

2. REVISÃO DE LITERATURA

Não se pode negar que a revolução digital consentiu para que países como o Brasil fossem integrados ao mundo globalizado em seus variados aspectos. Porém esta tecnologia não se limita a apenas benefícios para a comunidade Brasileira e a sociedade em geral. Muitos crimes surgiram ao mesmo tempo em que o advento da internet emergia, muitas informações disponíveis tornaram-se alvos fáceis e muitos criminosos se apoderaram dessa facilidade cometendo os chamados crimes informáticos (TRUZZI, DAOUN 2015).

Gisele Truzzi e Alexandre Daoun defendem o termo;

> "Entre as expressões utilizadas — algumas de forma equivocada— temos: ‘crimes de informática’, ‘crimes tecnológicos’, ‘crimes cibernéticos’, crimes virtuais etc. Contudo, preferimos adotar o termo “crimes informáticos”, pois, traduz de forma ampliativa, os crimes praticados contra ou pela utilização de sistemas informatizados englobando-se aqueles cometidos na rede mundial de computadores" (TRUZZI, DAOUN, 2015, p.2).

O Brasil vem se adequando a esta nova realidade, criando leis para a proteção dos cidadãos, porém existem divergências de alguns autores com relação a eficácia da aplicação dessas leis. Para Gisele Truzzi e Alexandre Daoun, é preciso cautela ao se criar leis penais que diz respeito à tecnologia, principalmente quanto ao objetivo e a verificação da eficiência da mesma, para não incorrer em "repetição-legislativa, inflação-legislativa ou utilização do Direito Penal em hipóteses que poderia ser dispensado" (TRUZZI, DAOUN, 2015, p.5).

Damásio de Jesus e José Antônio Milagre (2016), por sua vez, trazem o seguinte conceito:

> “O fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do direito informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo direito penal” (JESUS, DAMÁSIO de MILAGRE et al., 2016 p.49).

Para Higor Vinicius Nogueira Jorge (2016) e Emerson Wendt (2016), existem as ações prejudiciais atípicas e os crimes cibernéticos. As ações prejudiciais atípicas são aquelas condutas que causam prejuízo ou transtorno para vítima através da rede mundial de computadores, mas não são tipificados em lei. Por sua vez os crimes cibernéticos se dividem em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”.

- Os “crimes exclusivamente cibernéticos” são aqueles que necessariamente precisam do meio da informática para cometer tal crime (como é o caso do crime de invasão de dispositivo informático, artigos 154-A e154-B do código penal, introduzido pela Lei 12.735/2012, conhecido como Lei Carolina Dieckmann).
- Os “crimes cibernéticos abertos” são aqueles que podem ou não ser praticados pelo meio informático, como é o caso de estudo os crimes de violação de direito do autor, pode ser praticado tanto no ambiente virtual como no analógico (TEIXEIRA, apud. TATEOKI, 2017).

Havendo ainda outras definições quanto à classificação dos crimes cibernéticos, no qual subdivide-se em três tipos, os puros, mistos e comuns:

> “O primeiro são aqueles em que o sujeito visa especialmente o sistema de informática; as ações materializam, por exemplo, por atos de vandalismo contra a integridade do sistema ou pelo acesso desautorizado ao computador. Crime de informática misto se consubstancia nas ações em que o agente visa o bem juridicamente protegido diverso da informática, porém o sistema de informática é ferramenta imprescindível. E os crimes de informática comum são condutas em que agentes utilizam o sistema de informática como mera ferramenta, não essencial à consumação do delito” (TEIXEIRA, apud TATEOKI, 2017, p. 1).

De acordo com Tateoki (2017), essas classificações dos cibercrimes nos ajudam a entender sobre que tipo de crime está se tratando para se poderem tomar as medidas cabíveis, lembrando que o computador não faz nada por si só, mas, existe uma mente humana que se utiliza desses recursos para cometer tais delitos.

Uma das características mais marcantes dos crimes cibernéticos é como ele percorre cidades, estados e países, o que significa que uma pessoa de qualquer cidade, estado ou país pode cometer crimes contra qualquer pessoa conectada à rede, não importando o local onde a vítima e o agressor se conectam. Isso nos mostra que temos muitos problemas por trás de tudo isso, quanto à questão de quais proporções um crime informático pode alcançar e lesionar a vida de qualquer ser, enquanto individuo de uma sociedade, e até quando este mesmo indivíduo deixa de existir, ainda existem crimes que trazem á tona o nome dessas pessoas trazendo constrangimento até mesmo como os seus familiares e a revolta da população (Cury Soares, 2019).

No entanto, ao passar dos anos, o Brasil tem adaptado melhor a legislação nas questões que se referem aos crimes informáticos, reconhecendo o perigo que tais crimes oferecem no território nacional. E é justamente por ter um potencial de percorrer não só uma cidade, um estado até chegar a níveis globais que surge outro ponto que merece atenção: as questões relacionadas à segurança nacional.

Chamando a atenção para a dimensão continental do Brasil, Alexandre Hosang (2011), salienta que "o ciberespaço e a consequente infraestrutura crítica de informação possuem caráter estratégico diferenciado", com o objetivo de que os mesmos são essenciais na segurança da soberania, na cultura e na economia do país (HOSANG, 2011. p. 14). Por isso é de extrema importância proteger o ciberespaço, e esta proteção deve fazer parte da estratégia permanente, assegurando a continuidade dos serviços essenciais.

No estudo de Alcyon Ferreira de Souza Júnior, sobre Segurança cibernética para a Escola Superior de Guerra do Rio de Janeiro, foi feita uma avaliação na Política Cibernética de Defesa do Brasil (PCD), no intuito de "verificar sua aderência com as políticas de outros países." Ele ressaltou a dificuldade encontrada em se obter as informações sobre as leis estrangeiras, nesses países isto é considerado assunto de segurança nacional (SOUZA JÚNIOR, 2013, p. 59).

Inegavelmente o Brasil tem crescido bastante na área de tecnologia, e com esse crescimento vêm às responsabilidades. É preciso uma agenda nacional de ações que constam na Política Cibernética de Defesa do Brasil. Em sua conclusão Souza Júnior diz:

> “A PCD (Política Cibernética de Defesa) é um marco decisivo no painel da segurança cibernética nacional, pois foi um grande avanço que o Brasil realizou em comparação as outras nações. Alguns objetivos merecem atenção e urgência devido a sua importância como fator do desenvolvimento e atualização da doutrina que irá nortear as ações e emprego do setor cibernético. Isso possibilitará a realização de exercícios de simulação de combate e criação de um arcabouço de conhecimento sobre o assunto para melhor preparo dos atores envolvidos” (SOUZA JÚNIOR 2013, p. 60).

A Portaria Normativa n.º 3.389/MD, de 21 de dezembro de 2012 estabelece a citada política (PCD) entrou em vigor 27/12/2012.

Ao fim de seu trabalho, Souza Júnior observou que com relação a alguns países o Brasil está bem estruturado no que diz respeito à PCD, porém ainda existem pontos que devem ser verificados e corrigidos, uma vez que:

> “Entende-se que as diretrizes adotadas na política cibernética de defesa brasileira são pertinentes e estão muito bem norteadas, mesmo que a política não aborde alguns pontos discutidos neste trabalho. Sugere-se que os resultados deste estudo sejam aprofundados objetivando-se promover mais discussões e, consequentemente, o aprimoramento da política brasileira. Em outros pontos analisados, a política do Brasil está à frente das políticas dos países estrangeiros analisados no estudo” (SOUZA JÚNIOR, 2013 p. 62).

TRUZZI, DAOUN (2015), em seu trabalho em titulado de “Crimes informáticos: o direito penal na era da informação” teve como objetivo mostrar que, o direito penal só deve ser acionado quando outras fontes do Direito foram ineficazes para solucionar o problema. Portanto Truzzi e Daoun concluem que no que se refere à crimes tecnológicos tudo já está tutelado pela legislação do país, destruindo o conceito de que a internet é território livre de responsabilidades civis. Portanto salienta que deve haver ajustes "para melhor adequar nossa realidade tecnológica ao arcabouço das leis vigentes" (TRUZZI, DAOUN, 2015, p.5).

Celso Antônio Pacheco Fiorillo e Christiany Pegorari Conte concluem que os crimes informáticos como “os ilícitos perpetrados por intermédio da Internet ou com o auxílio desta, causando algum tipo de dano à vítima” (JESUS, DAMÁSIO DE MILAGRE et al., 2016, p. 49).

Hosang (2011) atenta para a necessidade de uma governança ativa na área de tecnologia da informação, para efetivo controle no ambiente por onde circulam todas as informações, concluindo que:

> “Existem diversos órgãos da Administração Pública, organizações da iniciativa privada e instituições de Ensino e Pesquisa que vem desenvolvendo iniciativas e ações no intuito de preservar a segurança do espaço cibernético brasileiro. Porém, verifica-se a necessidade de maior integração, além da interação que já ocorre, e a articulação destes organismos e suas respectivas ações com a finalidade de promover a cultura de segurança e a difusão de experiências adquiridas”. (HOSANG, 2011, p. 14).

Emeline Piva Pinheiro, em seu trabalho sobre crimes virtuais, fez uma análise da criminalidade informática e do sistema estatal, verificou que as leis brasileiras atuais já estão sendo colocadas em práticas aos crimes no âmbito virtual, mais precisamente aos de pedofilia, fraudes, contra a honra, propriedade industrial e intelectual, dentre outros. Chegou à conclusão que a resposta da estatal é dificultada pelo fato do crime não acontecer em ambiente fixo e sim no mundo virtual mundial, sem muitas vezes deixar pistas. Para Pinheiro é preciso à criação de uma agência reguladora que fiscalize o ciberespaço, assim como a celebração de tratados internacionais que incentivem uma política mundial para cooperação recíproca a fim de coibir os crimes. (PINHEIRO, 2006).

> "Por fim, podemos dizer que as normas penais existentes são suficientes para punir as condutas danosas que ocorrem na Internet, porém o aparato policial e as políticas de incentivo e proteção do Estado deixam muito a desejar, dificultando deveras a persecução desta nova criminalidade transnacional" (PINHEIRO, 2006, p. 30).

Paulo Vinícius de Carvalho Valera e Marcelo Yukio Misaka no seu trabalho sobre crimes virtuais, analisou a legislação brasileira mostrando o que existe de concreto com relação aos crimes virtuais, seus pontos positivos e apontou os negativos como exemplo a falta de legislação específica no país. Concluíram que o Código Penal tem servido como base para punições na maioria dos crimes informáticos cometidos no território brasileiro. E acrescentou que a legislação

brasileira ainda carece de uma legislação específica que preencham lacunas a determinadas condutas delituosas. Mas observa que o Brasil tem avançado em questões legislativas (VALERA et al., 2019).

> "As perspectivas futuras são positivas, pois o país tem avançado em questões legislativas. Espera-se que esse avanço continue, contribuindo para a punição daqueles que cometem crimes virtuais não deixando lacunas ou brechas para possíveis impunidades" (VALERA et al., 2019, p.56).

Com base nos estudos citados nos autores descritos a cima ao que se refere aos crimes informáticos e proteção dos direitos na legislação brasileira, fica entendido que, o Brasil hoje tem um código penal que supre a necessidade para punição dos crimes informáticos já existentes, porém é preciso uma atuação governamental mais agressiva, para autuação eficaz nos delitos cometidos e uma maior segurança tanto aos cidadãos quanto à soberania, segurança e ordem nacional.

3. A SOCIEDADE DA INFORMAÇÃO

Desde sua existência, o ser humano naturalmente cria meios tecnológicos para facilitar sua sobrevivência, contudo a cada nova tecnologia um novo tipo de sociedade nasce, isso é inevitável. No século passado surgiu então a sociedade da informação a qual vivemos atualmente.

Várias mudanças ocorrem nas sociedades contemporâneas, sendo imprescindível que se adequem as novas tecnologias, isso levou alguns autores a defender a existência de uma nova ideia de Sociedade baseada, especificamente, na Informação, daí a concepção de Sociedade de Informação. Este novo modelo de sociedade configura em novos quadros de desenvolvimento cultural, social e econômico procedente da globalização, o qual importa à forma como os países estabelecem as suas relações, sejam elas de natureza política, social, cultural ou econômica.

Luiz Manoel Borges Gouveia (2004) explica:

> "O conceito de Sociedade da Informação surgiu nos trabalhos de Alain Touraine (1969) e Daniel Bell (1973) sobre as influências dos avanços tecnológicos nas relações de poder, identificando a informação como ponto central da sociedade contemporânea" Borges Gouveia" (2004, p. 1).

Porém não é necessariamente a tecnologia que transforma uma sociedade, mas a situação que tudo envolve, a forma como no meio social essas tecnologias se comportam.

Segundo Luís Manuel Borges Gouveia (2004):

> "A Sociedade da informação está baseada nas tecnologias de informação e comunicação que envolvem a aquisição, o armazenamento, o processamento e a distribuição da informação por meios electrónicos, como a rádio, a televisão, telefone e computadores, entre outros. Estas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, económicos e políticos, criando uma nova comunidade local e global: a Sociedade da Informação" Borges Gouveia (2004, p. 1).

O mundo atual move-se pelo poder da informação e a velocidade com que as informações são trocadas exige que pessoas e empresas busquem recursos e formas de obter tais informações antes de seus concorrentes. De posse delas é possível fazer previsões e antecipações da frenética corrida do mercado econômico, ou até mesmo neutralizar os concorrentes. O problema com essa busca insana por informações é que muitos perdem o senso de ética e acabam invadindo a privacidade alheia a fim de obtê-las (Borges Gouveia, 2004).

Com o surgimento dos meios de comunicações como, rádios, jornais, televisão e principalmente a internet, as informações atingem quase que simultaneamente milhões de indivíduos no mundo.

O controle do acesso e da divulgação de informações e de dados pessoais tornou-se uma das principais preocupações da contemporaneidade no que tange à privacidade, principalmente na internet, em virtude da formação das identidades digitais. Os dados pessoais dos indivíduos, provenientes das atividades e interações realizadas no ciberespaço, são processados e armazenados por terceiros com propósitos comerciais e de vigilância. Uma das consequências desse comportamento é o *profiling*, técnica de rastreamento de pessoas on-line com base em seu comportamento, gostos e preferências, com a finalidade de segmentá-las com publicidade, ou seja, enviá-las anúncios com base em seus hábitos de navegação (ASSIS, 2018).

Não há como negar que na atual sociedade do registro, o oferecimento de dados pessoais tornou-se a regra no ambiente virtual. O indivíduo, automaticamente, perde o controle sobre as informações ao seu respeito logo após fornecê-las, não participando do processo de decisão referente ao tratamento do seu próprio patrimônio informativo. As entidades privadas e governamentais de posse dessas informações são capazes de classificar e relacionar cada pessoa a um determinado padrão de hábitos e de comportamento, circunstâncias que podem acabar favorecendo discriminações, especialmente se forem coletados e analisados dados sensíveis (SOUZA, 2018).

Nesse mesmo sentido é a opinião de Assis (2018), quando afirma que:

> “É apenas no conforto da proteção proporcionada pela privacidade que o indivíduo possui liberdade para desenvolver completamente a sua personalidade. Contudo, na atual era do registro, a tranquilidade proporcionada pela privacidade perdeu espaço para um sentimento coletivo de constante invasão e vigilância, especialmente na internet. A preocupação com as ameaças da sociedade da informação se tornou um tópico bastante discutido e merece a devida atenção de todos os setores da sociedade” (ASSIS, 2018, p. 16).

O avanço na área da tecnologia da informação, especialmente na utilização de técnicas para a personalização da venda de softwares, games, músicas, filmes, mercadorias e serviços, afetou a autonomia das pessoas em suas escolhas e intensificou a coleta, o armazenamento e a manipulação de dados pessoais. Em razão disso, cresce a demanda da sociedade por mecanismos jurídicos mais sólidos e eficientes, que sejam capazes de prevenir e garantir a defesa dos usuários na rede e a proteção de seus dados pessoais (ASSIS, 2018).

4. DIREITOS DE PERSONALIDADE

Os direitos da Personalidade representam um dos pilares mais importantes da Constituição Federativa do Brasil de 1988, que são os direitos dos nossos atributos fundamentais, como honra, imagem, integridade física, a privacidade e a intimidade, dentre outros muitos direitos da personalidade, os quais:

> "[...] englobam a integridade física (abrange o direito à vida, à saúde e ao próprio corpo), a integridade intelectual (abrange a liberdade de pensamento e os direitos morais do autor, nos termos do art. 24 da Lei nº 9.610/98) e a integridade moral (abrange a proteção à honra, ao recato e à identidade pessoal) [...]" (MEDEIROS, 2015, p.1-2).

A proteção aos direitos de personalidade também está inserida no postulado ou princípio fundamental correspondente à dignidade da pessoa humana, descrito no art. 1º, § 3° da Constituição Federal, como um princípio fundamental.

No que diz respeito à origem dos direitos da personalidade, a doutrina majoritária ou dominante, seguida por Carlos Alberto Bittar, Caio Mário da Silva Pereira e Carlos Roberto Gonçalves, acredita que os direitos da personalidade se originam do jusnaturalismo (direito natural). Isto porque os citados direitos "resultam dos valores e, portanto, são anteriores ao próprio ordenamento jurídico. Essa posição visa enaltecer a tutela dos direitos da personalidade, impedindo o Estado de aniquilar tais direitos" (MEDEIROS, 2015, p. 02).

De acordo com Medeiros (2015), no famigerado art. 5º, incisos V e X da Constituição Federal, também se evidenciam uma preocupação com os direitos da personalidade, que nos dá o entendimento de que os referidos direitos são, antes de tudo, direito fundamentais, porque eles são mencionados na Constituição Federal (CF), como está descrito no início do dispositivo legal: "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"; em seguida, reforça o inciso "V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;" e o "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;" da mesma forma o Código Civil de 2002 trás um capítulo em que ele cuida também dos direitos da personalidade a partir do Art. 11 até o Art. 21 (MEDEIROS, 2015, p. 2).

Sabendo-se que sendo uma forma de se tratar o ser humano enquanto pessoa humana que ele é, cabe ressaltar que tais direitos trazem consigo algumas características. De acordo com Medeiros (2015), uma das primeiras características que são inerentes a eles é o fato de serem absolutos, sendo possível valer-se da expressão de origem latina e comum no âmbito jurídico, de que os direitos de personalidade são oponíveis "*erga omnes*", e tal expressão significa no literal "contra todos", significando que, todo homem é titular do próprio direito e que pode se opor contra toda e qualquer pessoa, podendo exigir que as pessoas como um vizinho, amigos, colegas e a sociedade em geral respeitem mutuamente a honra, a imagem, a integridade física, a privacidade e a intimidade, dentre outros muitos direitos de personalidade que cada indivíduo possui e que são considerados absolutos.

Uma segunda característica, ainda na lição da doutrina em geral e, mais especificamente, de acordo com Medeiros (2015), é a inserção num rol exemplificativo, de modo que os direitos de personalidade não sofrem uma limitação ou restrição, no sentido de não poderem ser ampliados por analogia. Daí falar-se no "Direito à Personalidade Ilimitada", demostrando-se que eles não se limitam a um rol taxativo previsto em lei, uma vez que não tem como um legislador dizer quais são todos os direitos da personalidade. Por exemplo: o direito à moradia é considerado por alguns doutrinadores jurídicos como um direito especial de personalidade, ainda que classicamente seja enquadrado na categoria de direitos sociais, o que efetivamente não deixa de ser também.

A terceira característica, na lição de doutrinadores de direito civil, a exemplo, Medeiros (2015) e outros, remete ao fato de que os direitos a personalidade são "Extrapatrimoniais", o que significa que eles não apresentam um conteúdo econômico de forma imediata; não existe um preço para a honra dos sujeitos, bem como não há um valor econômico agregado aos atributos que o compõem. O que se busca, quando do pedido de indenizações por intermédio das ações judiciais, é compensar ou reparar os danos sofridos por uma pessoa, em decorrência da prática de um ato ilícito (via de regra). Então, estima-se um valor

compensatório ou reparatório, o que não significa dizer que o direito de personalidade tenha como valor monetário um valor X. Apenas se busca uma forma de punir ou educar o sujeito causador do dano e de se minimizar o sofrimento ou a perda material da vítima ou de quem lhe faça às vezes quando da ação de indenização.

Já quarta característica, conforme Medeiros (2015) é a intransmissibilidade, que decorre do fato de os direitos de personalidade serem extrapatrimoniais. Acabam se tornando “Intransmissíveis”, o que leva a entender que eles não se transmitem com a herança, pois a integridade física do ser humano não pode ser transferida diferentemente de um carro, casa e o dinheiro quando o ser humano deixar de existir neste plano material, como também não podem ser transferidas a privacidade, a integridade física, a intimidade e outros, pois, sendo os direitos da personalidade extrapatrimoniais são intransmissíveis, pois um depende do outro.

A quinta característica é a impenhorabilidade, que significa dizer que os direitos da personalidade não se submetem a qualquer tipo de constrição judicial (MEDEIROS, 2015).

A sexta característica é que são “Perpétuos os direitos ou Imprescritíveis”, o que demonstra que não existem prazos para o exercício de direito da personalidade, justamente porque a honra de um ser, a integridade física, dentre outras características ou direitos não têm prazo de validade (MEDEIROS, 2015).

Entretanto, quando uma pessoa faz algum tipo de divulgação de outrem sem o consentimento deste, seja por meio de mídias sociais ou de programas televisivos sensacionalistas ou qualquer outro meio de propagação, violando, por conseguinte, um direito da personalidade da outra pessoa, surge o direito a ser reparado civilmente. Porém existe um prazo para ser reclamada a violação de tais direitos (Código Civil, Art. 206, § 3º, inciso V) o qual traz um prazo máximo de 3 anos.

A última ou a sétima característica nos mostra que eles são “’Irrenunciáveis ou Indisponíveis” significando que em regra a pessoa titular do direito de personalidade não pode renunciar, dispor ou abrir mão de tal direito, a não ser quando uma pessoa se deixa dispor como, por exemplo: quando uma pessoa se deixa ser fotografada, filmada dentre outros, cedendo assim temporariamente o

direito de sua própria imagem, assim como é valido o ato de disposição do próprio corpo, por meio de doação de órgãos, quando o sujeito dispõe da sua integridade física, cedendo os órgãos, dentro dos limites legais, especialmente a dignidade da pessoa humana. Em virtude disso:

> "[...] muitos afirmam que os direitos da personalidade são relativamente indisponíveis (Enunciados nº 4 e 139 do CJF). Só não se admite que a renúncia seja permanente e geral. Assim, por exemplo, a cessão vitalícia de imagem por atletas – comum no exterior – não é bem recebida no direito brasileiro. A renúncia geral diz respeito à ideia de que a renúncia merece sempre interpretação restritiva [...]" (MEDEIROS, 2015, p. 4).

Na jurisprudência mencionada a seguir, a moradia é vista como um direito especial de personalidade e se aplica a dignidade da pessoa humana como parâmetro para a decisão judicial, como se transcreve abaixo:

> "O art. 5º da Lei nº 8.009/90 exige moradia permanente para configurar o bem de família. Mas o STJ já pacificou o entendimento de que a impenhorabilidade subsiste ainda que o proprietário não resida no imóvel, desde que fique evidenciado que o sujeito depende dos recursos advindos do aluguel para sua subsistência. É uma interpretação contra legem, mas em consonância com o princípio da dignidade da pessoa humana" (MEDEIROS, p. 4).

No que se refere aos direitos da personalidade de uma pessoa que já faleceu ou depois de sua morte é um tema de igual teor muito discutido entre os juristas e até entre os próprios familiares do falecido ("de cujus"), nesse sentido, observa-se que:

> "A proteção *post mortem* dos direitos da personalidade está positivada no art. 12, parágrafo único, do Código Civil. Além dos legitimados previstos expressamente no dispositivo legal, a proteção também pode ser exercida pelo companheiro, por força do art. 226 da Constituição da República de 1988" (Enunciado nº 275 do CJF) (MEDEIROS, 2015, p. 6).

Ademais, é sabido que quando se extingue a personalidade jurídica, da pessoa natural, quando ela morre também deixa de ter direitos, como deixa de ter obrigações, a pessoa quando morre deixar de ser pessoa em seu aspecto jurídico,

no entanto o ordenamento jurídico estende para depois da morte a tutela dos direitos de personalidade.

E com esses argumentos consegue-se entender que todas as pessoas que vieram a falecer deixam de ter direitos e obrigações civis, porém o direito de personalidade continua no seu pós-morte, aqui no plano físico, de acordo com o ordenamento jurídico, onde se estendem a tutela dos direitos de personalidade.

5. CRIMES INFORMÁTICOS

Neste capítulo abordaremos a história e os conceitos da Internet e dos crimes informáticos ou cibercrimes. Explicaremos as circunstâncias sociais que se deram para o surgimento até o fato de a Internet ter se tornado uma ferramenta a serviço dos crimes informáticos atuais. Falaremos sobre os principais crimes informáticos, dando ênfase aos crimes de difamação, calúnia, injúria, pedofilia, pornografia infantil e o crime de divulgação de conteúdos sem autorização. Por fim abordaremos como denunciar um crime informático e sua importância.

5.1 Histórias e conceitos

Para definir crimes informáticos é necessário entender o que é criptografia e alguns aspectos de suma importância para darmos continuidade a este estudo. Criptografia tem o significado básico de esconder ou mascarar informações através de linguagem codificada. Essa é uma linguagem muito antiga desde os primórdios da humanidade, como quando houve uma guerra entre a Grécia (com Alexandre “O GRANDE”) e Pérsia (com o Rei Xerxes) surgindo à necessidade de troca de informações secretas entre os grupos, fazendo com que só os que conheciam o código fossem capazes de interpretá-los (SILVA, 2016).

Ao longo do tempo, especialistas tem se interessado pelas mais vastas áreas de criptografia com o intuito de evoluir essa tecnologia e trazer confiabilidade e segurança em um altíssimo nível para coibir os ataques de peritos especializados em técnicas de cibercrimes, os famosos “Crackers”, (Este termo foi criado em 1985 por hackers em sua defesa), o indivíduo que pratica a quebra (ou cracking) de um sistema de segurança de forma ilegal ou sem ética e que violam a privacidade alheia recebem este título. Um Cientista e Matemático considerado pelos mais diversos cientistas em sua época como “O Pai da Computação”, foi um criptoanalista Britânico Alan Turing. Ele serviu a inteligência britânica durante a Segunda Guerra Mundial, e foi o responsável pela decodificação dos códigos alemães. Turing foi reconhecido por expor a fragilidade dos sistemas da época sendo o responsável pelo avanço da criptografia como ciência (SCHERCHTER, 2016, p. 19).

De acordo com Paesani (2000), após décadas de aperfeiçoamento da criptografia surge então as primeiras e rudimentares noções de internet. Desde a criação e seu desenvolvimento inicial a internet era considera como uma arma de guerra de grande poder bélico para sua época e nem se quer pensava-se em torná-la comercial, essa ideia só se deu décadas depois de sua criação no alto da guerra fria.

A corrida armamentista e a tensão da Guerra Fria entre Estados Unidos e União Soviética tiveram grande influência na caracterização e desenvolvimento desse invento, pois serviu de estímulo para aperfeiçoar esse sistema, tornando-o mais sofisticado e preventivo (CARVALHO, 2006).

Após isso a internet começou a ganhar uma forma mais próxima da atualmente conhecida, levando o conceito de crimes informáticos a patamares mais elevados. A popularização da internet somente começou em 1988. Com o fim da guerra e das tensões entre EUA e URSS, houve então a abertura da rede para interesses comerciais, quando os Estados Unidos começaram a “comercializar” a internet (PAESANI, 2000).

Em seguida, iniciou-se uma revolução tecnológica, um agitado ciclo de mudanças em toda a estrutura da internet, ela deixou de ser um sistema de acesso restrito às minorias, para se tornar o meio de comunicação mais utilizado no mundo.

Os crimes informáticos também iniciaram uma nova fase, já que a criptografia, utilizada para proteger dados digitais do mundo corporativo, se tornou objeto de atenção dos criminosos da internet.

Observa-se hoje que o formato digital tem substituído à forma de trabalho nas empresas e até nos órgãos públicos. A internet tornou-se uma necessidade na vida das pessoas, seja no trabalho, estudo ou entretenimento, há muitos meios para se acessar a internet, bem como as formas de invadir dispositivos através desta. Por PC, tablets, notebooks ou smartphones, o fato é que a frequência com que as pessoas se mantêm conectadas aumenta cada vez mais, aparelhos como o celular, tornaram-se necessidade na vida das pessoas. Atualmente, 4,1 bilhões

de pessoas utilizam a rede mundial. O número de usuários corresponde a 53,6% da população de todos do mundo (ONU NEWS, 2019).

O mundo digital, no início do milênio, era enigmático para pessoas comuns, mas com sua popularização ampliou-se o uso da internet e com isso vieram às preocupações sobre a segurança das informações que seriam compartilhadas on-line, não só os órgãos governamentais, mas todos os seus usuários (D'URSO, 2017).

A constante mudança tecnológica dificulta o combate aos crimes, que estão em constante alinhamento com as novas tecnologias. Assim, com o uso incontido e indiscriminado da internet, alguns indivíduos com conhecimento em informática passaram a se aprimorar e utilizar esses conhecimentos para roubar informações criptografadas ou não, como já havia sendo feito há muito tempo, para obter proveito econômico ou ainda, por mera diversão (JESUS; MILAGRE, 2016).

Essas pessoas hoje são denominadas de hackers, um designativo da era moderna para indivíduos que sempre existiram. Esse termo da língua inglesa é usado para designar programadores muito habilidosos, que secretamente obtém informações sobre o sistema informático de outra pessoa para que possam ver usar ou modificar, pelos mais variados motivos (JESUS; MILAGRE, 2016).

5.2 Principais crimes informáticos

Com o desenvolvimento e a popularização da internet, a quebra de códigos e invasão de sistemas deixou de ser um instrumento de guerras para se tornar uma oportunidade de lucro ilícito ou mero passatempo, fazendo do cibercrime o mal social que é hoje. Por exemplo, os estelionatários, que viram nas transações comerciais via internet à oportunidade de aplicar seus golpes. As vítimas atraídas pela facilidade de comprar e receber produtos sem sair de casa ou transacionar com suas contas bancárias através de uma tela de computador acabam caindo facilmente nos golpes (Convergência Digital, 2018).

As pessoas abraçaram esse novo mercado, sem muita preocupação em apurar a autenticidade dos sites em que estavam inserindo suas informações, o

que as fizeram presas fáceis desses criminosos, que agem no submundo da internet.

Os mais variados tipos de conduta delituosa são praticados de forma on-line, desde pedofilia, prostituição, tráfico, pirataria, até sabotagem e terrorismo. A digitalização dos métodos de trabalho tem causado em muitos países, inclusive ao Brasil, transtornos provocados por uma nova onda de crimes cibernéticos (Convergência Digital, 2018).

No mundo, durante os primeiros seis meses de 2018, mais de 25 milhões de registros foram comprometidos ou expostos a cada dia, ou 291 registros a cada segundo, incluindo dados médicos, cartões de crédito e/ou dados financeiros ou informações de identificação pessoal. Isto é particularmente preocupante, já que apenas 1% dos registros de dados roubados, perdidos ou comprometidos estava protegido por criptografia, uma queda de 1,5% quando comparada aos primeiros seis meses de 2017 (Convergência Digital, 2018).

Existem dois grandes grupos de crimes informáticos, Kerr os divide em um que tem como objetivo a violação dos sistemas de informática, independentemente do motivo; o outro tem como objetivo a violação de outros bens jurídicos ou valores sociais, usando a informática apenas como meio de cometer o ilícito (KERR, 2011).

Os crimes mais comuns praticados na *web* são: vazamentos de vídeos e imagens íntimas, fraudes bancárias, roubo de senhas de redes sociais, invasão de rede internet em computador, e-mails e sistemas operacionais, falsidade ideológica, invasão a privacidade e violação do direito autoral dentre outros crimes tipificados como crimes contra a honra, instigação ao suicídio (como a tal famosa baleia azul, em que criminosos “cassavam” as vítimas pela sua fragilidade emocional e a desafiava a cometer suicídio), furto por desvio de dinheiro em contas bancárias ou bancos virtuais, estelionato onde bandidos utilizam CPFs e cartões de créditos falsos para realizar compras na internet, violação de direitos autorais por meio de cópias e downloads, pedofilia divulgando imagens pornográficas de crianças e até aliciamento, favorecimento de prostituição sites de anunciados de garotas e garotos de programa, tráficos de drogas e armas onde

existem sites de divulgação desses materiais em famosos mercados negros (MENEZES, 2017).

Em uma análise sobre esses, Viana (2001) classifica os crimes virtuais em :

- crimes informáticos impróprios, os quais o computador é apenas um instrumento de realização do crime, não existindo violação de dados, como nas ocorrências de difamação, calúnia e injúria;
- crimes informáticos próprios, nesses o bem jurídico violado são os dados computacionais; crimes informáticos mistos, onde há a violação de dados computacionais e de outros bens jurídicos distintos;
- crimes informáticos mediatos ou indiretos, esses servem de instrumento para a consumação de outro delito não-informático, como no de furto de dinheiro de contas bancárias pelo computador.

Para Tulio Viana e Felipe Machado (2013), existem quatro tipos de classificações de crimes digitais, na qual segundo os autores o principal bem jurídico a ser protegido pela lei penal nesses casos é a inviolabilidade da informação automatizada (dados), assim:

- Os crimes informáticos impróprios (realizados por um indivíduo), são aqueles que o computador é usado como meio para executar o crime, mas não existe a inviolabilidade da informação automatizada (exemplos: ameaça, incitação ao crime e etc.);
- Os crimes informáticos próprios são aqueles em que o bem jurídico protegido pela lei penal é a inviolabilidade de dados (Como é o caso do crime de invasão de dispositivo informático do art. 154-A e 154-B do CP, inserção de dados falsos em sistema de informações do art. 313-A do CP e modificação e alteração não autorizada de sistema de informações do art. 313-B do CP);
- Os crimes mistos são aqueles que além de proteger a inviolabilidade de dados, a legislação visa proteger bem jurídico de natureza diversa (crime eleitoral do artigo 72, da Lei nº 9504/1997);

- O crime informático mediato ou direto é aquele considerado o delito fim não informático que herdou a característica do meio para consumar o crime.

Para outros autores como, Ivette Senise Ferreira (2001) e Marcelo Xavier de Freitas Crespo (2011) existem duas modalidades de crimes:

- A primeira modalidade fala-se em aos atos dirigidos contra o sistema da informática, essa modalidade para os autores são chamados de “crimes informáticos próprios”, praticados por meio da informática, sem a informática o crime não ocorrerá (como é o caso do crime de inserção de dados falsos em sistema de informações, art. 313-A do CP);
- A segunda modalidade, são os “crimes informáticos impróprios”, podem ser praticados de várias formas, sendo ela por meio da informática ou não, como são os casos os crimes contra a honra e violação dos direitos do autor, estelionato, pornografia infantil dentre outros.

Assim por fim poderão ser considerados crimes digitais, isto é que ocorra em meio digital: crimes contra a honra, ameaças, induzimento e instigação ou auxilio a suicídio, furto, falsificação de documentos, estelionato, espionagem industrial, violação de segredo, apologia de crime, racismo, atentado a serviço de utilidade pública, pornografia infantil, corrupção de menores em salas de bate papo de internet, violação de direitos de autor, inserção de dados falsos em sistema de informações, crimes contra equipamentos de votação, invasão de dispositivo informático (TATEOKI, 2016).

5.2.1 Crimes contra a honra (difamação, calúnia e injúria)

Atualmente os crimes cometidos nas redes sociais que mais têm destaque, são os referidos crimes contra a honra. Comumente escutamos sobre Difamação, Calúnia e Injúria. Temos muitos exemplos de processos de famosos que aconteceram nos últimos anos, e muitos desses processos caem sobre jornalistas,

que por não entenderem os "institutos da difamação, calúnia e injúria, acabam propagando notícias sobre a vida particular de artistas e muitas vezes acabam cometendo esses crimes” (MARQUES, 2020).

Um exemplo disso foi a do famoso jornalista Léo Dias, que foi condenado por divulgar erroneamente a foto de uma mulher em uma matéria com o seguinte título "Relação a três de Ronaldinho Gaúcho vira processo por agressão". No caso o jornalista usou a foto para ilustrar a matéria, e a reclamante não tinha nada a ver com a situação. O Juízo interpretou a situação como evidente atentado à honra, à personalidade e à vida privada da mulher (CONSULTOR JURÍDICO[1], 2020).

Ainda segundo a matéria "Veicular matéria jornalística de forma irresponsável, fazendo uso indevido da imagem de terceiros, tem caráter difamatório e, por isso, enseja indenização por danos morais" (CONSULTOR JURÍDICO[1], 2020).

Em primeira instância o jornalista foi condenado a pagar 12 mil reais à vítima, mas o juiz Paulo Sérgio Tinoco Néris, aumentou para 20 mil reais, visto que o jornalista tem mais de 5 milhões de seguidores no *Instagram* e mais de 300 mil no *Twitter*, dando uma proporção de divulgação de grande alcance e além do que Ronaldinho Gaúcho é mundialmente conhecido e o caso tomou proporções internacionais.

Casos de difamação são muitos comuns e repetitivos na *web*, os criminosos se utilizam do meio de comunicação para atacar pessoas, e as proporções são enormes, tendo em vista o grande alcance da rede. Este tipo de ato é definitivamente um crime sujeito a punições diante do artigo 139 do Código Penal que diz:

> "Art. 139. Difamar alguém, imputando-lhe fato ofensivo à sua reputação. Pena - detenção, de três meses a um ano, e multa" (BRASIL[2], 2020, p. 43).

Seguido a difamação, temos os casos de calúnia, pessoas mal intencionadas imputam falsamente informações desonrosas a respeito de outras, com o intuito de denegrir lhe a imagem, o ato é considerado crime.

O artigo 138 do Código Penal dispõe:

> "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." (BRASIL², 2020, p. 43).

Os casos de calúnia cresceram de modo significativo, falsas acusações as famosas fake news tem se propagado livremente nas redes sócias por pessoas que não checam a fonte das informações.

No portal R7, foi divulgada uma matéria de calúnia contra o senhor Ronaldo Souza na época com 39 anos, o mesmo teve sua foto, em qual ele aparecia com seu neto divulgado nas redes com a acusação de que ele era um homem muito perigoso e havia estuprado e matado o garoto. A postagem afirmava que Ronaldo era muito perigoso que se alguém tivesse informação do mesmo deveria entrar em contato com a polícia, que era um foragido e que as pessoas deveriam matá-lo. Essa calunia só foi excluída após a família denunciar ao aplicativo (R7, 2017).

Casos de injúria são um dos mais levianos, e ocorre com infeliz frequência na rede, um exemplo de caso emblemático de injúria racial que ocorreu recentemente foi o de racismo praticado online contra a jornalista Maria Júlia Coutinho, que apresenta a previsão do tempo no Jornal Nacional (SOARES, 2016).

A página do referido informativo eletrônico no *Facebook* serviu de ferramenta para os infratores atacarem a honra e a imagem da jornalista, com agressivos comentários racistas. A rede Globo promoveu uma campanha em solidariedade à sua funcionária, ao passo que pressionavam as autoridades policiais a tomar providências mais rígidas e imediatas. A estratégia teve êxito e a

polícia chegou a quatro indivíduos que seriam os fomentadores dessas ideologias discriminatórias na internet, com uma legião de vinte mil seguidores (SOARES, 2016).

Diante da ausência de tipos específicos para os delitos, como indica a reportagem de Soares (2016), os indivíduos foram enquadrados nos delitos de falsidade ideológica, racismo, injúria e corrupção de menores, além de formação de associação criminosa na internet. Esse último delito citado, o de “formação e associação criminosa na internet”, é o tipo previsto no art. 288 do Código Penal, associação criminosa.

Infelizmente não existe norma especial que enquadre essa conduta quando praticada pela internet, devendo a lei ser aplicada por analogia. A Lei 12.737/2012 apenas inseriu alguns delitos no Código Penal relacionados aos crimes praticados contra a atriz Carolina Dieckman, mas não abrange toda a gama de condutas delituosas existentes no mundo digital (SOARES, 2016).

Deste modo, Aparecido Rocha (2017), apresenta que, os agressores da jornalista global e tantos outros que atacam diariamente a honra das pessoas atrás da cortina do anonimato propiciada pela internet, são enquadrados em tipos genéricos. Em matéria de legislação específica alguns países estão mais adiantados que o Brasil. Os Estados Unidos, por exemplo, aprovaram sua primeira lei de crimes cibernéticos há quase 30 anos.

O crime de injúria baseia-se no ato de ofender verbalmente, por escrito ou até fisicamente, a dignidade da pessoa, ofendendo-lhe a moral, com o intuito de humilhar a vítima conforme diz o artigo 140:

> 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 à raça, cor, etnia, religião, origem ou à condição de pessoa idosa ou portadora de deficiência: (Redação dada pela Lei nº 10.741, de 2003).
>
> Pena - reclusão de um a três anos e multa. (Incluído pela Lei nº 9.459, de 1997) (BRASIL², 2020, p. 44).

Estes tipos de crimes cibernéticos acabam trazendo problemas para as pessoas acabando muitas vezes de vez com a sua imagem e podendo trazer problemas psicológicos para a vítima então devemos dar muita atenção às leis que existem e denunciar essas práticas que afetam tanto o ser humano em uma sociedade.

5.2.2 Pedofilia e pornografia infantil

Muito se tem discutido nos dias atuais, acerca da perda da privacidade ou da sua invasão, sobretudo na era cibernética em que se vive, pois, com a mesma velocidade com que se propagam as novas tecnologias, as redes sociais se disseminam e multiplicam, assim como se as notícias em geral são rapidamente compartilhadas, ao mesmo passo em que vídeos, fotos e outros recursos audiovisuais são espalhados na rede, inclusive no âmbito da pornografia, em geral (GILABERTE, 2020).

Ocorre que, dada a precoce iniciação da vida sexual entre crianças e adolescentes, tem se tornado de certo modo comum à divulgação de imagens e vídeos entre eles e de forma pública, com conteúdo sexual e pornográfico, não acometendo somente os adultos, Martinelli com suas palavras acerca deste assunto diz:

> “O crime que mais causa repulsa na sociedade é a pornografia infantil. É inaceitável as situações em que a criança é exposta e subordinada a atos tão infames, para diversão de pessoas desequilibradas. É totalmente fora da tolerância dos padrões sociais, esses delinquentes encontram na Internet um meio para satisfazer virtualmente os pedófilos. Esta modalidade aparece na Internet de duas maneiras: pelas "home pages" e por correio eletrônico. Na primeira opção, os gerenciadores das páginas 34 recebem uma quantia dos usuários, que dispõem de um acervo de fotos e vídeos. Na segunda opção, o material é distribuído de um usuário a outro, diretamente” (MARTINELLI, 2000, p. 33).

É cediço que há muitos casos de divulgação de imagens, vídeos, recursos audiovisuais que configuram a pornografia, praticados por adultos contra menores, casos de pedofilia ou mesmo de pornografia praticada entre adultos, os quais, contudo, apresentam limites delineados pela lei (GILABERTE, 2020).

Talvez pelo apelo da indignação social, o Estatuto da Criança e do Adolescente, que é o que melhor se destaca entre os demais, pois a lei não apenas dispõe de uma lista de crimes em espécies, praticados contra a segurança, bem-estar e integridade física e moral da criança e do adolescente, também através da internet, como ainda dispõe acerca dos procedimentos investigativos a serem realizados por agentes da polícia na internet (BRASIL ESCOLA, 2017).

As redes sociais na internet se tornaram um meio de comunicação e debate muito eficaz que, embora útil, tem sido usada de forma banal, especialmente por crianças e adolescentes, O ECA (Estatuto da Criança e do Adolescente) mostra-se importante frente a esse novo meio de interação social. Com o surgimento das redes sociais, as pessoas se deparam com a oportunidade de divulgar seus pensamentos, ideias e opiniões indiscriminadamente (BRASIL ESCOLA, 2017).

Com o intuito de aprimorar e combater a produção, venda e distribuição de artigos pornográficos, bem como criminalizar suas aquisições posse e quaisquer condutas relacionadas à pedofilia a Lei 11.829 de 35 de novembro de 2008, altera a Lei 8.069 de 1990:

> "Art. 1º Os arts. 240 e 241 da Lei no 8.069, de 13 de julho de 1990, passam a vigorar com a seguinte redação:
>
> “Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
>
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
>
> § 1o Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
>
> § 2o Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:

I – no exercício de cargo ou função pública ou a pretexto de exercê-la;

II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou

III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento" (BRASIL[3], 2020).

Art. 2º A Lei nº 8.069, de 13 de julho de 1990, passa a vigorar acrescida dos seguintes arts. 241-A, 241-B, 241-C, 241-D e 241-E:

"Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

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

§ 1o Nas mesmas penas incorre quem:

I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;

II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.

§ 2o As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 1o A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.

§ 2o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:

I – agente público no exercício de suas funções;

II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;

III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o

> recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
>
> § 3o As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido.
>
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:
>
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
>
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.
>
> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:
>
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
>
> Parágrafo único. Nas mesmas penas incorre quem:
>
> I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
>
> II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.
>
> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais."

Esta lei entrou em vigor no dia 25 de novembro de 2008, tipificando assim os crimes de pedofilia. Foi sancionada pelo presidente Luiz Inácio Lula da Silva (BRASIL[3], 2020).

5.2.3 Divulgação de conteúdo sem autorização

Devido ao crescimento da internet, tornou-se mais difícil de controlar a divulgação e propagação de fatos que acontecem diariamente em nossas vidas, quando o termo envolve a sociedade em si, com vários indivíduos munidos de tecnologia e acesso as redes e mídias sociais, onde cada um publica/posta o que

lhe convém, fazendo com que notícias que antes eram estudadas, por outros meios, fossem agora publicadas sem qualquer cuidado (SOUZA, 2018).

O surgimento da era digital trouxe facilidades, mas por outro lado tornou a vida uma exposição descontrolada, as pessoas divulgam, publicam fotos e vídeos, compartilham localizações, sem pensar nas consequências, não pensam na privacidade, nem tão pouco se lembram dos direitos e garantias de terceiros, que consequentemente são expostos e compartilhados sem consentimento (SOUZA, 2018).

Com a facilidade de acesso ilegal a informações e de objetos de propriedade intelectual e artística, também foi criada uma espécie de realidade virtual. Os usuários até desenvolveram uma linguagem, um meio de interação social, próprios dessa realidade. Nesse meio, direitos básicos do cidadão garantidos pela Constituição Federal, como a igualdade, a privacidade e a dignidade, foram sobrepujados e violados, uma vez que o braço da lei ainda não alcançava esses infratores (SOARES, 2016).

Pessoas começaram a utilizar a rede para extrapolar seu direito e ferir o direito do outro, através do anonimato, acreditando estar “a salvo” da Justiça. Mas o direto brasileiro vem lidando com essa questão dos crimes virtuais há tempos, lentamente, porém alcançado os infratores da norma no plano virtual e aplicado punições no mundo real (SOARES, 2016).

As formas de praticar crimes na Internet vêm evoluindo, e o Brasil já tem um longo histórico de condutas informáticas danosas. Um exemplo dessa infeliz estatística é o do ex-prefeito Paulo Maluf, o qual, nas eleições de 2003, foi o primeiro político a sofrer sabotagem digital. Os hackers invadiram o site do político espalhou e-mails a todos os eleitores cadastrados, divulgando mensagens de cunho difamatório (SOARES, 2016).

As pessoas perdem o rumo na hora de usar essa tecnologia, e assim acabam por cometer diversos ilícitos. Diante disso é notório então um conflito entre intimidade e liberdade de expressão. Dentro desse embate, o Superior Tribunal de Justiça (STJ), já proferiu decisões importantes mostrando os dois pontos de vista mostrando-se favorável à intimidade no caso em que uma pessoa

foi divulgada como partícipe com o exemplo ocorrido referente ao caso que ficou conhecido como “Chacina da Candelária”, objeto do Recurso Especial no 1.344.097-RJ (SOUZA, 2018).

O caso que ocorreu no dia 23 de julho de 1993, onde oito jovens, seis menores de idade, foram assassinados por criminosos armados, próximos à igreja da Candelária, neste caso estavam envolvidos diversas pessoas (mendigos e crianças de rua) que serviram como alvos dos ataques que causaram as mortes no Centro do Rio de Janeiro. Um dos acusados, o serralheiro J.G.F.8, após estar encarcerado por cerca de três anos, acabou sendo absolvido, por não terem fatos contundentes (de autoria negativa) (SOUZA, 2018).

Mesmo que já se encontre absolvido da acusação. O ministro afirmou ainda que o Marco Civil da Internet trata da proteção da intimidade e da vida privada. Entre os dispositivos citados aparece o artigo 7º, X, que, segundo o ministro, seria uma forma de direito ao esquecimento. A redação do artigo diz que é direito dos usuários a exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvado as hipóteses de guarda obrigatória de registros prevista nesta Lei (SOUZA, 2018).

Anos após o ocorrido, a empresa Rede Globo, através de seu veículo de comunicação, divulgou mais ainda o caso em um programa de informativo de crimes de toda natureza chamado de, “Linha direta”, divulgando de maneira infeliz o nome do réu de juízo e o resultado do seu julgamento, logo após ter sido veiculado, o acusado já em liberdade, entrou com uma ação, alegando que o que fora divulgado no programa e de seus modos midiáticos de propagar causaram-lhe inúmeros danos, tendo que, se deslocar do local aonde habitava de maneira rápida e sutil da comunidade onde ele e a família tinham convívios sociais com medo de sofrer futuras retaliações, para preservação da sua família (CONSULTOR JURÍDICO, 2013).

O caso foi reaberto e aconteceu que foi invocado o direito ao esquecimento, não para que fosse esquecido e sim como processo indenizatório com um embasamento específico e direto, consequentemente o caso foi dado como vitorioso e a emissora teve que lhe pagar a indenização. É de suma importância

lembrar que neste caso que foi reaberto é que o Acordão realizado realçou a vida privada, a segurança e proteção a intimidade e que o anonimato em nada prejudicaria o programa televisivo na sua divulgação. Foi evidenciado ainda em loco que não se pode confundir o direito à imagem com o direito a honra. O primeiro é violado quando se realiza por mínima que seja uma divulgação ou propagação de uma informação da imagem sem o consentimento da pessoa sem levar em consideração a veracidade dos fatos ocorridos (CONSULTOR JURÍDICO, 2013).

A Constituição Federal Brasileira de 1988 deixa claro o privilégio e o valor da dignidade humana, quando acontece de se ter um conflito com a liberdade de imprensa ou da liberdade da manifestação do pensamento iniciado pelo artigo 5º da mesma. No Tribunal de Justiça, o Ministro Relator Luiz Felipe Salomão acrescentou, ainda, o argumento de que, no próprio inciso, que a tutela a intimidade e a vida privada, há menção expressa ao direito à indenização pelo dano material ou moral decorrente de sua violação (inciso X do artigo 5º). E o que aconteceu dados os fatos, foi que, os que foram condenados tem total direito ao sigilo nas folhas de antecedentes e pelos tais fatores a uma razão maior de os absolvidos terem o direito ao total esquecimento. Sendo a notícia verdadeira ou não, não se pode sair divulgando os famosos “FAKE NEWS” (notícias falsas), sem consequência alguma, quando alguém divulga algo, torna-se refém da mesma informação, independente de sua procedência e o sujeito se torna responsável pela possível repercussão que será causada através dela (CONSULTOR JURÍDICO, 2013).

Tendo tomado todas as medidas cabíveis em meio ao caso concreto, o Ministro Salomão compreendeu que a omissão do nome da imagem do autor na retratação do crime ocorrido em nada poderia prejudicar a liberdade obtida pela imprensa, dada a repercussão que o caso tomou, mostrando que a informação por mais que tente preservar a vida dos indivíduos, observando o direito ao esquecimento, vai manter a memória dos fatos ocorridos em 1993, deixando um Marco no cenário brasileiro (CONSULTOR JURÍDICO, 2013).

Caso de extrema relevância e de grande repercussão social no Brasil foi o da modelo Daniela Cicarelli, que entrou com uma ação contra o Google para

remover um vídeo que foi filmado em uma praia publica onde no vídeo a mostram tendo supostas relações intimas com o seu namorado de uma forma imprudente, cientes que corriam um alto risco de seus atos onde por uma infelicidade havia um paparazzi a espreita que acabou viralizando o vídeo do casal e pessoas comuns que estavam no local que não estava em momento algum deserto. “[...] para a modelo Daniela Cicarelli que, buscando remover do *YouTube* um vídeo íntimo filmado (em local público) sem seu consentimento ou de seu ex-namorado, tornou-se a parte autora de um dos principais casos brasileiros relativos à exposição não autorizada de imagens em sites de compartilhamento de conteúdo e ao bloqueio de aplicações de Internet” (SOUZA, 2018, p. 09).

E eles ganharam a causa na justiça que ajuizaram como uma ação indenizatória baseada na violação dos direitos a imagem do casal em São Paulo, que foi enviada para a 23ª Vara Cível, justamente porque a Constituição Brasileira de 1988 diz em seu Art. 5, inc. X :

> “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL[7], 2020).

É importante saber que a veiculação de imagens pessoais e profissionais sem a devida autorização, independentemente do meio tecnológico utilizado, haverá o dever legal de reparação, garantido pela nossa Constituição Federal que prevê que a violação da intimidade, da vida privada, da honra e da imagem das pessoas, origina o direito a indenização pelo dano material ou moral (FERNANDES, 2019).

5.3 Como denunciar um crime informático

Após entender e reconhecer o que é o crime informático, quais são e suas características, é preciso saber como denunciar um crime informático.

A SaferNet que é uma organização não governamental, e sem fins lucrativos, dispõe em sua plataforma digital, uma sequência de medidas que uma pessoa que tenha sido lesionada, pode tomar para procurar seus direitos (SAFERNET, 2008).

A primeira coisa a se fazer, é preservar as provas do ato criminoso, segue as recomendações abaixo do Site SAFERNET:

> Imprima e salve: o conteúdo das páginas ou "o diálogo" do(s) suspeito(s) em salas de bate-papo ou mensagens de correio eletrônico (e-mail) ofensivas. É necessário guardar também os cabeçalhos das mensagens. Preserve as provas em algum tipo de mídia protegida contra alteração, como um CD-R ou DVD-R. Todas essas provas ajudam como fonte de informação para a investigação da polícia. No entanto, essas provas não valem em juízo, pois carece de fé pública. Uma alternativa é ir a um cartório e fazer uma declaração de fé pública de que o crime em questão existiu, ou lavrar uma Ata Notarial do conteúdo ilegal/ofensivo. Esses procedimentos são necessários porque, como a Internet é dinâmica, as informações podem ser tiradas do ar ou removidas para outro endereço a qualquer momento. Não esqueça: A preservação das provas é fundamental. Já houve casos de a Justiça brasileira ter responsabilizado internautas que não guardaram registros do crime on-line do qual foram vítimas (SAFERNET, 2008, p. 1).

Após isso, de posse de todas as provas a vítima deve procurar uma das Delegacias Especializadas em Crimes Cibernéticos, porém ainda não existe essas delegacias em todas as comarcas, mas a vítima pode e deve se dirigir a Delegacia de Polícia Civil mais próxima da sua moradia, a fim de fazer o boletim de ocorrência. E iniciar os processos cabíveis.

É possível também fazer denúncias anônimas, uma ferramenta disponível no site da SAFERNET, permite as denúncias de publicações de discriminação racial, homofóbicas, xenofóbicas, pornografia infantil e apologia ao nazismo, e ainda acompanhar as investigações. Para realizar a denúncia basta acessar o site (http://new.safernet.org.br/denuncie), após verificar o tipo de conteúdo e ofensa informe o link para a publicação. É interessante guardar os prints da publicação. O site Safernet têm diversas parcerias com órgãos importantes como a Polícia Federal, o Ministério Público Federal (MPF) e a Procuradoria-Geral Federal, e empresas como o Google, Facebook e o Twitter (SAFERNET, 2018).

O site do Conselho Nacional de Justiça também disponibiliza em sua plataforma um conteúdo referente o que são os crimes digitais e como denuncia-los e as leis que os tipificam (CNJ, 2018).

Publicar nas redes sócias conteúdos ofensivos não é liberdade de expressão e não deve ser confundida com tal. A ilusão de estar ileso e anônimo por trás das telas tem levado muitos internautas a publicarem ofensas as pessoas, sendo elas famosas ou não (CNJ, 2018).

A legislação brasileira possui duas leis que tipifica os crimes cometidos na Internet, essas alteram o código penal e institui penas para os crimes de invasão de computador, bem como vírus e códigos usados com o intuito de roubar senhas e informações (CNJ, 2018).

São estas a Lei dos Crimes Cibernéticos (12.737/2012), conhecida como Lei Carolina Dieckmann, que tipifica crime os atos de invasão de computadores, violação de dados, invasão e suspensão de sites, e o Marco Civil da Internet (Lei 12.965/2014), que protege informações e dados pessoais de usuários na rede (CNJ, 2018).

> "O Marco Civil da Internet também determinou que os Juizados Especiais são os responsáveis pela decisão sobre a ilegalidade ou não dos conteúdos. Isto se aplica aos casos de ofensa à honra ou injúria, que serão tratados da mesma forma como ocorre fora da rede mundial de computadores" (CNJ, 2018, p. 1).

Nos casos de racismo, homofobia, xenofobia, apologia nazista e pornografia infantil, é possível a denúncia anônima desses, no site da SAFERNET (CNJ, 2018).

6. ASPECTOS JURÍDICO-PENAIS RELACIONADOS AOS CRIMES INFORMÁTICOS

No frenesi das mudanças tecnológicas e com o constante crescimento de usuários da internet, tem crescido também o número de práticas licitas e ilícitas na rede. Não diferente de outras categorias de sociedade seja qual for, a internet também tem coisas boas e ruins, assim como o que é bom deve ser incentivado por todos responsáveis, o que é ruim deve ser excluído, evitado e no caso de cometido, deverá ser punido.

O uso da internet quando realizado para provocar dano ou constituir um crime tipificado, então o mesmo deverá ser reparado e os órgão competentes acionados para fazer cumprir as normas e leis cabíveis ao acontecido. Neste capítulo falamos sobre a responsabilidade civil e algumas subdivisões ou divisões do termo, para melhor compreensão do seu significado e visualização textual da sua importância.

6.1 Responsabilidade Civil

Responsabilidade como já diz o nome é o ato de arcar com as consequências dos próprios atos ou dos atos de outro indivíduo, essa responsabilidade torna-se obrigação jurídica quando há desrespeito ou violação de algum direito, é imprescindível a necessidade de compreender bem a responsabilidade civil, para reconhecer os direitos do próximo e o próprio direito e assim evitar as consequentes penalidades (MENEZES, 2017).

Qualquer atividade realizada deve ser feita com responsabilidade, isso inclui as ações de um individuo que havendo um ato ilícito, o mesmo deve acatar e reparar o patrimônio ou pessoa prejudicados, ou seja, “trata-se de uma obrigação pessoal que se resolverá em perdas e danos se houver nexo causal (relação de causalidade) entre o ato praticado pelo infrator e o dano sofrido pela vítima” (MENEZES, 2017, p. 1).

A responsabilidade civil é um termo oriundo do Direito Romano, um conjunto de leis, preceitos e princípios utilizado na antiguidade pela sociedade romana e seus domínios, criado para proteger o individuo de danos injustos causados por outros, “a forma de reparação desse dano, entretanto foi transformando-se ao longo do tempo, sofrendo desta forma uma evolução” (TRAJANO, 2015, p.1).

Com as consequentes evoluções a responsabilidade é hoje dividida em objetiva e subjetiva, “ela também pode ser dividida em responsabilidade contratual e extracontratual” (TRAJANO, 2015, p. 1).

Responsabilidade subjetiva é quando o causador de determinado dano por indução de culpa ou dolo comete um ato ilícito. Sendo que “a responsabilidade subjetiva se dará quando o causador do ato ilícito atingir este resultado em razão do dolo ou culpa em sua conduta, sendo obrigado a indenizar do dano causado apenas caso se consume sua responsabilidade” (CARDOSO, 2017, p. 2).

O Brasil se adéqua aos poucos as mudanças que ocorrem na responsabilidade civil e “no tocante a responsabilidade objetiva, o Brasil prever em sua Constituição Federal de 1946 a teoria da responsabilidade objetiva a qual foi mantida na Constituição federal de 1988” (TRAJANO, 2015, p. 2).

Responsabilidade objetiva é quando se torna necessário à indenização mesmo sem comprovação de culpa ou dolo, bastando apenas à comprovação do vínculo causador daquele fato. “O código civil por sua vez, adota a responsabilidade subjetiva como regra, sendo essas definidas nos artigos 186 e 187 do CC 2002” (CARDOSO, 2017, p. 3). Assim dispõe o Art. 186. “Aquele que por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dando a outrem, ainda que exclusivamente moral, comete ato ilícito”.

Na mesma linha de raciocínio, o art. 187 afirma que “Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé e pelos bons costumes” (BRASIL², 2020, p. 406-407).

Há também a classificação em responsabilidade contratual ou extracontratual, sendo que a primeira ocorre quando há a falta do cumprimento da

obrigação civil contratual, um ilícito ao dever especial estabelecido entre os contratantes. Nesse sentido, afirma-se que “a responsabilidade contratual é o resultado da violação de uma obrigação anterior, logo, para que exista é imprescindível à preexistência de uma obrigação” (LAMBERT, 2018 p.1).

Responsabilidade extracontratual conhecida também como aquiliana, é o incumprimento de uma regra, ou seja, a prática de ilícito por pessoa, “É a lesão a um direito sem que entre o ofensor e o ofendido preexista qualquer relação jurídica. Aqui ao contrário da contratual, caberá à vítima provar a culpa do agente” (SILVA, 2002, p.2).

A responsabilidade civil é mutável, se adéqua a cada mudança sofrida pela sociedade, e é preciso lembrar que com o advento da internet e o crescimento da tecnologia. Essas mudanças tornam-se cada vez mais rápidas, complexas e paradoxalmente necessárias. É preciso atenção às leis, regras e normas que estão sempre sendo atualizadas. É a mesma que preserva o direito do indivíduo contra a prática de danos, morais, emocionais e psicológicos (decorrentes dos chamados danos morais ou extrapatrimoniais), sendo possível além de uma indenização material, que seja também exigida uma indenização de cunho moral e em alguns casos se cogita até da responsabilidade de caráter estético (decorrente de lesões corporais que causam enfeixamento da vítima ou aleijões e/ou deformações) (SILVA, 2002).

De modo algum o mundo cibernético está livre de suas obrigações civis, do cumprimento dos direitos e deveres, uma vez que quando ocorre ato ilícito, o provedor, o usuário, o causador de ato criminoso, ou todos simultaneamente, devem ser identificados e para posteriormente serem punidos. Muitas vezes é difícil encontrar quem comete crimes na internet, mas com dedicação e conhecimento, um perito em informática pode ajudar a justiça á encontrar esses mal feitores, a fim de aplicar as punições cabíveis (MENEZES, 2017).

A tecnologia e a internet acabaram por munir criminosos para cometer atos ilícitos, e por acharem estar seguros de punições, qualquer um pode ser um potencial criminoso na rede, independente de sua idade ou localização. Atingindo bens e interesses que o estado deve tutelar, coibindo agressões contra tais bens através de penas privativas de liberdade, pela força coercitiva do Direito Penal;

desde 1960 que começaram a surgir os primeiros casos de uso dos computadores para a prática de crimes como sabotagem, chantagem e espionagem (MENEZES, 2017).

Hoje é necessário proteger não só os bens materiais, mas também o que desrespeita a vida pessoal, profissional e acadêmica com segurança com a finalidade de evitar invasões, utilizando-se de senhas e criptografia, da mesma forma são criadas leis que tipifique esses crimes, preferencialmente um tratado internacional aprovado. Como menciona Menezes (2017):

> "Afinal, não há crime sem lei anterior que o defina; em alguns casos os crimes são os mesmos já conhecidos, apenas executados de nova maneira; em outros casos é preciso nova tipificação penal. Deve-se analisar com cuidado a legislação penal já existente para tipificar os cybercrimes, e não apenas se acomodar com a possível falta de lei para não punir o criminoso digital" (Menezes, 2017, p. 3).

Ainda segundo Menezes, "na década de 80 os crimes ampliaram para o de estelionato, furto, de dinheiro em contas bancárias, introdução de vírus em computadores (crime de dano), trafico de drogas, sonegação fiscal e desrespeito aos direitos autorais" (MENEZES, 2017, p. 2).

6.2 Lei nº 12.737/2012 – Lei Carolina Dieckmann

Em maio de 2012, a atriz Carolina Dieckman passou por uma triste experiência, após ter sofrido ataques de hackers, que violando o e-mail da atriz fizeram downloads de 36 fotos e conversas íntimas, e ameaçaram a atriz a pagar R$ 10 mil para evitar a divulgação das imagens. A atriz não cedeu à chantagem e teve suas fotos divulgadas na Internet sem autorização (VEJA, 2013).

O caso ficou conhecido nacionalmente, e serviu para a criação da Lei n° 12.737/2012 apelidada de Lei Carolina Dieckman. A lei foi sancionada pela presidente da época Dilma Rousseff, em novembro daquele mesmo ano.

Essa lei tratou de tipificar os crimes informáticos, que anteriormente não havia:

> "Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências" (BRASIL[4], 2020).

A lei não apenas cobre os delitos de divulgação de fotos e imagem, mas uma série sequencial de delitos informáticos. Também aumentar a pena, caso o crime seja cometido contra o Presidente da República, do supremo, prefeitos e governadores e todo poder executivo e legislativo:

> 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" (BRASIL[4], 2020).

Além das alterações no Código Penal Brasileiro, que inseriu infrações cibernéticas no bojo da lei através da Lei 12.737/2012, apelidada de "Lei Carolina Dieckmann", temos ainda A Lei 8.069/90 (Estatuto da Criança e do Adolescente - ECA), a Lei de Software (Lei antipirataria nº 9.609/98), a Lei de Racismo (Lei nº 7.716/89) e a Lei de Segurança Nacional (Lei 7.170/83), compondo o conjunto de normas mais relevantes aplicáveis ao cibercrime.

6.3 Lei nº 12.965/2014 – Marco Civil da Internet

A Lei n° 12.965/2014 conhecida como Marco Civil da Internet, é a lei responsável por regular o uso da Internet no território Brasileiro, mediante a previsão de princípios, garantias, direitos e deveres para quem usa a Internet, bem como da determinação de diretrizes para a atuação do Estado.

Esta Lei foi sancionada em 23 de abril de 2014, pela presidente Dilma Rousseff, sendo que "o Marco Civil da Internet é considerado uma das mais avançadas leis no mundo no assunto da regulação da Internet, especificamente na garantia da neutralidade da rede" (Bragatto, 2015, p. 238).

A Lei 12.965 estabelece os limites, princípios e determina diretrizes nos direitos e deveres do uso da Internet no Brasil, com o intuito de disciplinar, mas preservando a liberdade de expressão:

> "Art. 1º Esta Lei 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.
>
> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
>
> I - o reconhecimento da escala mundial da rede;
>
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
>
> III - a pluralidade e a diversidade;
>
> IV - a abertura e a colaboração;

> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VI - a finalidade social da rede" (BRASIL[5], 2020).

O Marco Civil da Internet não priva o direito do cidadão a rede, ele garante o acesso à Internet no exercício da cidadania. Ele apenas garante outros direitos da pessoa, como a privacidade, a inviolabilidade da intimidade, acessibilidade, dentre outros, como garantias para o bem-estar social**.**

A mencionada lei providencia os princípios que regulam o uso da internet no Brasil, estes estão enumerados no seu artigo 3°, dentre os quais, o princípio da proteção da privacidade e dos dados pessoais. (TJDFT, 2016). Assim dispõe:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> “I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - proteção da privacidade;
>
> III - proteção dos dados pessoais, na forma da lei;
>
> IV - preservação e garantia da neutralidade de rede;
>
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - preservação da natureza participativa da rede;
>
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
>
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte” (TJDFT, 2016, p. 1).

O mencionado artigo 3° enumera os princípios dentre os quais, o princípio da proteção da privacidade e dos dados pessoais que a lei regulamenta (TJDFT, 2016).

6.4 Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD)

A Lei nº 13.709 de 2018, denominada nova Lei Geral de Proteção de Dados, a famosa LGPD, “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade” (BRASIL[6], 2020, p. 1).

De acordo com Pinheiro (2018):

> “A lei n° 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por se tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica” (Pinheiro, 2018, p. 9).

Esta nova lei está dividida em 10 capítulos e 65 artigos, sendo menor que sua referência europeia de sigla GDPR, que tem 11 capítulos e 99 Artigos (PINHEIRO, 2018).

Os capítulos tratam do seguinte:

> “Cap. I
>
> DISPOSIÇÕES PRELIMINARES;
>
> Cap. II
>
> DO TRATAMENTO DE DADOS PESSOAIS;
>
> Cap. III
>
> DOS DIREITOS DO TITULAR;
>
> Cap. IV
>
> DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO;
>
> Cap. V
>
> DA TRANSFERÊNCIA INTERNACIONAL DE DADOS;
>
> Cap. VI
>
> DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS;
>
> Cap. VII

> DA SEGURANÇA E DAS BOAS PRÁTICAS;
>
> Cap. VII
>
> DA SEGURANÇA E DAS BOAS PRÁTICAS;
>
> CAPÍTULO VIII
>
> DA FISCALIZAÇÃO;
>
> Cap. IX
>
> DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE;
>
> Cap. X
>
> DISPOSIÇÕES FINAIS E Transitórias" (BRASIL[6], 2020).

A LGPD regulamenta o tratamento de dados de clientes e usuários por parte das empresas. Entende-se como tratamento de dados qualquer processo que envolva dados pessoais, como armazenamentos, processamentos, transferências, enfim qualquer tipo de utilização. As empresas que descumprirem os procedimentos previstos nesta lei ficaram sujeitas a multas de até R$ 50 milhões (PASSARELLI, 2019).

Contudo, a LGPD encontra-se em período de *vacatio legis* (vacância da lei), em que a população se organiza para se adequar aos ditames legais desta nova norma, tendo sido o início da vigência da citada Lei adiado para 2021, em virtude do isolamento social e da crise sanitária instaurada pela pandemia do Covid-19, no Brasil e no mundo (BRASIL[6], 2020).

Há leis que regulam o uso da internet, mas nenhuma que preveja tão pouco traga a punição para os tipos de infrações mais graves praticadas on-line, especificamente. A maneira de legislar do Poder Judiciário brasileiro é temerária e, por vezes, incompreensível, pois estabelece padrão de conduta relacionado à sociedade, ao invés de prever e determinar punições a condutas erráticas, especialmente quando se fala de delitos de alto nível como o roubo ou o sequestro de informações (PINHEIRO, 2018).

A Lei de Segurança Nacional (Lei nº 7.170/83) é outra norma que prevê delitos cibernéticos, porém, relaciona-se apenas aos crimes contra a segurança

nacional, a ordem política e social, não prevendo quaisquer das outras condutas mais comumente praticadas através da internet. A Lei de Software, por outro lado, que dispõe sobre a propriedade intelectual de programas de computador, também não prevê a prática de condutas delituosas online.

7 CONCLUSÃO

O presente trabalho abordou a questão dos crimes cibernéticos no Brasil, fazendo um breve estudo acerca da legislação brasileira atual, com o objetivo de verificar a existência de proteção adequada às vítimas de crimes informáticos.

Vivencia-se de fato uma era virtual e os crimes nesse meio estão evoluindo, pela falsa aparência de impunidade dadas as dificuldades em se punir alguém que se esconde por trás da rede.

O mundo cibernético é imenso, seus integrantes de difícil localização; muitas vezes um aparente sujeito no mundo dos cibercrimes representa na realidade muitos. Entretanto existem garantias constitucionais que visam o direito à vida privada, à honra e à intimidade do ser humano. A observância ou o respeito a esses direitos evitam que fatos sejam expressos, causando constrangimento ao indivíduo, de modo que, se cada vítima de um ataque, uma vez munida do conhecimento dos seus direitos, busque amparo na lei, e assim, poderá inibir a ocorrência de novos ataques.

Sobre os principais crimes informáticos, pode-se considerar que estes estão amparados pela legislação e que as normas preveem punições adequadas a cada ato criminoso virtual cometido.

A lei Carolina Dieckman 12.737/2012 tratou de tipificar esses crimes, condutas ilícitas que antes não eram definidas como delitos pela lei, trazendo clareza aos tipos de punições cabíveis a cada situação de exposição da vítima nos meios virtuais.

O Marco Civil da Internet 12.965/2014, que é uma das mais avançadas leis que punem delitos informáticos no mundo, especialmente na neutralidade da rede, estabelecendo limites, princípios e determinando diretrizes nos direitos e deveres do uso da Internet, garantindo a acessibilidade com privacidade e inviolabilidade da intimidade para o bem social. Antes de esta lei entrar em vigor a sociedade estava à mercê de qualquer tipo de delito cometido na internet, em mídias sociais e por meio de outros mecanismos, por qualquer pessoa, pois diante do avanço das tecnologias e do amplo acesso à rede, assim como o acesso irrestrito por parte de alguns sujeitos, a sociedade – de um modo geral - encontra-se em

posição de vulnerabilidade, podendo sofrer ataques por meio da internet, sendo extremamente útil a previsão de direitos e garantias por essa legislação.

Também cabe ressaltar a lei Geral de Proteção de Dados (LGPD), foi elaborada com o intuito de fornecer garantias à privacidade de dados pessoais, direitos e deveres no tocante ao uso da Internet no país.

É fato que a liberdade de expressão é um direito facultado a toda a sociedade, porém, alguns excessos são cometidos no meio virtual, violam o direito à privacidade, e são, erroneamente, sustentados no argumento da liberdade de se expressar.

Porém, nenhum direito é absoluto, é dever do Estado coibir e corrigir os excessos cometidos no exercício do direito. Ademais, quando um direito viola outro é caracterizado como abuso ou exagero de um deles. Porém, existe uma ordem para que a sociedade flua de forma justa e pacífica, e essa ordem é imposta através do Direito, da lei, das normas de cunho jurídico, por serem cogentes, impositivas, sendo necessário que haja normas de caráter punitivo, mas também de cunho educacional, no sentido de que possibilite a conscientização de que não vale a pena.

Podemos concluir que o Brasil está bem amparado quanto às leis e medidas protetivas no âmbito virtual, porém é necessário comentar a necessidade de uma justiça mais rápida e efetiva e de uma governança adequada que resulte em uma autuação de sucesso a fim de coibir o aparecimento cada vez maior de criminosos Cibernéticos.

Assim sendo, constatada a importância desse assunto, torna-se necessário o desenvolvimento de estratégias pedagógicas, como instrumento educativo e a observância dos direitos, deveres e consequentes penalidades, caso ocorram infrações desses direitos, para que se previnam novos crimes e possíveis vítimas, pois para todos os males a prevenção é o melhor caminho.

8. REFERÊNCIAS

AMARAL, 2004, **Inclusive Education: History, Prejudices, and School and Family** Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1414-98932015000401106. Acesso em: 10 maio 2020.

ASSIS, 2018. Cassandra Lopes de et al. **A tutela da privacidade na sociedade da informação: O direito ao esquecimento no ambiente virtual pelos tribunais superiores no Brasil**. 2018. Trabalho de Conclusão de Curso. Disponível em: https://attena.ufpe.br/bitstream/123456789/33993/1/TCC%20-%20Cassandra%20Lopes%20de%20Assis%202.0%20Ajustado%20%C3%A0%20Revis%C3%A3o%20do%20Orientador%20%281%29.pdf Acesso em: 10 maio 2020.

BRASIL, 2020 **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 fev. 2020.

BRASIL[1], 2020. **Lei n° 10.406, de 10 de Janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 10 mar. 2020.

BRASIL[2], 2020. **Decreto-lei no 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1942. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 10 mar. 2020.

BRASIL[3], 2020. **Decreto-lei no 11.829, de 25 de novembro de 2008,** Presidência da República Casa Civil Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm Acesso em: 11 jul. 2020.

BRASIL[4], 2020. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências,** LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 11 jul. 2020.

BRASIL[5], 2020. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Presidência da República Casa Civil Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 jul. 2020.

BRASIL[6], 2020. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.** Presidência da República Casa Civil Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 11 jul. 2020.

BRASIL[7], 2020. **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988.** Presidência da República Casa Civil Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 jul. 2020.

BRASIL ESCOLA, 2017**, A DOUTRINA DA PROTEÇÃO INTEGRAL TRAZIDA PELO ESTATUTO DA CRIANÇA E DO ADOLESCENTE E AS PROPOSTAS DE REDUÇÃO DA MAIORIDADE PENAL**. Disponível em: https://monografias.brasilescola.uol.com.br/direito/a-doutrina-protecao-integral-trazida-pelo-estatuto-crianca-adolescente.htm. Acesso em: 04 abr. 2020.

BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso; NICOLÁS, Maria Alejandra. **A segunda fase da consulta do marco civil da internet: como foi construída, quem participou e quais os impactos**. Revista Eptic, v. 17, n. 1, p. 237-255, 2015.

CARDOSO, 2017. Philipe Monteiro. Você sabe o que é responsabilidade objetiva e subjetiva?. **Jusbrasil**, [S. l.], [S.a.], [S.n.], [S.ed.], [S.p.], 201?. Disponível em: https://philipemcardoso.jusbrasil.com.br/artigos/474353684/voce-sabe-o-que-e-responsabilidade-objetiva-e-subjetiva. Acesso em: 10 mar. 2020.

CARVALHO, 2006. Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. Dissertação (Mestrado em Engenharia de Sistemas e Computação), Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006. Disponível em: http://www.nethistory.info/Resources/Internet-BR-Dissertacao-Mestrado-MSavio-v1.2.pdf. Acesso em: 15 set. 2019.

CIBERCRIMES, 2019. Lei Azeredo e Lei Carolina Dickman. **Artigo 19**, São Paulo, [S.a.], [S.n.], [S.ed.], [S.p.], [S.d]. Disponível em: https://artigo19.org/liberdadedigital/category/cibercrimes. Acesso em: 15 fev. 2020.

CONSELHO NACIONAL DE JUSTIÇA, (CNJ) 2018. **Crimes digitais:** o que são, como denunciar e quais leis tipificam como crime?**,** 2018. Disponível em: <https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/>. Acesso em: 28 jun. 2020.

CONSULTOR JURIDICO, 2013, **“Direito ao esquecimento é garantido por Turma do STJ” -** Disponível em: https://www.conjur.com.br/2013-out-21/direito-esquecimento-garantido-turma-stj-enunciado-cjf. Acesso em: 23 maio 2020.

CONSULTOR JURIDICO[1], 2020, **“Jornalista é condenado por ligar mulher a triângulo amoroso com Ronaldinho”,** 2020. Disponível em: https://www.conjur.com.br/2020-fev-11/jornalista-condenado-sugerir-entre-mulher-ronaldinho Acesso em: 23 maio 2020.

CONSULTOR JURIDICO[2], 2018 “**Minas Gerais terá vara federal especializada em crimes cibernéticos”** - Disponível em: https://www.conjur.com.br/2018-abr-11/minas-gerais-vara-federal-especializada-crimes-ciberneticos Acesso em: 28 jun. 2020.

Convergência Digital, 2018. **Vazamento de dados: mais de 4,5 bilhões de registros foram violados no 1º semestre de 2018,** Link Disponível em: http://sis-publique.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=49169&sid=18. Acesso em: 12 maio 2020.

Daniel Menah Cury Soares, 2019. **Crimes informáticos: Uma breve resenha e apontamento de complicações,** Disponível em: https://www.migalhas.com.br/depeso/308978/crimes-informaticos-uma-breve-resenha-e-apontamento-de-complicacoes Acesso em: 01 jul. 2020.

DELGADO, Mário Luiz, 2005. **Direitos da personalidade nas relações de família**. V Congresso Brasileiro de Direito de Família, 2005. Disponível em: http://www.ibdfam.org.br/_img/congressos/anais/34.pdf. Acesso em: 06 jul. 2020.

DONEDA, Danilo, 2006. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. Acesso em: 15 jan. 2020.

D’URSO, Luiz Augusto Filizzola, 2017. Cibercrime: perigo na internet. **Estadão**, São Paulo, [S.a.], [S.n.], [S.ed.], [S.p.], 25 jul. 2017. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/cibercrime-perigo-na-internet. Acesso em: 16 fev. 2020.

FERNANDES T Alves, Lauren Juliê L**, Exposição nas redes sociais sem autorização**. 2019. Disponível em: https://laurenfernandes.jusbrasil.com.br/artigos/686195090/exposicao-nas-redes-sociais-sem-autorizacao#:~:text=Havendo%20a%20veicula%C3%A7%C3%A3o%20de%20image Acesso em: 22 jun. 2020.

FONSECA. André Luiz Jesus. Ética na internet existe?. **Webartigos**, [S. l.], [S.a.], [S.n.], [S.ed.], [S.p.], 08 fev. 2011. Disponível em: https://www.webartigos.com/artigos/etica-na-internet-existe/58761. Acesso em: 10 mar. 2020.

FRANÇA, Rubens Limongi, 2010. **Direitos da personalidade – Coordenadas Fundamentais,** Revista do Advogado, São Paulo, AASP, n. 38, p. 5; Manual de direito civil, 3. ed., São Paulo, RT, 1981. 06 jul. 2020.

GARCIA, Gabriel, 2015. 1 bilhão de registros de dados foram roubados na internet em 2014, diz pesquisa. **Exame**, São Paulo, [S.a.], [S.n.], [S.ed.], [S.p.], 12 dez. 2015. Disponível em: https://exame.abril.com.br/tecnologia/1-bilhao-de-registros-de-dados-foram-roubados-na-internet-em-2014-diz-pesquisa. Acesso em: 12 dez. 2019.

GILABERTE, Bruno. **Lei nº 13.718/2018: importunação sexual e pornografia de vingança.** Disponível em: <https://canalcienciascriminais.jusbrasil.com.br/artigos/629753885/lei-n-13718-2018-importunacao-sexual-e-pornografia-de-vinganca>. Acesso em: 10 abr. 2020.

HOSANG, Alexandre. Política Nacional de Segurança Cibernética: uma necessidade para o Brasil. **Escola Superior De Guerra**, Rio De Janeiro, 2011.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes de Informáticos**. São Paulo: Saraiva, 2016. Acesso em: 28 jun. 2020.

JUS - **Direitos da personalidade** Publicado em 01/2017 por: Anne de Fátima Pedrosa Araújo, Natália Bernadeth Fernandes Rodrigues. Disponível em: https://jus.com.br/artigos/55019/direitos-da-personalidade Acesso em: 28 jun. 2020.

JUSNATURALISMO, 2017 - GONZAGA, Alvaro de Azevedo. **Direito natural e jusnaturalismo**. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tema: Teoria Geral e Filosofia do Direito. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga, André Luiz Freire (coord. de tema). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017.Disponível em: https://enciclopediajuridica.pucsp.br/verbete/63/edicao-1/direito-natural-e-jusnaturalismo Acesso em: 20 maio 2020.

Jusbrasil, 2016. Classificação dos Crimes Digitais, **Publicado por Victor Augusto Tateoki**. Disponível em: https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais. Acesso em: 03 fev. 2020.

Jusbrasil, 2018. **A violação dos direitos da personalidade pelas redes sociais**, Publicado por Luana dos Santos Silva Afonso e Carlos Eduardo Malinowski. Disponível em: https://jus.com.br/artigos/64335/a-violacao-dos-direitos-da-personalidade-pelas-redes-sociais#:~:text=Diversos%20acontecimentos%20da%20hist%C3%B3ria%20mundial,pessoa%20humana%20acima%20do%20patrim%C3%B4nio.&text=Diante%20disso%2C%20o%20Direito%20P%C3%BAblico,devendo%20para%20tanto%20defend%C3%AA%2Dlos. Acesso em: 04 jul. 2020.

KAZMIERCZAK, 2007. Luiz Fernando. Responsabilidade civil dos provedores de internet. **Informativo Migalhas**, Ribeirão Preto (SP), [S.a.], n. 1639, [S.ed.], [S.p.], 20 abr. 2007. Disponível em: https://www.migalhas.com.br/depeso/38123/responsabilidade-civil-dos-provedores-de-internet. Acesso em: 10 mar. 2020.

KERR, 2011, Vera Kaiser Sanches. **A disciplina, pela legislação processual penal brasileira, da prova pericial relacionada ao crime informático praticado por meio da internet.** São Paulo: USP, 2011. Disponível em: <http://www.teses.usp.br/teses/ disponiveis/3/3142/tde-07112011-115417/publico/Dissertacao_Vera_Kaiser_Sanches_ Kerr.pdf> Acesso em: 20 abr. 2020.

LAMBERT, 2018. Henrique. **Responsabilidade civil**. Jusbrasil, [S. l.], [S.a.], [S.n.], [S.ed.], [S.p.], 201?. Disponível em: https://henriquelambert.jusbrasil.com.br/artigos/519779120/responsabilidade-civil. Acesso em: 10 mar. 2020.

LEI 'Carolina Dieckman', que pune invasão de Pcs, entra em vigor. **G1**, São Paulo, [S.a.], [S.n.], [S.ed.], [S.p.], 01 abr. 2013. Disponível em: http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html. Acesso em: 08 ago. 2019.

LEI de Imprensa - Lei 5250/67 | Lei no 5.250, de 9 de fevereiro de 1967. **Jusbrasil**, [S. l.], [S.a.], [S.n.], [S.ed.], [S.p.], 196?. Disponível em: https://presrepublica.jusbrasil.com.br/legislacao/128588/lei-de-imprensa-lei-5250-67?print=true. Acesso: 15 fev. 2020.

LENZA, Pedro. **Direito Constitucional Esquematizado**. 16. ed. São Paulo: **Saraiva**, 2012.

MALDONADO, Viviane Nóbrega. **Direito ao esquecimento**. Barueri, SP: **Novo Século Editora**, 2017.

MEDEIROS, 2015, Rafael. **OS DIREITOS DA PERSONALIDADE**. Revista Científica **Semana Acadêmica. Fortaleza**, ano MMXV, Nº. 000076, 02/12/2015. Disponível em: https://semanaacademica.org.br/artigo/os-direitos-da-personalidade Acessado em: 19 fev. 2020.

MENEZES, 2017, Rafael José**. Responsabilidade Civil na internet e Cybercrimes.** Rafael de Menezes, Recife, [S.a.], [S.n.], [S.ed.], [S.p.], 10 nov. 2017. Disponível em. http://rafaeldemenezes.adv.br/artigo/responsabilidade-civil-na-internet-e-cybercrimes. Acesso em 10 mar. 2020.

MORAES PEREIRA, 2010, Leidiane, **BULLYING**: Da brincadeira de criança à tragédia social www.pergamum.univale.br › pergamum › tcc › Bullying, Governador Valadares, 2010. Acesso em 10 fev. 2020.

NAÇÕES UNIDAS BRASIL, 2015, **No Brasil quase 60% das pessoas estão conectadas à internet, afirma novo relatório da ONU**. Brasília, [S.a.], [S.n.], [S.ed.], [S.p.], 21 set. 2015. Disponível em: https://nacoesunidas.org/no-brasil-quase-60-das-pessoas-estao-conectadas-a-internet-afirma-novo-relatorio-da-onu/. Acesso em: 15 fev. 2020.

NETO, João Araújo Monteiro. Crimes informáticos uma abordagem dinâmica ao direito penal informático. **Pensar-Revista de Ciências Jurídicas**, v. 8, n. 1, p. 39-54, 2010.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Paris: ONU, 1948. Disponível em: https://www.un.org/en/universal-declaration-human-rights. Acesso em: 10 mar. 2020.

ONU NEWS, **Estudo da ONU revela que mundo tem abismo digital de gênero**, 2019. Disponível em: https://news.un.org/pt/story/2019/11/1693711 Acesso em: 08 abr. 2020.

PAESANI, 2000, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil. São Paulo, Atlas: 2000.

PASSARELLI, 2019 Vinícius. **LGPD: entenda o que é a Lei Geral de Proteção de Dados Pessoais**, 2019. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais/ Acesso em 18 jul. 2020.

PINHEIRO 2006, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal.** Disponível em: https://d1wqtxts1xzle7.cloudfront.net/45640575/ciberneti.pdf?1463312299=&response-content-disposition=inline%3B+filename%3DCRIMES_VIRTUAIS_UMA_ANALISE_DA_CRIMINALI.pdf&Expires=1596051104&Signature=biiSq3q-dhq7fFeww-41FlgFvmrEfhw0SDFtCGOwaFOwcq1wliOgf8P30nQi0HpaOHYbLl2jOwiZ3IuE31dYalZDC978TZGLHag~rh-Gk4uT7~RoCbsnZMjXaEU~Q5mqgQRYxxDGidF-M2VGdGxxQM68dP4tSuTA5CExigXMq7QHWTEr-WU--5j88yitWFvDyaPVF0YMTnXiPQUgZZ9t6bbTCBBQ8jr5H34CibJlKYnEB6rQtEwvG6UxRLj1x9TehVnrL38cPZzGvUoFYjf6cfYFNLxQwIAyHML5XxXj0YDvA~VZ8Qz5Bwxb85s3qPAAo-E173-o1l0c2j1k1948oA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em 18 jul. 2020.

PINHEIRO 2018, Patricia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD. Saraiva Educação SA, 2020.

PODER 360 2018, **Denúncias de crimes cibernéticos aumentaram 109,9% em 2018, diz associação**. Disponível em: https://www.poder360.com.br/justica/denuncias-de-crimes-ciberneticos-aumentaram-1099-em-2018-diz-associacao/. Acesso em 18 jul. 2020.

R7, 2017, Portal de notícias - **Homem é vítima de calúnia na internet ao ter foto divulgada com acusação de estuprar e matar neto**. Disponível em: https://noticias.r7.com/bahia/homem-e-vitima-de-calunia-na-internet-ao-ter-foto-divulgada-com-acusacao-de-estuprar-e-matar-neto-26032017 Acesso em 18 jul. 2020.

REVISTA CIENTÍFICA ELETRÔNICA DO CURSO DE DIREITO – ISSN: 2358-8551 13ª Edição – Janeiro de 2018 – Periódicos Semestral, **CRIMES CIBERNÉTICOS E A FALSA SENSAÇÃO DE IMPUNIDADE**.
Disponível em: faef.revista.inf.br/arquivos_destaque. Acesso em: 10 mar. 2020.

ROCHA, 2017, Rafael. **Direito ao esquecimento**. Jus, Teresina, [S.a.], [S.n.], [S.ed.], [S.p.], dez. 2017. Disponível em: https://jus.com.br/artigos/62577/direito-ao-esquecimento. Acesso em: 10 mar. 2020.

RULLI JÚNIOR, Antonio; RULLI NETO, Antonio. **Direito ao esquecimento e o superinformacionismo: apontamentos no direito brasileiro dentro do contexto de sociedade da informação.** Revista Esmat, Palmas, ano 5, n. 6, p. 11-30, jul/dez 2013. Disponível em: http://esmat.tjto.jus.br/publicacoes/index.php/revista_esmat/article/view/57/63. Acesso em: 20 jan. 2020.

SAFERNET, 2008; PREVENÇÃO – **CALÚNIA/INJÚRIA/DIFAMAÇÃO**.
https://www.safernet.org.br/site/prevencao/orientacao/calunia Acesso em: 02 jul. 2020.

SALOMÃO, Lídia. **A repercussão civil do caso Cicarelli**. Jurisway, [S.l.], [S.a.], [S.n.], [S.ed.], [S.p.], [S.d]. Disponível em: https://www.jurisway.org.br/v2/reflexo.asp?idmodelo=2029&id_area=24. Acesso em: 02 abr. 2020.

SCHERCHTER, Luis Menasche. A Vida e o Legado de Alan Turing para a Ciência. *In*: Palestra Espacial, 2016, Rio de Janeiro. [**Anais**]. Rio de Janeiro: DCC/UFRJ, 2016. Disponível em: https://dcc.ufrj.br/~luisms/turing/Seminarios.pdf. Acesso em: 03 jun. 2019.

SILVA, 2016, Fernanda Tatiane da; PAPANI, Fabiana Garcia. **Um pouco da história da criptografia**. *In*: SEMANA ACADÊMICA DE MATEMÁTICA DA UNIOESTE, 22., 2016, Cascavel (PR). **Anais** [...]. Cascavel (PR): EDUNIOESTE, 2016. Disponível em: http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/16.pdf. Acesso em: 18 abr. 2020.

SILVA, 2002, Giselle Miranda Ratton. **Responsabilidade Contratual e Extracontratual**. **Direitonet**, [S.l.], [S.a.], [S.n.], [S.ed.], [S.p.], 13 set. 2002. Disponível em: https://www.direitonet.com.br/artigos/exibir/874/Responsabilidade-contratual-e-extracontratual. Acesso em: 10 mar. 2020.

SOARES, 2016, Will. **Denunciados por ofensas a Maju tinham verdadeiro exército, diz MP**. G1, São Paulo, [S.a.], [S.n.], [S.ed.], [S.p.], 22 jun. 2016. Disponível em: http://g1.globo.com/sao-paulo/noticia/2016/06/denunciados-por-ofensas-maju-tinham-verdadeiro-exercito-diz-mp.html. Acesso em: 02 out. 2019.

SOUZA, 2018. Carlos Affonso Souza; TEFFÉ, Chiara Spadaccini de Teffé. **O STJ e o direito ao esquecimento**: em que medida essa figura oferece tutela ainda não alcançada pelo exercício dos direitos à imagem, privacidade e honra?. Jota, São Paulo, [S.a.], [S.n.], [S.ed.], [S.p.], 05 abr. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-stj-e-o-direito-ao-esquecimento-05042018. Acesso em: 02 abr. 2020.

SUPERINTENDÊNCIA DA ZONA FRANCA DE MANAUS. **SUFRAMA Cidadão**: **direitos e deveres**. Manaus: SUFRAMA, 2005. Disponível em: http://www.suframa.gov.br/cidadao/direitosedeveres.cfm. Acesso em: 10 mar. 2020.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Provedores, redes sociais e conteúdos ofensivos: o papel do STJ na definição de responsabilidades**. Jusbrasil, [S. l.], [S.a.], [S.n.], [S.ed.], [S.p.], 201?. Disponível em: https://stj.jusbrasil.com.br/noticias/499617832/provedores-redes-sociais-e-conteudos-ofensivos-o-papel-do-stj-na-definicao-de-responsabilidades. Acesso em: 30 jan. 2020.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Justiça usa Código Penal Para Combater Crime Virtual**. Jusbrasil, [S. l.], [S.a.], [S.n.], [S.ed.], [S.p.], 200?. Disponível em: https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual. Acesso em: 10 set. 2019.

TARTUCE, Flávio. **Direito ao esquecimento. Xuxa x Google. Julgamento no STF**. Jusbrasil, [S. l.], [S.a.], [S.n.], [S.ed.], [S.p.], 201?. Disponível em: https://flaviotartuce.jusbrasil.com.br/noticias/142265662/direito-ao-esquecimento-xuxa-x-google-julgamento-no-stf?ref=serp. Acesso em: 02 abr. 2020.

TATEOKI, Victor Augusto. **Classificação dos crimes digitais**, 2016. Disponível em: https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais. Acesso em: 28 jun. 2020.

TOLEDO, Marcelo. **Hackers invadem sistema do Hospital do Câncer de Barretos e pedem regaste**. Folha de São Paulo, São Paulo, [S.a.], [S.n.], [S.ed.], [S.p.], 28 jun. 2017. Disponível em: https://www1.folha.uol.com.br/cotidiano/2017/06/1896638-hackers-invadem-sistema-do-hospital-de-cancer-de-barretos-e-pedem-resgate.shtml. Acesso em: 05 jul. 2019.

TRAJANO, 2015, Thiago. **Responsabilidade Civil: resumo prático**. Jus, Teresina, [S.a.], [S.n.], [S.ed.], [S.p.], fev. 2015. Disponível em: https://jus.com.br/artigos/36698/responsabilidade-civil-resumo-pratico. Acesso em: 10 mar. 2020.

TRUZZI, 2015, Gisele; DAOUN, Alexandre. Crimes informáticos: o direito penal na era da informação. In: **Proceedings of the Second International Conference of Forensic Computer Science**. 2015. p. 115-120.

TJDFT – por ACS, 2016. **Marco Civil da Internet.** Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet#:~:text=O>. Acesso em: 07 jul. 2020.

VALERA 2019, Paulo Vinícius de Carvalho, MISAKA, Marcelo, Yukio **CRIMES VIRTUAIS E A LEGISLAÇÃO BRASILEIRA** Disponível em: https://servicos.unitoledo.br/repositorio/handle/7574/2268. Acesso em: 07 jul. 2020.

VEJA, 2013, Por James Della Valle, **Lei Carolina Dieckmann entra em vigor nesta terça-feira.** Disponível em: https://veja.abril.com.br/tecnologia/lei-carolina-dieckmann-entra-em-vigor-nesta-terca-feira/. Acesso em: 15 jun. 2020.

VIANA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos do direito penal informático.** Belo Horizonte: UFMG, 2001. Disponível em: http://www.bibliotecadigital.ufmg.br/dspace/handle/1843/BUOS-96MPWG. Acesso em: 15 jun. 2020.

VIANA, 2015, Tulio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013, Disponível em: https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais. Acesso em: 15 jun. 2020.

WENDT, 2016, Emerson; NOGUEIRA, Jorge Higor Vinicius Nogueira. **Crimes cibernéticos:** ameaças e procedimentos de investigação**.** 2. ed. Rio de Janeiro: Brasport, 2013. Acesso em: 29 jun. 2020.