

**FACULDADE EVANGÉLICA DE RUBIATABA
CURSO DE DIREITO
ERNANES ADOLFO DE CARVALHO GUNDIM**

**A TIPIFICAÇÃO DOS CRIMES VIRTUAIS: A DIVULGAÇÃO DE
IMAGENS ÍNTIMAS (NUDES) SEM AUTORIZAÇÃO E A INFLUÊNCIA DAS LEIS
12.737 DE 2012 E 12.965 DE 2012 NA APURAÇÃO E PUNIÇÃO AOS INFRATORES
DESSE TIPO DE CRIME VIRTUAL**

**RUBIATABA/GO
2018**

ERNANES ADOLFO DE CARVALHO GUNDIM

**A TIPIFICAÇÃO DOS CRIMES VIRTUAIS: A DIVULGAÇÃO DE
IMAGENS ÍNTIMAS (NUDES) SEM AUTORIZAÇÃO E A INFLUÊNCIA DAS LEIS
12.737 DE 2012 E 12.965 DE 2012 NA APURAÇÃO E PUNIÇÃO AOS INFRATORES
DESSE TIPO DE CRIME VIRTUAL**

Monografia apresentada como requisito parcial
à conclusão do curso de Direito da Faculdade
Evangélica de Rubiataba, sob a orientação do
professor Especialista Gláucio Batista da
Silveira.

**RUBIATABA/GO
2018**

ERNANES ADOLFO DE CARVALHO GUNDIM

**A TIPIFICAÇÃO DOS CRIMES VIRTUAIS: A DIVULGAÇÃO DE
IMAGENS ÍNTIMAS (NUDES) SEM AUTORIZAÇÃO E A INFLUÊNCIA DAS LEIS
12.737 DE 2012 E 12.965 DE 2012 NA APURAÇÃO E PUNIÇÃO AOS INFRATORES
DESSE TIPO DE CRIME VIRTUAL**

Monografia apresentada como requisito parcial
à conclusão do curso de Direito da Faculdade
Evangélica de Rubiataba, sob a orientação do
professor Especialista Gláucio Batista da
Silveira.

MONOGRAFIA APROVADA PELA BANCA EXAMINADORA EM 21/07/2018

Especialista Gláucio Batista da Silveira
Orientador
Professor da Faculdade Evangélica de Rubiataba

Mestre Rogério Gonçalves Lima
Examinador
Professor da Faculdade Evangélica de Rubiataba

Especialista Fabiana Savini B. P. de A. Resende
Examinador
Professor da Faculdade Evangélica de Rubiataba

“Dedico este trabalho primeiramente a Deus, por ser essencial em minha vida, autor de meu destino, meu guia, socorro presente na hora da angústia e em todo caminho percorrido para chegar até aqui, ao meu pai Sebastiao C. Gundim, minha mãe Dilma G. Carvalho Gundim e a minha Irma Alyne C. Gundim.”

AGRADECIMENTOS

A Deus, por ter me dado saúde e força para superar todos os obstáculos que tive pelo caminho.

Ao meu orientador Gláucio B. da Silveira, pelo suporte no pouco tempo que lhe coube, pelas suas correções e incentivos.

Aos meus pais, pelo amor, incentivo e apoio incondicional.

E a todos que direta e indiretamente fizeram parte da minha formação, o meu muito obrigado.

EPIGRAFE

“Porque sou eu que conheço os planos que tenho para vocês”, diz o Senhor, “planos de fazê-los prosperar e não de causar dano, planos de dar a vocês esperança e um futuro.”

(Jeremias 29:11)

RESUMO

O objetivo desta monografia é examinar a tipificação no direito penal do crime virtual de divulgação de imagens íntimas sem autorização. Os objetivos específicos direcionam-se no sentido de retratar a evolução da prática dos crimes virtuais associado pelo aumento do uso da internet nos últimos anos, mostrar a incorporação pelo Direito Penal de dispositivos que sancionam os crimes virtuais, apontar no Direito Penal a tipificação do crime de divulgação de imagens íntimas sem autorização. Para atingimento deste objetivo o autor desenvolveu o estudo com o método de abordagem dedutivo, onde a fonte principal de conteúdo para essa pesquisa são as leis que alteraram o Código Penal e a tipificação desses direitos dos usuários da internet, atualmente conhecidas como práticas ilícitas. Descrevendo uma pesquisa dentro do Código Penal e das leis que normatizaram essas condutas, assim como um levantamento conceitual bibliográfico desse assunto. O direito brasileiro apresentou uma demora considerável para positivação dos crimes virtuais, permitindo com isso que se proliferasse a ação de criminosos, que encontraram na internet um campo fértil de atuação, especialmente marcada pelo despreparo das pessoas no uso da rede mundial de computadores e na ausência de proteção do Estado quanto à regulamentação dessa rede. A internet no Brasil teve origem na década de 1980, no seu final, tendo como expansão nas décadas de 1990 e 2000, atingindo grande parte dos lares brasileiros e se tornando uma febre na sociedade brasileira, associada a uma evolução tecnológica. O tema objeto da pesquisa é a tipificação do crime virtual de divulgação de imagens íntimas sem autorização, popularmente conhecido como nudes. Descrevem-se nessa monografia os posicionamentos das jurisprudências brasileiras em torno dessa disposição de fotos “nudes” sem a devida autorização, com base nos artigos 154-A e 154-B do Código Penal e Lei nº 12.737 de 2012.

Palavras-Chave: Direito Penal. Divulgação de Imagens sem autorização Internet. Nudes.

ABSTRACT

This monograph aims to examine the typification in the criminal law of virtual crime for the dissemination of intimate images without authorization. The specific objectives are aimed at portraying the evolution of the virtual crimes practice associated with the increase in Internet use in recent years, to show the incorporation by the Criminal Law of devices that sanction virtual crimes, to point out in Criminal Law the typification of crime of the dissemination of intimate images without authorization. To achieve this aim, the author developed the study using the deductive approach method, where the main source of content for this research are the laws that changed the Criminal Code and the typification of these rights of Internet users, currently known as illicit practices. Describing a research within the Criminal Code and the laws that regulated these conduct, as well as a conceptual bibliographical survey of this subject. The Brazilian law has presented a considerable delay for the affirmation of virtual crimes, allowing with that the proliferation of the action of criminals, who found on the internet a fertile field of action, especially marked by the unpreparedness of people in the use of the worldwide computer network and in the absence of State protection regarding the regulation of this network. The Internet in Brazil originated in the 1980s, in its end, having as expansion in the decades of 1990 and 2000, reaching a large part of Brazilian households and becoming a fever in Brazilian society, associated with technological change. The subject-matter of the research is the typification of the virtual crime of divulging of intimate images without authorization, popularly known as nudes. This monograph describes the positions of Brazilian jurisprudence around this provision of "nudes" photos without the proper authorization, based on Articles 154-A and 154-B of the Criminal Code and Law 12.737 of 2012.

Keywords: Criminal Law. Disclosure of Images without Authorization. Nudes.

Traduzido por Marise de Melo Lemes, graduada em Letras com Licenciatura em Português e Inglês, pela Faculdade de Filosofia do Vale de São Patrício (FAFISP/UniEvangélica).

LISTA DE ILUSTRAÇÕES

Figura 01 - Fotos Íntimas compartilhadas na Internet.....	53
Figura 02 – Vazamento de “nudes” no Brasil.....	54

LISTA DE SÍMBOLOS

% PORCENTAGEM

LISTA DE ABREVIATURAS E SIGLAS

ARPANET	ADVANCED RESEARCH PROJECTS AGENCY NETWORK
ART	ARTIGO
CIA	CENTRAL INTELLIGENCE AGENCY
ECA	ESTATUTO DA CRIANÇA E DO ADOLESCENTE
EMBRATEL	EMPRESA BRASILEIRA DE TELECOMUNICAÇÕES E PARTICIPAÇÕES S.A.
EUA	ESTADOS UNIDOS DA AMÉRICA
FAPESP	FUNDAÇÕES DAS PESQUISAS DO ESTADO DE SÃO PAULO
GO	GOIÁS
IBM	INTERNATIONAL BUSINESS MACHINES
IP	INTERNET PROTOCOL
KBPS	QUILOBIT POR SEGUNDO
KM	KILÔMETROS
MG	MINAS GERAIS
MPF	MINISTÉRIO PÚBLICO FEDERAL
MSN	MESSANGER
NSA	NATIONAL SECURITY AGENCY
PL	PROJETO DE LEI
PROF	PROFESSOR
PSDB	PARTIDO DA SOCIAL DEMOCRACIA BRASILEIRA
PT	PARTIDO DOS TRABALHADORES
RNP	REDE NACIONAL DE PESQUISA
SMS	SHORT MESSAGE SERVICE
STJ	SUPERIOR TRIBUNAL DE JUSTIÇA
TCP	TRANSMISSION CONTROL PROTOCOL
TELERJ	TELECOMUNICAÇÕES DO ESTADO DO RIO DE JANEIRO
URSS	UNIÃO DAS REPÚBLICAS SOCIALISTAS SOVIETICAS
5°	QUINTO

SUMÁRIO

1.	INTRODUÇÃO.....	13
2.	A DIFUSÃO DO USO DA INTERNET NO BRASIL E O SURGIMENTO DOS CRIMES VIRTUAIS.....	17
2.1.	A DIFUSÃO DA INTERNET NO BRASIL.....	18
2.2.	O AUMENTO DOS CASOS DE CRIMES VIRTUAIS COM A EXPANSÃO DA INTERNET NOS LARES BRASILEIROS.....	24
3.	OS CRIMES VIRTUAIS E A SUA POSITIVAÇÃO NO DIREITO BRASILEIRO.....	31
3.1.	A MOROSA POSITIVAÇÃO DOS CRIMES VIRTUAIS NO BRASIL.....	31
3.2.	A TIPIFICAÇÃO DOS CRIMES VIRTUAIS NO BRASIL.....	34
3.2.1.	A Lei 12.735 de 2012 e a tipificação do uso de aparelhos eletrônicos, digitais e similares.....	35
3.2.2.	A Lei 12.737 de 2012 e a expansão da proteção aos usuários da rede mundial de computadores no Brasil.....	37
4.	A DIVULGAÇÃO DE IMAGENS ÍNTIMAS (NUDES) SEM AUTORIZAÇÃO E A INFLUÊNCIA DAS LEIS 12.737 DE 2012 E 12.965 DE 2012 NA APURAÇÃO E PUNIÇÃO AOS INFRATORES DESSE TIPO DE CRIME VIRTUAL.....	42
4.1.	BREVES CONSIDERAÇÕES ACERCA DO ARTIGO 154-A E 154-B DO CÓDIGO PENAL BRASILEIRO.....	43
4.1.1.	A positivação do Marco Civil da internet e o auxílio a identificação dos usuários da rede no combate a privacidade dos usuários.....	46
4.2.	A DIVULGAÇÃO DE IMAGENS ÍNTIMAS SEM AUTORIZAÇÃO NA INTERNET.....	53
	CONSIDERAÇÕES FINAIS.....	55
	REFERÊNCIAS.....	56

1. INTRODUÇÃO

O Brasil enfrenta um sério problema quanto à segurança pública e a prevenção da ocorrência de crimes. Acarretando dificuldades também quanto a apuração dos infratores e ao julgamento desses criminosos, causando uma comoção social em torno dessa ineficácia do cumprimento das normas.

Sendo um Código datado do ano de 1940, muitos dispositivos do Código penal brasileiro encontram-se defasados, havendo muitas condutas que podem ser nocivas a sociedade e que não encontram dispositivos que a criminalizem no Código Penal, como o caso, por muito tempo, dos crimes virtuais.

O tema objeto da pesquisa é a tipificação do crime virtual de divulgação de imagens íntimas sem autorização, popularmente conhecido como nudes, esboçando um relato histórico da evolução da ocorrência de condutas criminosas envolvendo crimes virtuais. Acelerada pelo aumento do uso da internet e a dificuldade em se conter a ação desses criminosos e de se descobrir quem está envolvido nessas práticas criminosas.

A tipificação dos crimes virtuais representa uma das grandes conquistas nos últimos anos relacionada à proteção dos usuários na rede mundial de computadores, pois a maior parte das condutas ilícitas na internet é de difícil identificação dos culpados e se proliferam em questão de pouco tempo. Portanto, a problemática é como se apresenta no ordenamento jurídico brasileiro a divulgação de imagens íntimas sem autorização através da invasão de equipamentos eletrônicos?

O direito penal por ter o caráter preventivo e repressivo, visa à prevenção de uma forma geral, para que as pessoas não pratiquem crimes, sabendo que poderão ser punidos pelos atos praticados. Por outro lado, o caráter repressivo vem a ser elucidado posterior ao cometimento do crime, quando o Estado tem que agir para punir quem infringir uma conduta tipificada como crime.

A tipificação dos crimes virtuais ocorreu depois de anos de impunidade para aqueles que utilizam a internet para causar transtornos ou praticar atos atualmente conhecidos como ilícitos, mas que até poucos anos atrás não existia regulamentação que prevenisse a ocorrência desses crimes.

As condutas, atualmente tipificadas como crimes, encontram respaldo com a sanção das leis 12.735 e 12737, ambas do ano de 2012, quando se passou a proteger de forma mais uniforme e abrangente os usuários da internet, criando mais meios que facilitem a descoberta dos criminosos e a punição desses agentes.

O objetivo geral, a ser estudado no texto monográfico, é examinar a prática da divulgação de imagens íntimas sem autorização no ordenamento jurídico brasileiro. Os objetivos específicos direcionam-se no sentido de retratar a evolução da prática dos crimes virtuais associados pelo aumento do uso da internet nos últimos anos; Mostrar a incorporação pelo Direito Penal de dispositivos que sancionam os crimes virtuais; Apontar no Direito Penal a tipificação do crime de divulgação de imagens íntimas sem autorização.

A internet está presente no cotidiano das pessoas, em diversificados dispositivos que têm acesso à rede mundial de computadores, facilitando o contato das pessoas e impedindo um controle maior sobre o conteúdo a ser acessado. Celulares, computadores, *tablets*, são alguns dos instrumentos que possuem capacidade para ter acesso à rede mundial dos computadores e que estão presentes nos lares brasileiros e ambientes de trabalho.

Por essa facilidade de acesso à internet, aliada a dificuldade de proteger os usuários e controlar a má fé de dos agentes criminosos, fez-se crescer a necessidade de se tipificar condutas na internet que se mostravam nocivas às pessoas e acabavam ameaçando quem utilizava da grande rede.

O método de abordagem dedutivo contribui com a pesquisa ao direcioná-la no sentido de analisar os crimes virtuais como um todo, para posteriormente se estudar os mais relevantes crimes virtuais, diferenciando as condutas que passaram a ser tipificadas como crimes virtuais, chegando a uma análise particular dessas condutas.

O direito penal é a fonte principal de conteúdo para essa pesquisa, com as leis que alteraram o Código Penal e a tipificação desse código de condutas que até então não tinham uma tipificação, embora causassem prejuízos e ferissem direitos dos usuários da internet, atualmente conhecidas como práticas ilícitas.

Descrevendo uma pesquisa documental do Código Penal e das leis que normatizaram essas condutas, a pesquisa sobre crimes virtuais é mais marcada por análise de casos concretos, que foram levados a julgamento do que especificamente de doutrinas, pois além de ser um tema atual, não existem doutrinas tão consistentes sobre o tema. A pesquisa documental é a mais apropriada para elucidar a pesquisa, partindo para uma análise de casos e a posição jurisprudencial sobre o tema e definição conceitual de algumas condutas em doutrinas.

Os crimes virtuais demoraram a ser tipificados, sendo que muitas condutas que constantemente ocorrem na internet e que constituem crimes não reconhecidos ainda pelas pessoas que são usuárias da rede, tornando a punição dos infratores mais difícil. Justifica-se nesse sentido a escolha do tema, para esclarecer as mudanças proporcionadas no uso da

internet para a proteção dos usuários e a criminalização dos infratores de crimes virtuais. Embora ainda exista uma dificuldade em se buscar ajuda para solução para esses casos, sendo um dos mais comuns à divulgação de imagens íntima sem autorização, popularmente conhecida como vazamento de *nudes*.

A primeira parte do trabalho monográfico interpelará a expansão da internet no Brasil, para que se possa ter uma noção da evolução dessa ferramenta enquanto importante meio de comunicação no país e a seu adentrar nos lares brasileiros, visto suas diversas utilidades, focando-se no objetivo da ferramenta.

A segunda parte do texto monográfico dá prosseguimento ao estudo, com a análise da positivação dos crimes virtuais no Brasil, através da incorporação pelo ordenamento jurídico pátrio de normas voltadas para o controle e punição dos infratores que fizerem uso das práticas tipificadas como crimes virtuais.

Na terceira parte, destaca-se dentre as práticas abrangidas como crimes virtuais pelo direito penal brasileiro, a divulgação dessas imagens via internet, direcionando o estudo a esse meio de comunicação, justamente por sua incidência na sociedade e a dificuldade em se proteger as pessoas e punir os infratores.

2. A DIFUSÃO DO USO DA INTERNET NO BRASIL E O SURGIMENTO DOS CRIMES VIRTUAIS

A criminalidade atinge cada vez mais índices elevados no cenário brasileiro, causando um alerta na sociedade quanto aos meios de se controlar esse avanço criminal e a tentativa de reduzir os impactos e riscos a sociedade derivada da ação desses criminosos a sociedade.

Essa preocupação perpassa por uma atuação efetiva do Estado, como gestor de um modelo de combate eficaz da criminalidade, o que não vem sendo demonstrado na prática, pois existe uma diversificação, assim como uma consolidação do medo dentro da sociedade.

Entretanto, existe um despreparo estatal no combate à criminalidade em todos os parâmetros que possam ser analisados, sobretudo no combate direto aos criminosos, que em algumas circunstâncias chegam a apresentar melhor preparo para a manutenção da criminalidade do que o próprio Estado para combatê-lo.

Se no âmbito material, a criminalidade vivenciada diretamente pelas pessoas se faz de difícil combate pelo Estado e a própria sociedade, a ascensão da internet e sua difusão pelos lares trouxeram as pessoas uma ameaça constante quanto à atuação de criminosos nesse ambiente, ameaça que enfrenta maiores dificuldades ainda para serem descobertos os agentes criminosos e a sua punição pelos órgãos responsáveis do Estado.

A primeira parte do trabalho monográfico interpelará a expansão da internet no Brasil, para que se possa ter uma evolução dessa ferramenta enquanto importante meio de comunicação no país e a seu adentrar nos lares brasileiros, visto suas diversas utilidades, focando-se no objetivo da ferramenta.

Nessa primeira parte, posterior a transcrição da evolução da internet, e sua incorporação pelas pessoas no Brasil, apresentam-se os relatos da disseminação de crimes, no ambiente virtual e sua rápida proliferação pela rede mundial de computadores, assim como as dificuldades encontradas quanto à prevenção da ação desses criminosos na internet.

Em última análise, na primeira parte do trabalho monográfico, far-se-á um levantamento da demora do ordenamento jurídico brasileiro em positivar leis que auxiliem o Estado no controle e punição daqueles agentes que fizerem uso de práticas nocivas no ambiente virtual.

2.1. A DIFUSÃO DA INTERNET NO BRASIL

A internet, atualmente, constitui um dos meios de comunicação mais utilizados pela população mundial. Bastante difundida em todas as idades e classes sociais, o que tem levado a internet a ser alvo constante de variados crimes, os crimes virtuais. Criada inicialmente para fins militares, a Internet foi primeiramente usada para facilitar a comunicação entre militares norte-americanos durante a Guerra Fria, sendo posteriormente introduzida nos ambientes universitários, para depois ser disponibilizada a sociedade.

A origem desse meio de comunicação se tem por volta da década de 1960, onde a princípio, essa ferramenta representava uma evolução na transmissão de informações, bem mais avançada e rápida que os até então encontrados, como telégrafos, jornais, cartas, entre outros. Essa facilidade de uso e efetividade, concretizada pela velocidade maior de troca de informações possibilitou que a internet se arraigasse na sociedade, tornando-se um instrumento essencial para as relações humanas, especialmente nos dias atuais, com a evolução dessa ferramenta.

Quando criada, essa foi uma importante arma norte-americana durante a fase da Guerra Fria, na disputa com a União Soviética e também um dos principais legados deixados desse povo para a humanidade, observando sua utilidade. Sobre o surgimento da Internet, Dumas (2013, p. 01) cita:

De acordo com o dicionário Houaiss, internet é “rede de computadores dispersos por todo o planeta que trocam dados e mensagens utilizando um protocolo comum”. Ela nasceu no final dos anos 1960, em plena Guerra Fria, graças à iniciativa do Departamento de Defesa americano, que queria dispor de um conjunto de comunicação militar entre seus diferentes centros. Uma rede que fosse capaz de resistir a uma destruição parcial, provocada, por exemplo, por um ataque nuclear.

A época de criação da internet, como exposto para fins militares, foi marcada como uma época de grande desenvolvimento tecnológico. Inicialmente, esse meio de comunicação não tinha a abrangência atual na sociedade, por ser este caráter mais restrito da sua finalidade, demorando décadas a adentrar a sociedade e a expandir para outros países. Ainda Sobre a criação da internet, Rodrigues (2008, p.03) relata:

Relembrando o momento histórico de origem da internet, tem-se que essa ferramenta originou-se da *Arpanet*, que foi a primeira rede nacional de computadores, criada ainda no ano de 1969, pelo então Departamento de Defesa dos EUA, com a finalidade de garantir a segurança em caso de acidente nas comunicações.

Esta rede de computadores, que na época era restrita, destinava-se a interligar os computadores dos centros de pesquisa, universidades e instituições militares americanas, permitindo o compartilhamento de recursos entre os pesquisadores que trabalhavam com projetos estratégico-militares com esses centros científicos.

A criação da internet pelos pesquisadores norte-americanos tinha como objetivo inicial proteger os dados bélicos daquela nação, preparando-se para uma eventual guerra física, que poderia levar ao fim dessas informações. Portanto, a princípio, a internet era voltada para armazenamento dos dados, como forma de defesa desses informes norte-americanos.

Em segunda escala, a internet tinha como finalidade transmitir essas informações de um campo de pesquisa norte-americano para outro centro, sendo inicialmente desenvolvida para um alcance numa distância de 650 km, bastante diferente dos dias atuais, mas que na época representava uma novidade surpreendendo.

Os anos posteriores à década de 1960 representaram a consolidação da internet como meio de comunicação, surgindo instrumentos que facilitassem essa troca de informações dentro da rede e fazendo com que a precursora *Apartnet* ficasse ultrapassada.

Criou-se então uma dupla função para a internet, onde a *ARPANET* (A Advanced Research Projects Agency Network) para fins militares, ganhando contornos civis nas décadas de 1970 e 1980, com o crescimento das funcionalidades dessa rede mundial de computadores, isso possibilitou que se dividisse a rede em duas, de acordo com a suas funcionalidades: militares e civis.

A década de setenta consolidou a internet, ao mesmo tempo deu margem para o surgimento dos primeiros problemas relacionados ao uso dessa ferramenta de comunicação, como vírus e *spams*, até então não denominados assim. Um dos grandes avanços dessa década merece atenção é a criação do *e-mail*, um instrumento de envio de mensagens virtual. Kleina (2011, p. 10) cita:

O engenheiro Ray Tomlinson começou a desenvolver o hoje indispensável e-mail em 1971. A ARPANET já possuía alguns métodos de transmissão de mensagens entre o mesmo computador, mas faltava um sistema simples e que integrasse toda a ARPANET.

Observa-se então que com o passar dos anos e as facilidades de comunicação proporcionadas por essa descoberta, foi sendo introduzida no convívio da sociedade em geral. Destacando-se o uso nas universidades para desenvolvimento de pesquisas. Isso possibilitou que a internet se tornasse uma febre entre as diferentes faixas etárias a nível mundial,

acelerando as formas de comunicação e diminuindo as distâncias na comunicação. Rodrigues (2008, p.04) relata que:

Em 1972 o governo americano decidiu mostrar o projeto pioneiro à sociedade, e a ideia expandiu-se entre as universidades americanas, interessadas em desenvolver trabalhos cooperativos. Para interligar os diferentes computadores dos centros de pesquisa, em 1980 a Internet adotou o protocolo aberto TCP/IP para conectar sistemas heterogêneos, ampliando a dimensão da rede, que passou a falar com equipamentos de diferentes portes, como micros, workstations, mainframes e supercomputadores.

Ligado ao desenvolvimento dessas novas tecnologias relacionadas à internet fez com que na década de 1970 fosse realizada mediante diversos estudos a primeira transmissão de dados entre continentes, sendo um grande marco para época. Aliado a isso, três grandes empresas atuais da tecnologia surgem em destaque e começam a emergir com gigantes desse ramo: a IBM, a Apple e a Microsoft.

Na década de 1980, a descoberta de novas funcionalidades foi sendo abrangidas por essas empresas, exemplo foi o surgimento das salas de bate papo, onde as pessoas poderiam se relacionar com as outras de maneira virtual. Isso contribuiu para a difusão da internet pelo mundo e consolidação do seu caráter informativo, mesmo que fugindo do caráter inicial da ferramenta.

Porém, foi a década de 1990, a responsável pela difusão da internet a níveis mundiais. Nesse período, vários equipamentos eletrônicos foram criados, o que possibilitou o acesso à rede mundial de computadores a partir de suas funcionalidades desses aparelhos, aproximando mais essa ferramenta das pessoas.

Apesar de o final da década de 1980, representar a chegada desse meio de comunicação no território brasileiro, ainda de maneira bem restrita a esse ambiente universitário, foi na década de 1990 que ela se instalou em definitivo. O ano de 1987 é o grande marco de início da transmissão de dados via internet no Brasil, onde as informações foram conectadas entre FAPESP (Fundações das Pesquisas do Estado de São Paulo) e as instituições de pesquisas presentes nos EUA.

Nesse momento, eram feitos os primeiros usos da internet no Brasil. Com o iminente sucesso dessa conexão, a internet começou a ser requisitada por outras empresas e universidades, utilizando-se desse importante meio de comunicação. Foi nessa década de 1990 que a internet se consolidou no Brasil, seguindo os moldes da difusão da internet no restante do mundo, principalmente nos EUA. Porém, diferente da norte americana, essa rede

no país não teve inicialmente funções militares, voltando-se para o uso em universidade e centros de pesquisa, coligadas às redes norte-americanas.

Três anos após a implantação da internet em solo brasileiro, essa rede começou a ser difundida pelo restante do país, embora ainda atendesse aos critérios educacionais em universidades e centros de pesquisa. A criação da Rede Nacional de Pesquisa foi a responsável pela implantação dessas novidades quanto à internet. Carvalho (2006, p. 109):

O projeto de uma RNP, como já se sabia, necessitava de uma infraestrutura pesada e cara, que dependia fortemente do governo, que finalmente reconheceu a necessidade de investir em comunicações de dados, de modo a envolver (e comprometer) os vários atores de pesquisa e desenvolvimento em atividades cooperativas que, assim, viessem a contribuir de forma mais efetiva para o desenvolvimento nacional nessa área.

O Estado do Rio de Janeiro desenvolveu, no ano de 1992, uma conexão através da TELERJ (Telecomunicações do Estado do Rio de Janeiro) em parceria com a EMBRATEL (Empresa Brasileira de Telecomunicações), onde as informações eram ligadas com a universidade de San Diego, na Califórnia.

Atendendo a um suporte de velocidade de transmissão de dados a 64 kbps, essas informações eram utilizadas para pesquisas nos centros universitários do Estado. Desenvolveu-se no Brasil nessa época um sistema de utilização mista da internet, fugindo da restrição apenas para uso acadêmico, difundindo-se dentro da sociedade e chegando aos lares brasileiros, ainda de forma bem simples e lenta.

Com o passar dos anos, foi surgindo à necessidade de expandir a área de atuação da internet no Brasil, possibilitando seu uso sem restrição aos ambientes universitários e de pesquisa. Em meados do ano de 1995 representam a expansão do uso da internet no Brasil, onde essa rede pode ser compartilhada além dos fins educacionais, até então observados em universidades. Através da ação do Ministério da Comunicação e Ministério da Ciência e Tecnologia.

Até então, eram desenvolvidas conexões com essas velocidades, ofertadas em algumas regiões do país, nas velocidades 9.6 e 64 kbps. Todas elas eram ligadas a centros de pesquisa norte-americanos. Nessa época, houve a disseminação da venda de microcomputadores no Brasil, trazendo uma nova ferramenta para que as pessoas tivessem a possibilidade de acessar a internet. No Brasil, a grande responsável pela gestão da comunicação através da internet era a EMBRATEL.

A Embratel tentou ser o grande provedor da Internet comercial no Brasil, mas sua iniciativa acabou sendo bloqueada pela forte estratégia governamental de desestatização da economia, que começava pelo setor de telecomunicações. Mas já era tarde demais e a caixa de Pandora já estava aberta. “O problema (do monopólio do acesso à Internet) deu tanta dor de cabeça aos dirigentes da Embratel que os 140 assuntos passou a (internamente) ser chamado de Infernet”. (SIQUEIRA, 2005, p.90).

A internet expandia suas funções para outras áreas, agora na área comercial, o que aumentou a demanda para a internet no Brasil. Nesse momento, a Empresa Brasileira de Telecomunicações e Participações S.A. (EMBRATEL) possuía e tinha a liberação de fornecer a internet para empresas, não para pessoas físicas.

Com o sucesso da internet na finalidade inicial implantada no Brasil, foram surgindo requerimentos de implantação desse novo sistema aos estabelecimentos comerciais no Brasil, que gerou um sobrecarga dos serviços, pois não existia, ainda naquela época, estrutura suficiente para atender a essa demanda crescente. Carvalho (2006, p. 143) destaca esse momento:

A Internet comercial no Brasil chegou ao ano de 1996 com uma infraestrutura insuficiente para atender à demanda dos novos provedores de acesso comercial e, principalmente, dos seus usuários. Com a saída da Embratel do mercado de provimento de acesso para pessoas físicas e a RNP ainda se estruturando para permitir o acesso dos novos provedores comerciais ao seu backbone, muitos usuários no Brasil ficaram sem ter como se conectar a Internet.

O final da década de 1990 tem, na ação do Governo Federal, uma importância na divulgação da internet, assim, criou o Programa Sociedade da Informação. O objetivo desse programa era difundir a internet a todas as camadas sociais, possibilitando a expansão dessa rede por um maior número de pessoas e permitindo que o acesso à internet se tornasse comum nos lares brasileiros.

Depois de expandida na década de 1990, nos anos 2000 representaram a consolidação da internet dentro da sociedade brasileira nas suas mais variadas utilidades, não somente se restringindo ao uso nos centros de pesquisa e universitários, como no início da década de 1990.

Assim, como difundiu esse meio de comunicação as escolas, auxiliando nas fontes de pesquisa. O surgimento de várias redes sociais colocou o Brasil entre os países com mais usuários em todo mundo. Redes sociais como MSN, Orkut, Fotolog foram essenciais para a difusão da internet entre as diversas camadas sociais brasileiras.

Já no ano de 2004, mesmo após pouco tempo de uso da internet no país, o Brasil já figura entre os principais países usuários da internet no mundo, alavancada pelo uso dessas redes sociais, que são plataformas para a troca de informações entre as pessoas, a curta e longa distância, nos mais remotos cantos do mundo. Miecoanski e Tavares (2012, p. 10) citam:

Em 2000, a internet era acessada por 9,8 milhões de brasileiros – menos de 6% da população. Pouco mais de uma década, o agora alfabetizando digital assiste às aulas com a intenção de se tornar parte de uma rede de quase 70 milhões de internautas. A tribo agora abrange 35% do país e a tendência é de conversão quase integral ao longo dos próximos dez anos. Foi a década da informática no Brasil. O computador ruma para se tornar um item presente na maioria dos lares do país, tendo como obstáculo apenas a possibilidade de se tornar obsoleto antes de romper a marca, substituído por tablets e celulares inteligentes. O Censo 2010 apontou a presença de algum tipo de computador (desktop, laptop, notebook ou netbook) em 38% dos domicílios. Desses, três em cada quatro estão conectados à internet.

Um dos fatores que possibilitaram a expansão da internet e a facilitação do uso dessa rede foi à criação no Brasil da banda larga, que garantia uma velocidade maior de navegação, garantindo estabilidade maior aos usuários no uso da rede. Assim, a internet do tipo discada, difundida pela EMBRATEL até então, dava lugar ao tipo banda larga.

Atrelado a essa difusão de redes sociais, a expansão do comércio virtual também garantiu um lugar de destaque a internet nos estabelecimentos comerciais. Grandes grupos de empresas passaram a realizar suas atividades por meio da grande rede mundial de computadores, justamente pela facilidade que essas plataformas geravam, além da busca de um novo mercado consumidor, agora no âmbito virtual.

O comércio virtual tem agradado bastante aos empresários à medida que representa uma forma de comercialização geralmente de baixo custo, onde os investimentos com a implantação de um site são menores na maioria das vezes que a implantação de uma estrutura física para funcionar como sede das empresas.

Além disso, a expansão de acesso das informações em um site tem maior abrangência que em espaços físicos, possibilitando que mais pessoas obtenham informações sobre essas empresas e seus produtos. A possibilidade de acesso a qualquer hora do dia também expande a possibilidade de expansão e venda dessas marcas que optam pelo comércio virtual.

Atrelado a essa diversidade de horário, facilidade na implantação, tem a questão das pessoas não precisarem se deslocar para realizarem suas compras, assim como a possibilidade

de interligação de vários segmentos da empresa, como financeiro, vendas, entregas, estoque, administrativo.

Atualmente, a internet está presente nas diversas atividades desenvolvidas pelos brasileiros. As universidades cada vez mais aderem às facilidades trazidas pela internet, seja no ramo de pesquisas, seja ministrando cursos em plataformas na internet. Existem vários cursos de níveis superiores atualmente que podem ser ministrados na internet, garantindo as pessoas uma possibilidade diferente de especialização.

O Poder Judiciário também tem aderido ao uso da internet, como importante auxílio na aceleração dos processos, possibilitando as pessoas uma resposta mais rápida desse Poder quando buscar a solução de conflitos. Em várias repartições do Poder Judiciário já existem sistemas que dão a chance das ações do Poder Judiciário serem realizadas através do ambiente virtual, como o PJD e PJE.

A internet por se tratar de uma ferramenta de fácil acesso e grande abrangência geográfica, acaba por influenciar na divulgação de informações por todo mundo, conhecimento de culturas e proliferação de informações até então restritas aos locais que acontecem. Um fato pode em questão de segundos ser exibido aos mais remotos lugares do mundo por meio da internet em questão de minutos.

Em 2010, foi proposto um Projeto Nacional de Banda Larga, que seria responsável por difundir essa forma de acesso à internet pelo Brasil. Assim, até o ano de 2014, o Brasil estaria antenado à internet por meio da banda larga. Seria função, segundo o referido programa do Governo Federal, expandir essa rede por outras regiões até então escassas dessa inovação tecnológica.

Nos dias atuais, a utilização da internet no Brasil encontra-se difundida principalmente nos grandes centros urbanos, em estruturas melhores, nas regiões sul e sudeste do país, onde estão concentradas as principais tecnologias do país em todos os parâmetros.

2.2. O AUMENTO DOS CASOS DE CRIMES VIRTUAIS COM A EXPANSÃO DA INTERNET NOS LARES BRASILEIROS

Um dos fatores mais relevantes para o crescimento dessas práticas criminosas no ambiente virtual é a dificuldade em se deter a ação desses criminosos, assim como a identificação desses agentes, visto que não é, em muitos procedimentos, preciso se identificar ao usar essa ferramenta de comunicação.

O crescimento do comércio virtual tem urgido como um dos pontos que merecem um controle maior, pois tem trazido uma nova possibilidade aos criminosos de aumento da forma de se praticar os crimes. A facilidade com que as compras são realizadas, a comodidade que a ausência de necessidade de se mover até os pontos comerciais fez essa prática comercial ganhar destaque entre as atividades realizadas na internet. Por envolver quantias volúpias de dinheiro, as transações envolvendo dinheiro estão cada vez mais passíveis da ação de criminosos.

As redes sociais são utilizadas por um grande número de pessoas, das mais variadas idades, nos mais distantes locais do mundo. Pessoas que nem se conhecem, aproximam-se por meio desses sites de relacionamento. Muitas vezes utilizando identidades falsas, que dificultam a ação da justiça na punição a possíveis crimes que possam ser cometidos pelos criminosos.

Como exposto, o desconhecimento nessas redes sociais acaba se tornando ambiente fácil de ocorrência de crimes no meio virtual, tornando-se uma das maiores causas da proliferação de crimes virtuais, onde os usuários caem em truques simples, cometidos por criminosos, além de realização de crimes em outro sentido, como crimes contra a honra.

A falta de sabedoria de grande parte dos usuários quanto ao uso da rede é um dos elementos a serem observados quando se toca em crimes virtuais, além do despreparo de regulação dos provedores e de controle do uso da rede por pessoas mal intencionadas.

Muito se divulga a ação de *hackers* quando se fala em crimes no ambiente virtual, mas diferente do que a maioria da população pensa, o termo *hacker* não se remete aquelas pessoas que fazem uso do seu conhecimento avançado para cometer crimes pela internet, podendo ser qualquer pessoa que descubra novas funções, novos meios de se utilizar instrumentos de informática.

Hackers são indivíduos que criam e modificam softwares e hardwares de computadores, desenvolvendo novas funcionalidades ou adaptando as antigas. Já, o termo *cracker* é usado para indicar quem pratica a quebra de um sistema de segurança e usa seus conhecimentos de forma ilegal, sendo assim vistos como criminosos. Portanto, o que difere os “grupos” é como cada um usa os seus conhecimentos, um de forma maliciosa, outra com a finalidade de simples manipulação dos dados.

Ainda seguindo essa linha de pensamento, tem-se o termo *cracker*, que se referem aqueles que utilizam sua capacidade avançada em informática para realizar crimes, ou seja, tirar proveito das demais pessoas que utilizam a internet. Sobre isso, Stringari (2013, p. 02) relata que:

Cracker, de acordo com o significado originalmente cunhado ao termo, designa sim, elementos mal intencionados, que estudam e decodificam programas e linguagens a fim de causar danos a computadores alheios. A intenção é invadir e sabotar sistemas, quase sempre objetivando a captação de dados passíveis de render cifras. Ou seja, roubo eletrônico, estelionato ou o que quer que seja.

Nota-se então uma diferença, já que muitas pessoas atribuem aos hackers esse crime, fato que deveria ser atribuído aos *crackers*, que são os que agem com essa finalidade criminoso. Assim, tem-se a primeira conceituação importante na definição dos crimes virtuais.

Como exemplo de crime praticado na internet, a pedofilia é um dos crimes previstos no Código Penal que migraram para o ambiente virtual, que tem mais se valido do mundo virtual para proliferação desses criminosos, o que dificulta tanto a prisão desses, como tem na velocidade da troca dessas informações uma ameaça às crianças e adolescentes vítimas desses infratores.

Um dos agravantes dessas ações de pedofilia é o alto índice de uso da internet entre os jovens, que os tornam em presas fáceis desses criminosos. As redes sociais representam grandes ameaças a esses jovens que são induzidos por pessoas maliciosas, muitas vezes utilizando de perfis falsos para cometerem esses crimes. Carreiro (2012, p. 12):

E paralelamente aos avanços, científico tecnológico, que conduzem (e conduzem) a humanidade a caminhos dantes considerados inatingíveis, que a violência encontra campos para demonstrar a sua face mutante, constituindo um cibernético paradoxo. A facilidade de acesso aliada ao caráter sigilos que configura o tipo de comunicação estabelecido entre os internautas (termo que designa as pessoas que se comunicam no ambiente virtual) favorece a ação criminosa de indivíduos inescrupulosos.

Muitos criminosos usam desse sigilo das redes sociais para aliciar principalmente crianças a práticas que levam a exploração sexual. Esse sigilo às vezes dá ao criminoso a oportunidade de não revelar sua verdadeira face na internet, criando perfis falsos. Fatos que são piores quando esses infratores usam dessa confiança adquirida das crianças para marcarem encontros com esses jovens, consumando fisicamente esses crimes.

A internet, ao mesmo tempo em que se tornou uma ferramenta muito útil em diversas áreas da sociedade, tem na exposição dos usuários uma ameaça a eles mesmos. As agências bancárias, por exemplo, teve no uso de aplicativos ligados a internet uma crescente atividade dentro das agências, mas que deu a esses criminosos uma chance de expandir sua atuação na prática criminosa, tudo isso feito de maneira virtual, sem contato com a vítima desses golpes, pois existe uma dificuldade em conter a ação dos criminosos.

Nesse sentido, o acesso às contas eletrônicas das agências bancárias tem sido constantemente vítimas de interferência por parte de criminosos, que cometem fraudes como desvio de dinheiro mediante furto desses dados. Nos dias atuais, as agências bancárias disponibilizam quase todas as suas funções no ambiente virtual, para que o usuário possa ter acesso do local onde se encontre, de maneira mais rápida, não precisando se deslocar a agências físicas desses bancos, isso faz com que sejam crescentes esses usos de aplicativos de agências bancárias, assim como o foco dos criminosos em atuar nessa área.

Novamente, nesses golpes aplicados, a rapidez da internet dificulta tanto a prisão dos criminosos, quanto em casos de desvio de dinheiro, a dificuldade em resgatar esses valores. Uma das fraudes mais comuns contra usuários de bancos é o roubo de dados pessoais ao clicarem em *malwares* ou páginas falsas de bancos, que sendo controlados por infratores penais, deixam os usuários dos bancos vulneráveis quanto ao uso virtual de suas agências.

A criação por parte dos criminosos de páginas falsas também atinge o crescimento do comércio virtual, que passam a iludir as pessoas na esperança de ofertas melhores e assim cometem fraudes com documentos e dinheiro dessas pessoas, com oportunidades falsas de compra, tendo acesso aos dados das pessoas, dando início a outras práticas criminosas.

Quanto a essa prática, de roubo de informações que é bastante comum, vê-se que é acentuada pela inocência das pessoas, conhecidas como *pishings*, fazendo-se uso de endereços de *e-mail*, atraindo as pessoas para ofertas oportunas que quando as pessoas clicam no endereço de *e-mails* falsos tem sua privacidade invadida e furtado seus dados. Fachini (2014, p. 12):

O phishing é algo muito frequente. É uma maneira de fazer a pessoa informar os dados pessoais achando que era para uma finalidade, quando na verdade estão sendo roubados por criminosos. Isso é feito mandando e-mails falando que a pessoa ganhou um prêmio ou que recebeu uma encomenda que precisa ser rastreada e para isso é necessário postar os dados. Há também os que se passam por instituições bancárias e mandam e-mail cobrando dívidas. A pessoa clica, digita os dados e a senha e o criminoso rouba. O ‘Smishing’ ou phishing por SMS também vem crescendo.

Observa-se que o sucesso dessa prática criminosa realizada por *e-mail* fez com que os criminosos virtuais desenvolvessem essas práticas também via *sms*, o que aumenta o potencial de possíveis vítimas dessas práticas criminosas, formando o chamado *smishing*, sendo uma variação da falsificação dos dados.

A pirataria, tão comum na sociedade, foi aperfeiçoada por meio da internet e se tornou outra prática bastante utilizada no Brasil, especialmente de produtos eletrônicos.

Acontece atualmente uma variação com relação à forma de pirataria de produtos, sendo trocada a até então difundida através de cópias físicas, transformando em ações no mundo virtual. Gusmão (2015, p. 10) diz:

Os norte-americanos são donos de mais de 108 milhões de IPs “criminosos”, que realizaram pouco mais de 2,1 bilhões de downloads piratas em 2014. No entanto, em termos de demanda não monetizada – conceito que é basicamente a soma dos valores de músicas, séries, filmes e programas baixados irregularmente –, o país fica apenas em terceiro lugar. À frente dele, estão a Índia e o Brasil, em segundo e primeiro lugares, respectivamente. Por aqui, o total de arquivos baixados equivale a cerca de 99,6 bilhões de dólares, valor mais de 30 bilhões acima dos registrados pelos indianos e pelos norte-americanos. O total mundial, aliás, foi de 836,8 bilhões de dólares, com 77,9% dele vindo de programas “ilegais”.

Quando se fala em pirataria virtual, atividades que mais ganham destaque são os *downloads* de músicas, vídeos, jogos, programas de computadores. Produtos que perdem a procura no mercado tradicional, quando observada que podem ser baixados de graça na internet. Assim, são violados os direitos das empresas e pessoas responsáveis por divulgar suas marcas e trabalhos, de maneira legal. Acompanhadas dessas cópias falsas de programas, aplicativos, geralmente os criminosos disseminam vírus e outros *softwares* que causam um mau uso dos aparelhos eletrônicos.

Os brasileiros estão entre os usuários que mais se utilizam da pirataria na internet. Essas atividades causam um rombo enorme para as empresas que poderiam lucrar a venda convencional de seus produtos de maneira legal. A pirataria na rede também gera custo para os responsáveis por esses atos que comercializam os produtos de preços menores, sem passar por fiscalizações e impostos que os produtos originais passam.

O compartilhamento de dados através das redes sociais é uma febre principalmente entre os jovens, mas representa outra alternativa utilizada pelos criminosos para atuação, quando eles invadem essas redes sociais para roubar informações, imagens ou vídeos compartilhados. Além dessa forma, a difusão de imagens, vídeos em sites pornográficos redes sociais com intuito de denegrir a imagem de alguém têm ganhado campo entre os criminosos virtuais, especialmente entre pessoas famosas.

Dentre as práticas criminosas no ambiente virtual, uma que chama atenção pela sua abrangência é a perpetuação de crimes contra a honra. Onde vem sendo comum à proliferação de campanhas de cunho racista na internet, incitando a realização de práticas preconceituosas.

Dentre as formas de preconceito, o racial constitui principalmente dentro das redes sociais uma ameaça à sociedade. Assim, alguns grupos sociais têm sua cultura degradada em grande escala na rede, espalhando informações errôneas e perigosas que podem atingir

consequências drásticas em questão de segundos, principalmente quando essas informações são postadas em grupos com diversos adeptos, que espalham essas informações para milhares de pessoas. Maatsura (2015, p. 20) cita:

Se a internet é um espelho da sociedade, está difícil encarar nossa própria imagem de frente. O número de denúncias de racismo e preconceito de origem – sobretudo contra nordestinos e nortistas – disparou no ano passado, segundo relatório da ONG SaferNet divulgado na terça-feira [10/2], Dia da Internet Segura. Mais de 86,5 mil casos de ódio a negros e outras etnias foram relatados em 17.291 sites, aumento de 34,15% em relação a 2013. Mas foi o cômputo de menções ofensivas a pessoas do Nordeste que viveu uma explosão: 365,46% de crescimento, com 9.921 casos em 6.275 endereços. As páginas denunciadas por todos os tipos de crime somaram 58,717, ou 8,29% mais do que no ano anterior. Delas, algo mais que 7 mil foram retirados do ar.

O que se observa nessa proliferação do preconceito por meio virtual é que existe somente uma mudança de área de atuação, onde o ódio é difundido por meio da internet, mas com os mesmos alvos determinados, aumentasse também o potencial de difusão desse preconceito com a capacidade de expansão e velocidade da internet.

Alguns *softwares* utilizados pelos criminosos para cometer crimes virtuais são bastante conhecidos de parte da população, como os spams, e-mails difundidos geralmente por empresas divulgando suas marcas, que vem sendo utilizados por criminosos para roubar informações dos usuários.

Os vírus são dentre os *softwares* prejudiciais os mais conhecidos, que são transferidos entre os computadores e outros dispositivos que usam a internet. Dentre os vírus, os *Trojan Horse* são os mais famosos, capazes de deixar os aparelhos vulneráveis com a destruição de meios de proteção desses aparelhos e de dados contidos nesses aparelhos eletrônicos.

Ainda quanto à atuação dos criminosos nos aparelhos eletrônicos, os *spywares* ganham destaque na espionagem dos dados, principalmente entre usuários que fazem download via internet, baixando programas espões que retiram seus dados dos aparelhos. Os *malwares* são instalados nos equipamentos eletrônicos com único objetivo de causar danos a esses equipamentos, danificando seu uso e causando com isso prejuízo aos usuários desses equipamentos.

Um dos crimes que foram introduzidos ao ambiente virtual foi o sequestro virtual, porém agora voltado para os sequestros de dados virtuais. Essa ação é baseada no bloqueio de dados de um sistema virtual, onde os criminosos acessam a base desses equipamentos e criam

meios de bloquear o acesso, só liberando após o pagamento desse sequestro. Nascimento (2015, p. 10) cita:

Sejam dados internos como de seus colaboradores, ou mesmo confidenciais como os dados de seus clientes, é fundamental que eles estejam disponíveis em tempo hábil para garantir a continuidade dos negócios e, além disso, que sejam protegidos de ataques ou interceptações, para que a corporação não se torne vítima de uma modalidade de crime conhecida como sequestro virtual. Semelhante ao que acontece quando uma pessoa é sequestrada, só que por meio da internet, os criminosos “sequestram” os dados empresariais ou pessoais e os bloqueiam, gerando uma interrupção de acesso e manipulação destes dados, e para que sejam desbloqueados, estes marginais cobram grandes quantias em dinheiro das vítimas. Muitos, para não terem um prejuízo ainda maior, acabam pagando.

A dimensão que os crimes virtuais tomaram na atualidade é de difícil mensuração, assim como é muito difícil propor alternativas eficazes para a diminuição dessas práticas criminosas e a descoberta desses infratores, a positivação dos crimes de natureza virtual é o primeiro passo, porém é necessário mais ações no sentido de não permitir a atuação desses criminosos.

Em suma, na primeira parte do texto monográfico expôs-se como um atualizado meio de comunicação, a internet se destaca pela velocidade com que as informações são difundidas aos quatro cantos do mundo. A facilidade de uso e a presença em diversos instrumentos eletrônicos torna essa rede mundial mais próxima das pessoas. Além de se destacar nesse sentido dentro da sociedade, isso tem a tornado numa grande ferramenta de criminosos para realização de práticas ilícitas.

Na segunda parte do texto monográfico, faz-se um levantamento acerca da recente positivação dos crimes virtuais no direito brasileiro, garantindo a sociedade meios legais de proteger os usuários quanto à ação desses criminosos virtuais. Sendo abordadas as Lei 12.735 e 12.737, ambas do ano de 2012.

3. OS CRIMES VIRTUAIS E A SUA POSITIVAÇÃO NO DIREITO BRASILEIRO

A segunda parte do texto monográfico dá prosseguimento ao estudo com a análise da positivação dos crimes virtuais no Brasil, através da incorporação pelo ordenamento jurídico pátrio de normas voltadas para o controle e punição dos infratores que fizerem uso das práticas tipificadas como crimes virtuais.

A difusão da internet no Brasil trouxe grandes possibilidades às pessoas, consolidando-se como um dos meios de comunicação mais importantes na atualidade. Por outro lado, o crescimento do uso da internet foi acompanhado pelo surgimento de uma nova categoria de criminosos, os virtuais, que se fazem valer da demorada positivação dos crimes virtuais e a dificuldade de conter e descobrir os criminosos um risco para os usuários.

3.1. A MOROSA POSITIVAÇÃO DOS CRIMES VIRTUAIS NO BRASIL

Dentro do direito brasileiro, o Código Penal é o principal amparo legal para tipificação de quais ações são considerados crimes no Brasil e quais as possíveis sanções para essas ações. Embora existam leis que tipificam que ações são consideradas crimes e quais a punição a ser aplicada para cada ação ilícita esse conjunto de leis enfrenta problemas relacionados à desatualização de suas normas em relação à época em que o Código Penal foi criado, na década de 1940.

Associado a isso, o mundo enfrenta uma constante evolução tecnológica, marcada pelo surgimento de novos produtos, novas técnicas que encontram respaldo dentro da sociedade. A internet foi uma das grandes invenções do homem até hoje, apresentando evoluções constantes dentro de suas funcionalidades que levaram a sociedade a aderir a essas ferramentas. Viana (2017) aborda esse assunto:

Vem aumentando muito o desenvolvimento tecnológico pelo mundo e principalmente pelo Brasil, a popularização da internet, computadores celulares, vem também abrindo caminhos para a prática de novos crimes, não especificados totalmente em nosso ordenamento jurídico, que são os chamados “Crimes Virtuais” ou “Crimes Cibernéticos”. O computador, o celular, entre outros aparelhos eletrônicos foram criados especificadamente para facilitar o dia a dia de todos, assim ajudando a realizar tarefas que demorariam a ser concluído, acabarem sendo realizadas quase que instantaneamente, um exemplo disso seria uma compra feita pela internet, no aconchego de seu lar, sem ter que sair de sua casa e dirigir-se até a uma loja para realizar a compra de algo, tendo a opção ainda de buscar preço em vários lugares e escolher onde gostaria de realizar a compra.

Apesar de ser bem utilizadas e reconhecidas à valia da internet para a sociedade atualmente, foram surgindo alguns problemas derivados da ação de criminosos que observaram a ausência de tipificação legal para umas ações no ambiente virtual.

Criou-se na concepção dos criminosos uma visão da internet como uma área sem atuação da justiça, onde a ausência de normas que regulassem a ação das pessoas e o controle dos usuários maléficos a sociedade. Criminosos que ao encontrarem um campo fértil de atuação na internet se valem da ausência de informação dos usuários ou de ferramentas novas para se dar bem em relação aos outros usuários que visam à utilização da internet para fins legais. Viana (2017) informa:

Porém conforme se amplia o desenvolvimento tecnológico e a criação dessas coisas, o nosso ordenamento jurídico não consegue acompanhar criando leis que impeçam a prática de delitos por pessoas que se aproveitam desses meios novos e brechas deixadas por falta de leis para se sobressaírem sobre outras pessoas. Esses crimes que vem sendo cometidos por esse meio podem também ser conceituados como sendo condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicação, modificações de dados.

De fato, a internet é uma região bastante difícil de separar aqueles usuários que agem de boa fé e aqueles que desenvolvem condutas de má-fé, causando prejuízos às pessoas que usam a rede. Muitos usuários usam de dados falsos durante a navegação, o que deixa as autoridades responsáveis por avaliar os casos ilícitos com mais dificuldades em encontrar essas pessoas.

Assim, a proliferação dos crimes virtuais encontrou na dificuldade dos legisladores em tipificar esses crimes no ambiente virtual, ou seja, definir as práticas que são criminosas e atribuir penas a elas uma chance de crescer a atuação na rede e alcançar seus objetivos maléficos. Quanto a esse fato, Oliveira e Dani (2013, p.04) citam que:

O grande problema nesses delitos praticados na internet é a ausência quase total de punibilidade pelo Estado, uma vez que, a criminalidade avançou mais rapidamente do que nossa legislação pátria; e as técnicas para chegar ao autor do crime ainda estão em fase de aprimoramento. Os crimes virtuais vêm se tornando corriqueiros em nosso país, e, infelizmente, a lentidão do poder legislativo em tipificar essas modalidades de crimes, vem criando um clima de “terra sem lei” na internet, pois os criminosos sabem que suas identificações são quase impossíveis e mesmo que estes sejam identificados, a lentidão do judiciário ao punir essas condutas cria um clima de impunidade.

Existente no Brasil desde o final da década de 1980, quanto à prática de crimes no ambiente virtual, até o ano de 2012 não existia no Código Penal Brasileiro a tipificação desses

crimes, ou seja, as pessoas que praticassem esses crimes não responderiam pelo ato praticado, pois não existia definição legal para essas ações.

Fato que se modificou somente após anos de análise de projetos de lei, que culminará a demora na proliferação de crimes na rede, surgindo então as Leis 12.735 de 2012 e 12.737 de 2012. Observando um lapso temporal de aproximadamente vinte e cinco anos de inoperância do Estado na criação de normas de regulação do uso da internet. Galli (2013, p.03) cita o Brasil como um dos países que mais utilizam a internet e também um dos que mais sofrem com a ação desses criminosos:

Com 94,2 milhões de pessoas utilizando a internet no Brasil e 45% delas usando redes sociais diariamente, não é difícil imaginar que algumas pessoas vão achar estratégias para roubar dados. Segundo a Bitdefender, a cada 15 segundos, um brasileiro é vítima de fraudes com documentos roubados ou informações furtadas na rede. Mais de 28 milhões de pessoas foram prejudicadas por cibercrimes, o que custou perto de R\$ 16 bilhões ao país em 2012.

O Brasil apesar de ter dimensões continentais e estar entre as nações mais populosas na atualidade, enfrenta variados problemas estruturais, sobretudo na efetivação da justiça, resolvendo as lides. Porém esse atraso estrutural é observado em situações distintas.

A utilização da internet no Brasil é um dos exemplos do atraso do Brasil na adequação da evolução das tecnologias no país, tendo adentrado ao Brasil a mais de vinte anos posteriores a sua criação, que fizeram com que o país já acompanhasse um atraso no uso dessa rede de computadores.

Assim, dentro desse lapso entre a entrada da internet no Brasil e a sua positivação houve um crescimento desordenado do uso da internet e a falta de positivação contribuiu para o crescimento dos crimes no ambiente virtual. Nesse contexto, os brasileiros estão entre as maiores vítimas de crimes virtuais, Oliveira (2011, p. 05):

Os crimes virtuais utilizam a mesma metodologia de crimes utilizados em crimes já conhecidos. A técnica empregada que difere um pouco dos delitos presentes em nosso ordenamento jurídico penal, mas o fim que se pretende é o mesmo da conduta já tipificada. A intenção do criminoso pode ser de ludibriar uma pessoa para obter uma vantagem financeira ou pessoal, enganar suas vítimas ou mesmo furtar informações particulares com o intuito de utilizá-las em proveito próprio.

Embora os brasileiros não possuíssem até o ano de 2012 leis que tipificassem essas condutas, também a ausência de ferramentas que possibilitem a identificação desses criminosos tornaram a rede uma área de fácil acesso para os criminosos. Nota-se que as

formas de se deter os criminosos não acompanharam o desenvolvimento das técnicas de praticar esses crimes.

A ausência de atuação do Estado para coibir a ação dos criminosos e de autoridades especializadas nesses crimes, capazes de entender essas ações lesivas à sociedade fez com que a sociedade se encontrasse desguarnecida. Essa noção fez com que os criminosos desenvolvessem várias técnicas que causaram sérios problemas a usuários que por desconhecimento foram vítimas desses infratores.

O sentimento de impunidade por parte dos usuários da internet gera esse sentimento de medo aos usuários, que por desconhecimento muitas vezes são pegos desprotegidos por esses agentes criminosos e se tornam vítimas em situações do cotidiano do uso da rede.

3.2. A TIPIFICAÇÃO DOS CRIMES VIRTUAIS NO BRASIL

O direito penal brasileiro não detinha até o ano de 2012 nenhuma previsão de crimes para os atos nocivos na rede mundial de computadores que possam ser considerados delitos virtuais. Sendo assim, esses crimes não poderiam ser punidos, pela ausência de tipificação.

Embora esteja entre as nações que mais fazem uso da internet, observa-se que a evolução da rede no Brasil não foi acompanhada pelo direito interno brasileiro, efetivando uma proteção aos usuários. Esse atraso dos legisladores em tipificar esses crimes causou grandes transtornos nos usuários até o ano de 2012 e o surgimento de grandes danos, vivenciados até hoje.

O Brasil ocupa lugar de destaque no cenário global de cibercrimes. Em 2016, 42,4 milhões de brasileiros foram vítimas de crimes virtuais. Em comparação com 2015, houve um aumento de 10% no número de ataques digitais. Segundo dados da Norton, provedora global de soluções de segurança cibernética, o prejuízo total da prática para o país foi de US\$ 10,3 bilhões. Em maio de 2012, o Brasil acompanhou um dos casos mais emblemáticos de crime cibernético cometidos no país: o roubo e a divulgação de mais de 30 fotos íntimas da atriz Carolina Dieckmann. Hackers do interior de Minas Gerais e de São Paulo invadiram o e-mail da artista e a chantagearam, por meio de mensagens anônimas, pedindo R\$ 10 mil para apagar as imagens. O caso foi parar no Congresso Nacional: a Câmara dos Deputados aprovou e colocou em vigor a Lei nº 12.737, apelidada de Lei Carolina Dieckmann, que tipifica delitos cometidos em meios eletrônicos e na internet. (ESTADÃO, 2017).

A visão criada pelos criminosos da internet no Brasil, vista como uma área sem normas, violando padrões morais, éticos e legais estabelecidos foram sendo questionadas como o passar dos tempos, surgindo uma necessidade de se tipificar esses atos, ainda mais

quando se observado que o Brasil é um dos principais usuários de internet dentre as nações, consequentemente como um dos que mais tem ocorrência das práticas de crimes virtuais.

Consequência de um sistema penal que não acompanhou a evolução social, permitindo que os criminosos se espalhassem por meio das brechas que as normas penais davam e a própria ausência de normas capazes de tipificar e punir os agentes dessas práticas lesivas na internet.

Nesse contexto, as Leis 12.735 e 12.737 de 2012 foram grandes conquistas dos usuários da rede mundial de computadores para proteger o uso da internet no Brasil e visando coibir a ação desses criminosos, assim como possibilitar uma punição a esses que afetarem outros usuários com as suas ações.

3.2.1. A Lei 12.735 de 2012 e a Tipificação do Uso de Aparelhos Eletrônicos, Digitais e Similares

O uso da internet no Brasil foi por um longo período ausente de normas de controle, embora não se possa dizer uma inoperância legislativa quanto à busca de criar normas, visto que existiam projetos há anos no Congresso Nacional para serem apreciados, no sentido de proteger o uso da internet no Brasil. Pereira (2013) celebra o surgimento das leis de combate aos crimes virtuais:

A legislação para combater a crimes cibernéticos lembra a internet por celular: chegou tarde, é inadequada e não atinge todos os pontos necessários. As regras eram debatidas desde 1999, mas só quando fotos de Carolina Dieckmann nua vazaram na rede, medidas foram tomadas. A lei que leva o nome da atriz entrou em vigor em 2 de abril, mas acabou deixando de fora pontos óbvios. O sigilo dos e-mails, por exemplo, não está previsto. Como no Direito brasileiro vale somente o que está escrito em uma lei, apenas cartas e telegramas são invioláveis.

Por quase vinte anos, foi discutida dentro da sociedade e os governantes, a criação de normas específicas quanto ao uso da internet, tipificando condutas no ambiente virtual que vierem a causar danos a outros usuários, configurando crimes virtuais, pelo ambiente onde essas práticas eram praticadas.

Até o ano de 2012, existiam apenas algumas práticas contidas no Código Penal que tiveram sua conduta estendida ao uso da internet, ou seja, a prática das ações já descritas crimes no ambiente virtual também já mereciam penas para os agentes, através de uma associação entre a prática descrita no código e a ação no ambiente virtual.

A crescente criminalidade durante a década de 2000 fez com que acentuasse a discussão acerca da necessidade de se tipificar as práticas criminosas na internet. Nessa época,

a internet se difundiu pelo Brasil, sobretudo com a utilização da banda larga e a chegada aos pais de novidades vindas de fora, pois a tecnologia brasileira ainda era inferior a de alguns países.

Nesse contexto, o Projeto de Lei 84 de 1999 da Câmara dos Deputados, proposto por Eduardo Azeredo, que posteriormente foi analisado no Senado com a numeração PL 89/2003 representou legalmente o primeiro ato legislativo voltado especificamente para o uso indevido de aparelhos eletrônicos com a finalidade de causar danos aos outros usuários. Landim (2012, p. 05) cita esse projeto:

Trata-se do projeto de Lei nº 84/1999, que popularmente ficou conhecido como “Lei Azeredo” em razão de ter sido proposta pelo ex-senador e atualmente deputado Eduardo Azeredo (PSDB – MG). Atualmente, não há nenhuma lei específica para monitorar crimes do gênero. Entre as ações propostas por Azeredo, a destruição de dados eletrônicos de terceiros, o acesso e obtenção de informações em sistemas restritos sem autorização e a transferência não autorizada de dados ou informações particulares se tornariam crime, passíveis de prisão e multa.

A demora de atuação dos legisladores em criar as normas, embora existisse o projeto que mesmo depois de quase treze anos de tramitação no Congresso Nacional, somente no ano de 2012 foram realizadas essas alterações legais, com a tipificação dos crimes virtuais.

Referindo-se a Lei 12.735/12, que dentre outras exigências indica que a polícia deve criar locais especializados no combate a crimes eletrônicos. Sendo que são através da denúncia da vítima que serão investigados os casos na rede mundial de computadores. Cunha (2013, p.02) cita que:

Inclui um novo dispositivo na Lei de Combate ao Racismo (7.716/89) para obrigar que mensagens com conteúdo racista sejam retiradas do ar imediatamente, como já ocorre atualmente em outros meios de comunicação, como radiofônico, televisivo ou impresso. Prevê a criação das delegacias especializadas no combate a crimes cibernéticos na Polícia Federal e nas Polícias Civis.

Através da reclamação realizada pela vítima, em casos de veiculação de imagens, dados e informações de usuários por outros mal intencionados podem mediante projeto da lei exposto que é a retirada de imagens veiculadas de maneira ilegal na internet. Exemplo disso é a retirada de imagens racistas imediatamente do ar, protegendo essas pessoas da ação dos criminosos.

Essa medida é oportuna pois muitas dos crimes tipificados e condutas nocivas na internet se proliferam em rápidos lapsos temporais quando postos nas redes, como a

divulgação de imagens íntimas de pessoas pela rede, especialmente quando essas pessoas envolvidas são pessoas famosas. Segundo Melo (2012, p. 03):

A lei tipifica “condutas realizadas mediante uso de sistema eletrônico, digitais ou similares, que sejam praticadas contra sistemas informatizados e similares”. A lei diz que os órgãos da polícia judiciária estruturarão setores e equipes especializadas no combate à “ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado”.

Dotada de seis artigos, a Lei 12.735 de 2012 foi um avanço, embora tenha sua eficácia minada pelos vetos da presidente na época de sanção da lei, o que ocasionou sua perda de efetividade no controle do uso dos aparelhos eletrônicos e a proteção aos usuários da ação dos criminosos.

3.2.2. A Lei 12.737 de 2012 e a Expansão da Proteção aos Usuários da Rede Mundial de Computadores no Brasil

Dentre todas os posicionamentos do direito brasileiro com relação a regulação do uso da rede mundial de computadores, a Lei 12.737 de 2012 foi a mais significativa que alterou o Código Penal brasileiro, introduzindo artigos no tocante a proteção dos usuários de aparelhos eletrônicos contra a ação de pessoas má intencionadas, além de inserir dispositivo referente a falsificação de documentos através da ação desses criminosos. Segundo Cavalcante (2012, p.03):

A Lei n.º 12.737/2012 promoveu as seguintes alterações no Código Penal: I – Acrescentou os Art. 154-A e 154-B, inserindo um novo tipo penal denominado de “Invasão de dispositivo informático”; II – Inseriu o § 1º ao art. 266 prevendo como crime a conduta de interromper “serviço telemático ou de informação de utilidade pública”; III – Inseriu o parágrafo único ao art. 298 estabelecendo que configura também o crime de falsidade de documento particular (art. 298) a conduta de falsificar ou alterar cartão de crédito ou de débito.

Com a Lei 12.737 de 2012, foi introduzido a legislação penal brasileira, no Código Penal os artigos 154-A e 154-B, assim como os provocou alterações nos artigos 266 e 298 do referido código, ambos voltados para a regulação do uso de aparelhos elétricos e crimes no ambiente informático.

Sobretudo, ressalta-se que essa lei se destaca por criar punições às pessoas contra a invasão de equipamentos eletrônicos alheios e a divulgação dessas informações em ambiente virtual. Muito se questiona a aplicabilidade dessas penas, tido por muitas pessoas como penas

brandas; sendo a detenção de três meses a um ano, acrescida de multa aos criminosos virtuais. Manzeppi (2013, p. 05) ainda cita sobre essa punição:

Como prevê o parágrafo 2º, aumenta-se a pena de detenção em 1/6 a 1/3 se da invasão resultar em prejuízo econômico à vítima. Tratou no parágrafo 3º da invasão que ocorre para obter mensagens de e-mails, quando a proposta prevê pena maior, ou seja, de 6 (seis) meses a 2 (dois) anos, além de multa, "se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais e industriais, informações sigilosas assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido." Quanto ao texto do parágrafo 4º, a pena aumenta de 1(1/3) a 2(2/3) terços se houver "divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas, se o fato não constitui crime mais grave."

Alguns dispositivos merecem destaque na lei aprovada, como conforme o Artigo 5º existe a previsão de aumento até a metade da pena em algumas circunstâncias, como quando crime for praticado contra chefes do Executivo, Legislativo e Judiciário. Dentre eles, os Presidentes da República e do Senado, que constantemente são alvos dos brasileiros quanto a sua atuação enquanto líderes políticos no Brasil.

A Lei ainda prevê que em casos que fique comprovada a ocorrência de prejuízos financeiros, deve-se acrescer pela metade a pena, para resguardar aqueles que ficaram prejudicados pela ação desses criminosos, dando a eles uma punição e impedindo que novos agentes pratiquem esses atos.

Além disso, a lei prevê e dá a legitimidade para propor uma ação para as pessoas que forem vítimas desses crimes, se tratando de ação penal pública condicionada, mediante representação da pessoa. Nos casos de crime contra administração pública, a ação será penal pública incondicionada. Cavalcante (2013) informa:

Com o aumento da utilização de smartphones, tablets e computadores portáteis, mais redes sem fio ou redes wireless vão sendo instaladas, dando acesso gratuito à internet, contudo, estas redes permitem o uso de pessoas não identificadas, o que é uma porta de oportunidades para criminosos, pois dificulta sua localização, assim como facilitam a intrusão nestas redes para fins maliciosos. Outra questão relacionada é a falta de registro de usuários que utilizam o serviço de internet nas denominadas lan houses e cyber cafés, assim como o uso de documento falso para preencher cadastros, sejam para acesso a serviços de internet, seja para outros contratos relacionados com o crime investigado, como a abertura de contas bancárias.

Um dos grandes questionamentos acerca dessa lei é justamente que ela não dá às autoridades, meios de identificação dos criminosos e auxílio no colhimento das provas durante o processo, o que dificulta a punição dos responsáveis. A lei prevê que os sites

guardem os dados dos usuários que os acessarem, mas não representou até então uma efetividade desse dispositivo na realidade.

Essa lei foi a mais significativa no âmbito de alertar ao combate aos crimes virtuais existente no direito brasileiro. Apesar de representar um avanço, ainda existem várias questões a serem mudadas na regulação do uso da internet no Brasil, necessitando da incorporação de mais medidas para garantir a efetivação dessa norma e a regulação do uso da rede.

A incorporação de novas ferramentas de controle dos usuários esbarra na estrutura nacional, onde o país embora seja um dos que mais têm usuários não possui tecnologia capaz de identificar criminosos, aumentando-se a cada ano o número de delitos, assim como a variação de crimes a serem difundidos pela rede, aumento à vulnerabilidade dos usuários no acesso à internet. Cavalcante (2013) detalha essa dificuldade:

Apesar dos desafios, soluções estão sendo procuradas, como as novas legislações; treinamentos para policiais, busca de cooperação policial e jurídica internacional, entre outras soluções necessárias para acompanhar o desenvolvimento de novos dispositivos que acessam a internet, a expansão desta, e o conseqüente surgimento de diferentes ameaças. A criminalidade cibernética tornou-se um grande adversário da investigação, havendo necessidade de preparação das polícias, do ministério público e do judiciário para este enfrentamento. Esta modalidade de crimes tem trazido imensos prejuízos para a sociedade, sendo que algumas dificuldades devem ser solucionadas para se adequar ao novo mundo.

A ausência de ferramentas de controle e descoberta dos usuários acaba por influenciar a efetivação dessas, embora não se possa dizer que a sua validade seja comprometida com essa falta de regulação, pois ela representou um marco significativo, dando à sociedade a noção ideal da prioridade em proteger os usuários e conter o avanço desses criminosos.

O Projeto de Lei datado do ano de 2011 já expunha uma demora brasileira em atender essa necessidade de combate aos crimes no ambiente virtual. Apesar de ter dado destaque no momento de sanção da lei a um crime ocorrido contra uma atriz famosa brasileira, Carolina Dieckman, que teve suas fotos íntimas divulgadas mediante a violação de seu aparelho eletrônico. Pinheiro (2013) destaca esse momento:

A nova lei, apelidada de “Carolina Dieckmann”, em referência à atriz que teve 36 fotos íntimas vazadas na internet em maio do ano passado, prevê pena de seis meses a dois anos de reclusão se a invasão resultar na obtenção de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas. “Aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou

transmissão a terceiro, a qualquer título, dos dados ou informações obtidos”, diz o artigo 154-A, do Código Penal.

É notório que a violação da privacidade na internet vem ocorrendo a dados alarmantes, aumentando-se todos os dias o número de vítima pela ação de criminosos. Pessoas famosas tendem a serem mais visadas, pelo seu potencial de divulgação dessas informações.

Uma das vítimas mais comentadas desse crime virtual, nos últimos anos foi a atriz Carolina Dieckmann, que teve imagens suas retiradas de seu e-mail no ano de 2012, por meio da ação de um *hacker*. Revelando também uma tentativa de extorsão, onde os criminosos cobraram o valor de 10 mil reais para devolver as informações retirar, sob a ameaça de divulgá-las. Carrilho (2014, p. 14):

Ao todo, 36 imagens íntimas da atriz foram trazidas ao público em maio de 2012. Ela recebeu ameaças de extorsão para que pagasse cerca de R\$ 10 mil para não ter as fotos publicadas. Carol não cedeu. Após dar queixa, a Polícia descartou a hipótese de as imagens terem sido copiadas de uma máquina fotográfica que havia sido levada para o conserto. A justiça constatou em laudo que a caixa de e-mail da atriz havia sido violada por hackers. Em entrevista, Carol afirma que continua a fazer selfies eróticas para o namorado, que vive na ponte aérea Rio-SP.

As fotos da atriz foram divulgadas na internet e tiveram uma difusão imediata por diversas regiões. Observa-se nesse caso a aglomeração de vários crimes, além do roubo das imagens, tem-se a tentativa de extorsão, difamação. Muito se discutiu na época a possibilidade dessas imagens terem sido retiradas de um computador que tinha sido enviado à assistência, mas posteriormente foi investigado que esses dados foram obtidos por *e-mail*.

Um dos casos recentes mais disseminados e que causou maior revolta dentre a população em geral foi a divulgação das imagens referentes ao cantor Cristiano Araújo, que se envolveu em um acidente no ano de 2015, vindo a óbito juntamente com sua namorada.

Assim, os funcionários da clínica responsável por cuidar do corpo do cantor e sua namorada usaram má-fé e divulgaram imagens do estado do cantor, causando uma grande disseminação em questão de pouco tempo. O que causou grande comoção nacional em relação ao desrespeito cometido contra a vítima.

Essa situação reflete que embora existam já, desde 2012 normas de coação desses criminosos, as pessoas ainda agem acreditando na ausência de punibilidade desses infratores. O que de fato ainda é bastante raro, observando principalmente a dificuldade de descoberta desses criminosos.

Além dos funcionários da clínica, que gravaram o vídeo durante o cuidado do corpo das vítimas, um estudante foi indiciado pelo vazamento desses dados. Os três já enquadrados pelas normas das Leis 12.735/12 e 12.737/12, que são específicas na regulação dos crimes virtuais.

Outro caso de repercussão envolve um dos atores mais famosos do país, Stênio Garcia teve fotos nuas suas e de sua esposa, divulgadas na internet, após serem retiradas de seu celular. Demonstrando mais uma ação dos criminosos virtuais, que não respeitam os dados das pessoas.

Segundo relatos das duas vítimas, as informações eram para serem enviadas para a nutricionista dos envolvidos. O ator e a esposa procuraram a delegacia especializada em crimes virtuais para prestar queixa e depoimento acerca dos fatos ocorridos, visando à identificação dos criminosos.

Por serem famosas, essas vítimas tiveram uma repercussão maior que alguns casos, atingindo grande grau de divulgação dessas imagens principalmente pelas redes sociais e sites pornográficos, assim como cobertura da mídia na busca de solução para esses casos. Apesar disso, a todo o instante, pessoas são vítimas desses crimes no mundo, com um crescimento constante no cenário brasileiro.

É inegável que a repercussão causada por crimes em pessoas famosas é maior, assim como no caso da atriz Carolina Dieckmann, que chamam a atenção popular para o tema, resultaram em grandes avanços na tipificação das leis contra crimes virtuais, onde fica comprovada a vulnerabilidade de toda a frente à internet, independente de classe social, profissão e localização, todos estão ameaçados pela ação de pessoas má intencionadas.

Na segunda parte do texto monográfico foi descrito em breves considerações o surgimento dos crimes virtuais a partir da positivação de leis que introduziram dispositivos no Código Penal brasileiro, regulando a utilização de aparelhos eletrônicos, digitais e a divulgação ilícita dessas informações, sem o consentimento do proprietário do aparelho.

Na terceira parte do texto monográfico, será direcionado o estudo para uma ocorrência bastante comum nos dias atuais, que é a divulgação de imagens íntimas sem autorização, que passaram a ser tipificadas pelo Código Penal a partir da Lei 12.737 de 2012, alterando o artigo 154-A e 154-B.

Desse modo, faz-se nessa parte do estudo, breves considerações acerca desses artigos introduzidos ao Código Penal, assim como um levantamento sobre casos que relatem esses fatos, tão comuns, identificando na jurisprudência brasileira decisões que foquem nessas ocorrências e avaliando a eficácia dessas modificações no dispositivo penal nos dias atuais.

4. A DIVULGAÇÃO DE IMAGENS ÍNTIMAS (NUDES) SEM AUTORIZAÇÃO E A INFLUÊNCIA DAS LEIS nº 12.737 DE 2012 E 12.965 DE 2012 NA APURAÇÃO E PUNIÇÃO AOS INFRATORES DESSE TIPO DE CRIME VIRTUAL

A divulgação de imagens íntimas, sem autorização das pessoas na rede mundial de computadores é bastante comum no cotidiano brasileiro, que vem regada a diversos motivos, principalmente quando os envolvidos são pessoas famosas, sendo alvos de criminosos que divulgam essas imagens, atingindo a privacidade dessas pessoas.

Apesar de representar uma prática comum, mas bastante questionada na sociedade, a divulgação dessas imagens íntimas, sem autorização, popularmente conhecidas como “*nudes*,” caracteriza-se como crime a partir da Lei nº 12.737 de 2012, que acresceu ao Código Penal brasileiro os artigos 154-A e 154-B, que tratam especificamente desses assuntos que serão expostos no estudo. Oliveira (2015) estabelece sobre esse crescimento dessas práticas criminosas:

Os casos de vazamento de imagens íntimas, popularmente conhecidas como “*nudes*”, sem autorização das pessoas que aparecem nas imagens, ganham cada vez mais espaço. As mulheres, segundo o delegado, são os principais alvos de vazamentos de fotos e vídeos íntimos no Rio.

Após ser abordado o surgimento da internet, assim como a proliferação dos crimes virtuais na primeira parte do texto monográfico e na segunda parte do estudo trazer a tipificação dos crimes virtuais, acrescido de breves considerações sobre a morosidade na tipificação das normas referentes aos crimes virtuais.

Na terceira parte do texto monográfico, destaca-se dentre as práticas abrangidas como crimes virtuais pelo direito penal brasileiro, a divulgação dessas imagens via internet, direcionando o estudo a esse meio de comunicação, justamente por sua incidência na sociedade e a dificuldade em se proteger as pessoas e punir os infratores.

Portanto, nesse momento do estudo, focam-se na análise desse tipo de crime voltado ao uso da internet, ações de forma ilegal por parte de pessoas mal intencionadas que ao terem acesso a essas imagens, acabam por violar a privacidade de outras pessoas e expõem a público esse “*nudes*”, causando transtornos a privacidade dessas pessoas.

Para se alcançar uma análise da efetividade da legislação penal referente a esses crimes virtuais a partir da Lei nº 12.737 de 2012, far-se-á um estudo analítico dos artigos inseridos no Código Penal, seguidos de uma abordagem acerca da Lei nº 12.965 de 2014 como meio de auxiliar na identificação dos usuários da internet e consequente forma de descobrir os criminosos que atuam na rede, partindo para uma exposição de casos que

demonstrem a ação desses criminosos, assim como decisões jurisprudenciais aplicadas a esses casos.

4.1. BREVES CONSIDERAÇÕES ACERCA DO ARTIGO 154-A E 154-B DO CÓDIGO PENAL BRASILEIRO

Apesar de tardia, a positivação dos direitos e deveres dos usuários da internet, assim como a tipificação de alguns crimes no ambiente virtual através das Leis nº 12.735 e 12.737 de 2012 e a Lei nº 12.965 de 2014 representaram um marco na utilização da internet no país.

Nesse momento, analisa-se a introdução dos artigos 154-A e 154-B ao Código Penal brasileiro pela Lei nº 12.737 de 2012, com relação a tipificação de crimes referentes a utilização maléfica de aparelhos eletrônicos, digitais ou similares sem a autorização do proprietário.

A legislação brasileira ao incorporar os dispositivos da Lei nº 12.737 de 2012 delimitou a criminalização de ações bastante nocivas no ambiente virtual, que ainda não tinham uma previsão legal para esses fatos, conforme determina o artigo 154-A do Código Penal brasileiro:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012). (BRASIL, 2012)

De acordo com esse artigo, o tipo penal estabelece não determina a necessidade de estar o aparelho eletrônico, digital ou similar conectado à rede mundial de computadores, necessitando apenas a violação desse aparelho sem autorização do proprietário do mesmo.

Além disso, estabelece o tipo penal analisado que para que seja configurada a infração penal, deve-se comprovar a vontade do invasor em obter vantagem com essa ação, tirando proveito das informações obtidas através dessa violação do dispositivo.

Para ampliar o controle e alcançar um número maior de criminosos do ambiente virtual, a lei 12.737 de 2012 acresceu as ações de reprodução, produção, oferecimento, venda e distribuição, de programas ou aparelhos para que se facilite ou permita à violação desses dispositivos a punição do artigo em questão, transformando esses atos em crimes virtuais. Nesse contexto, de acordo com o artigo 154-A, § 2º:

Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. (Incluído pela Lei nº 12.737, de 2012) § 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: (Incluído pela Lei nº 12.737, de 2012) Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012) Vigência. (BRASIL, 2014)

Por meio desses artigos, estabelece-se que a finalidade econômica do infrator ao invadir o dispositivo alheio quando resultar em prejuízo financeiro para a vítima deverá a pena ter uma contagem acrescida em 1/6 a 1/3, de acordo com o grau do prejuízo provocado pelo infrator.

Do mesmo modo, protege-se pelo § 3º desse artigo algumas circunstâncias, como a violação de segredos de empresas ou invasão de dados sigilosos, que possam provocar desvantagens ao proprietário desses dispositivos eletrônicos.

“§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão à terceiro, a qualquer título, dos dados ou informações obtidos”. (BRASIL, 2012)

Determina o parágrafo terceiro desse artigo sobre o cômputo de 1/3 a 2/3 quando o invasor ao encontrar dados do proprietário do dispositivo divulgar essas informações, quando houver a comercio dessas informações ou ainda quando o invasor repassar a terceiros essas informações colhidas nos aparelhos alheios sem autorização. Milen (2017) detalha:

E caso o crime ocorra através de invasões de dispositivos informáticos o Código Penal tem uma tipificação específica acrescida pela lei Nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann), com pena de reclusão de seis meses a 2 anos e aumento de um a dois terços quando houver a divulgação a terceiros do conteúdo obtido.

É justamente o § 3º do artigo 154-A do Código Penal que se relaciona com o objeto de estudo desse texto monográfico, que é a análise da divulgação de imagens íntimas sem autorização, passando a constituir crime a partir dessa positivação pela Lei 12.737 de 2012.

Por meio do artigo 154-B do Código Penal, para que seja dado providência judicial para análise desses casos, deve-se haver a representação por parte do ofendido, ou seja, somente com a sua representação que dá-se início a ação penal, por violar direito da pessoa, sobretudo sua imagem.

Abstrai-se dessa situação quando os fatos transcritos no tipo penal referirem-se a Administração Pública, devendo ser iniciado procedimento de outra forma. Torres (2013) discorre sobre essa representação:

No entanto, só poderão ser protegidas pela lei as vítimas que fizerem registro de ocorrência. "Diferente de outros crimes, o Estado só entra em ação se houver uma denúncia de quem sofreu a invasão", disse o advogado, que explicou que a exigência está no artigo 154-B, também criado pela lei.

O crime descrito no tipo penal do artigo 154-A pode ser praticado por qualquer pessoa, bastando somente à invasão do dispositivo sem autorização para atingir a finalidade, além disso, o ato de instalação de aplicativo ou programa também descreve um ato passível de punição por essa norma, também podendo ser praticada por qualquer pessoa.

Portanto, o ato de divulgar imagens íntimas sem autorização, configura-se como um ato nocivo a privacidade das pessoas, demarcado pela violação da intimidade da pessoa por parte do invasor do dispositivo, podendo ser representada pela divulgação de vídeos, imagens, áudios de natureza íntima.

No polo passivo dessa prática criminal, pode ser qualquer pessoa, que tenha sua intimidade violada a partir da ação desses criminosos, ou seja, não se exige nenhuma qualidade especial para que a pessoa seja atingida por esse crime, além do fato da existência dessas imagens íntimas em dispositivos ou programas. Maggio (2012) aprimora:

O núcleo do tipo penal está representado pelos verbos *invadir* (entrar, tomar conhecimento ou acessar sem permissão) e *instalar* (baixar, copiar ou salvar sem permissão), tendo como objeto material os dados e informações armazenadas bem como o próprio dispositivo informático da vítima que sofre a invasão ou a instalação de vulnerabilidades.

Porém, a dificuldade de controle dessas divulgações de imagens íntimas sem autorização e consequente da apuração da prática dos crimes, associado com a branda punição aplicada nessas ocorrências criminais acaba por atrapalhar a efetivação dessas normas penais, impedindo que elas atinjam a sua finalidade na íntegra e possam representar um resguardo maior as pessoas.

Apesar de ter-se havido um alerta maior posterior a criação da lei e consequentemente haver uma penalização a esses criminosos, demonstrou-se um crescimento nas denúncias desses crimes, apresentando um fenômeno a ser destacado quando se analise a efetividade dessa lei. Serra (2016) informa:

Denunciar é sempre o melhor caminho. Assim que recebemos a denúncia, emitimos uma medida para que o servidor tire imediatamente a publicação do ar. E isso tem que ser cumprido em no máximo 24 horas. Até por telefone cumprimos uma ordem judicial. Ainda que não dê tempo de evitar que a imagem viralize na rede, tentamos minimizar os danos.

Após a positivação da Lei 12.737 de 2012 e a criação da primeira lei voltada para a proteção dos usuários de dispositivos eletrônicos e similares contra a prática de crimes virtuais, observou-se a necessidade criar mecanismos legais para auxiliar a apuração desses crimes e a identificação desses criminosos.

Assim, surge o Marco Civil da Internet no Brasil, com a Lei 12.965 de 2014, que no sentido de coibição do cometimento de crimes no ambiente virtual pode ser entendido como uma norma essencial para proteção da privacidade dos usuários e a identificação dos usuários da rede de computadores.

4.1.1. A Positivação do Marco Civil da Internet e o Auxílio a Identificação dos Usuários da Rede no Combate a Privacidade dos Usuários

Criado pela Lei nº 12.965/14, o Marco Civil da Internet representou mais um avanço do ordenamento jurídico nacional para regular a ação dos usuários na rede mundial de computadores. Representando um auxílio a legislação penal para coibir a ação de criminosos virtuais e surgindo para resolver diversas questões históricas.

“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”. (BRASIL, 2014)

Atualmente, uma das grandes preocupações dos usuários da internet é em relação à privacidade de seus dados pessoais durante o acesso a essa rede. Preocupação acentuada com os constantes casos de invasão de dados e fraudes ocorridos com usuários que muitas vezes são pegos de surpresa em golpes simples. Tomasevícius Filho (2016) esclarece:

A internet transformou as distinções entre esses espaços. Sendo possível acessar a rede de qualquer lugar e a qualquer hora do dia, permite-se a atuação na esfera social, ser visto e ouvido por todos, sem o necessário contato presencial para o estabelecimento dessas relações. Dessa forma, surge uma terceira esfera: a esfera virtual, em que a pessoa se apresenta na rede sem estar presente. O trabalho pode ser realizado socialmente com os trabalhadores em seus lares. O comércio é realizado não mais exclusivamente no mercado, mas também de um ambiente privado ao outro. Crimes podem ser agora praticados a distância. O próprio Estado, que, sem controle, sempre deseja ser onipotente, onipresente e onisciente, quer interferir nessa esfera virtual.

Desde a sua introdução ao cenário brasileiro, à internet foi difundida em larga escala para a sociedade brasileira a partir do ano de 1995, quando deixou de fazer parte somente dos

ambientes universitários e passou a ser espalhada pelos lares brasileiros, sem regulações legais quanto ao seu uso.

As facilidades de seu uso da rede mundial de computadores, assim como a velocidade da troca de informações que serve de grande auxílio para as pessoas fizeram com que elas tornassem a internet numa febre e em um dos instrumentos mais utilizados pelas pessoas no Brasil.

O avanço da internet no cenário brasileiro trouxe consigo a proliferação de atividades de infratores que se valeram da falta de regulação e segurança para os usuários dessa rede mundial no país, que na maioria das vezes foram presas fáceis desses criminosos, que agem sem ter sua identidade encontrada, disseminando ainda mais essas práticas. Tomasevícius Filho (2016) declara:

Ao largo desse problema envolvendo invasão de privacidade praticada por um Estado contra outro, o governo brasileiro pressionou o Congresso Nacional para a aprovação de uma lei sobre comportamentos na esfera virtual, denominada "Marco Civil da Internet" ou de "Constituição da Internet", termo equivocadamente pela própria estrutura internacional da rede, para tentar pôr fim à ideia de que a internet é "terra sem lei".

Por mais de vinte anos, a utilização da internet no Brasil não teve meios de regulação, conseqüente a isso, teve-se o crescimento do uso da rede e o aumento da prática de crimes virtuais fez surgir à necessidade de regular o uso dessa rede. Depois de anos de discussão entre os legisladores, surgiram às primeiras leis de proteção contra as ações de criminosos virtuais e posteriormente, o chamado Marco Civil da Internet.

Discutido desde 2011 pelo Congresso Nacional, o Projeto de Lei nº 2.126/11 representou um alento para as pessoas que buscam a utilização segura da internet no Brasil. Viu-se por anos um atraso dos legisladores brasileiros em relação à regulamentação da utilização da internet, que impôs um cenário de risco no uso da internet no Brasil.

A falta de regulação da internet foi um dos fatores que levaram a tornar a rede um fenômeno mundial de uso pelas pessoas, embora não apresentasse condições seguras para sua utilização e a apuração de crimes quando vivenciados no ambiente virtual. Machado (2016) preceitua sobre uma das medidas tomadas pelos servidores para auxiliar na apuração dos crimes virtuais:

Mas, identificado o usuário no mundo virtual, como se pode chegar até ele? Para resolver esta questão, o art. 13 estabelece que o provedor de conexão (o responsável pelo serviço de acesso do usuário à internet) deverá manter a guarda dos registros de conexão (dados como o IP, com data, horário e fuso horário da conexão de acesso),

sob o sigilo, em ambiente controlado e de segurança, pelo prazo de um ano. Assim, em uma eventual investigação criminal, cruzando-se os registros de acesso a aplicações de internet, armazenados pelo provedor de aplicativos de internet, com os registros de conexão, guardados pelo provedor de acesso, é possível a localização geográfica do ponto de acesso à rede mundial de computadores, a partir do qual se acessou o aplicativo de internet para o cometimento de crimes.

O Marco Civil ao ser regulamento, passou por aprovação do Senado e posterior a isso foi encaminhado a Chefe do Poder Executivo brasileiro, a Presidente Dilma Rousseff para que fosse sancionado, no ano de 2014.

Como grande marco desse projeto, tem-se a neutralidade quanto ao uso da rede. O surgimento do Marco Civil da Internet tem como uma das funções regular a ação das pessoas na rede. Segundo Hudson (2014, p. 01):

Marco Civil da Internet (oficialmente chamado de Lei nº 12.965, de 23 de abril de 2014) é a lei que regula o uso da internet no Brasil, por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

Assim, observa-se que a criação dessa lei que institui o marco civil da internet, tem como uma das funções a busca de um uso mais transparente da internet, mais claro, garantindo aos usuários garantias de segurança melhores, assim como estabelecimento de direitos e deveres aos envolvidos nessa rede mundial de computadores.

Dentre os direitos introduzidos aos usuários da internet no Brasil, a partir do marco civil, tem-se a proteção à privacidade desses usuários, impedindo que possam ser disponibilizados dados pessoais dessas pessoas pelos provedores da rede de computadores. Lourenço (2014, p.02) cita que:

O marco civil, aprovado pelo plenário do Senado na noite de ontem (22), define os direitos e deveres de usuários e provedores de serviços de conexão e aplicativos na internet. A aprovação abre caminho para que os internautas brasileiros possam ter garantido o direito à privacidade e à não discriminação do tráfego de conteúdo.

Através desse marco da internet, é obrigação das empresas delimitar meios que protejam as informações pessoais dos usuários da internet. Também será dado tratamento igual aos usuários, independente das atividades que venham a realizar na rede.

O inciso VII do artigo 7º da Lei 12.965 de 2014 assinala esse dever dos órgãos envolvidos com dados dos usuários nas redes sociais, delimitando com isso o “não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei”. (BRASIL, 2014).

Ainda, o texto dessa lei sancionada tem dado às empresas e sites a oportunidade de contribuir de maneira eficiente para a proteção aos usuários de internet, agindo na criação e utilização de mecanismos que visem dar a esse usuário uma segurança quando fizerem uso da rede.

Assim, as empresas que necessitarem de dados pessoais dos seus usuários, não poderão mais disponibilizar esses dados a outras empresas ou outros usuários, ficando o uso restrito a essa empresa inicial. Essas informações deverão ser guardadas pelas empresas e somente através de decisão judicial poderão ser divulgadas quando solicitadas. Martins (2014, p. 14) declara:

O marco também garante a privacidade dos usuários da internet, ao estabelecer que informações pessoais e registros de acesso só poderão ser vendidos se o usuário autorizar expressamente a operação comercial. Atualmente, os dados são usados por grandes empresas para obter mais receitas publicitárias, já que elas têm acesso a detalhes sobre as preferências e opções dos internautas e acabam vendendo produtos direcionados.

Atualmente, a internet possui várias redes sociais, onde as pessoas expõem sua vida por meio de fotos, vídeos, dados, representando uma ameaça a esse uso. Um dos principais problemas e dos mais constantes enfrentados pelos usuários que é o uso dessas informações, sejam elas fotos, vídeos, dados por pessoas com objetivo de distorcer a imagem das pessoas, como a divulgação de imagens íntimas de uma pessoa em redes sociais.

Assim, de acordo com o Novo Marco Civil da Internet prevê algumas alterações quanto a essas possibilidades, dando a justiça o poder de responsabilizar as empresas e pessoas pela veiculação dessas informações quando feita de má-fé. Pereira (2012, p. 03) cita:

A empresa que fornece conexão nunca poderá ser responsabilizada pelo conteúdo postado por seus clientes. Já quem oferece serviços como redes sociais, blogs, vídeos etc. corre o risco de ser culpado, caso não tire o material do ar depois de avisado judicialmente. Por exemplo: se a Justiça mandar o Google tirar um vídeo racista do YouTube e isso não for feito, o Google se torna responsável por aquele material. Haverá um prazo para que o conteúdo considerado ofensivo saia de circulação, mas o juiz que cuidar do caso pode antecipar isso se houver “prova inequívoca”, levando em conta a repercussão e os danos que o material estiver causando à pessoa prejudicada.

Essa é uma das medidas que visa à proteção das pessoas, que por descuido ou por má fé de pessoas tem sua intimidade exposta. Tem-se então a responsabilização das empresas responsáveis, que para não serem punidas, terão uma atenção maior quanto ao conteúdo veiculado.

É bastante comum os sites, atualmente, possuírem classificação etárias, assim como avisos sobre o conteúdo divulgado nesses sites, buscando que as pessoas obtenham informações pertinentes ao material divulgado antes mesmo do acesso inicializado.

Ferramentas como *e-mails* também ganharam um caráter mais restrito com esse Marco Civil, no artigo 7º da referida lei, onde se vê que os usuários da internet deverão ter seus conteúdos protegidos, não podendo ser acessados, assumindo o formato sigiloso, visto a privacidade eludida por trás desses endereços postais.

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização. (BRASIL, 2014).

Quanto a atuação estatal no controle dos usuários, caberá ao Poder Judiciário também a competência de analisar a retirada de conteúdos tidos como impróprios do ar, não sendo obrigados os proprietários desses sites, retirá-los sem previa autorização judicial.

Prevê ainda a Lei 12.965 de 2014 a privacidade dos usuários no sentido de “Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet”. (BRASIL, 2014).

Nesse sentido, a divulgação de imagens íntimas tem nessa atuação do Poder Judiciário, uma ferramenta essencial para conter essa difusão pelos sites e redes sociais, impedindo que os efeitos sejam mais maléficos às vítimas dessas ações. Nesse sentido, o artigo 19 da Lei 12.965 de 2014 prevê essa situação:

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (BRASIL, 2014)

Abre-se somente uma possibilidade, quando houver a divulgação de conteúdos que visem à difamação de pessoas, dando a essas pessoas o poder de requerer diretamente a esses provedores a retirada do ar dessas informações, sendo realizada de forma imediata.

As pessoas poderão solicitar aos Juizados Especiais a apreciação desses casos, onde serão avaliadas as possíveis violações a honra dessas pessoas. Protegendo as vítimas desses casos da má-fé de alguns criminosos. Martins (2014, p. 16):

Os internautas deverão, de acordo com a lei, ter informações claras e completas sobre os contratos de prestação de serviços e coleta, uso, armazenamento, tratamento e proteção de dados pessoais, bem como ter garantida a acessibilidade, levando em conta as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário.

Assim, como em outras áreas da sociedade, a conscientização talvez seja a solução para esse mau uso da internet. A difusão de campanhas de conscientização, de notas que explique e capacitem às pessoas para o uso seguro da internet pode garantir a esses usuários uma sabedoria maior na luta contra os criminosos.

Dá-se maior liberdade aos usuários de poderem utilizar da internet para expor suas ideias com o Novo Marco Civil, garantindo a esses usuários que os provedores não podem censurar, nem privilegiar conteúdos em detrimento de outros. A internet passa então a ser uma rede mais neutra, desenvolvendo possibilidades de acessos igualitários a todos os usuários.

Como esse Marco Civil é atribuído ao Governo Federal, estados, municípios e Distrito Feral a função de reduzir à desigualdade relativa ao conhecimento e uso da internet criando formas de que a tecnologia chegue ao povo, possibilitando a todos o manuseio da rede mundial. Pereira (2012, p. 03) cita que:

Os governos serão obrigados a estimular a expansão e o uso da rede, ensinando as pessoas a mexer com a tecnologia para “reduzir as desigualdades” e “fomentar a produção e circulação de conteúdo nacional”. Os serviços de governo eletrônico precisarão ser integrados para agilizar processos, inclusive com setores da sociedade, e a internet ainda será usada para “publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada”.

Procurou-se com essa atribuição de deveres ao governo, nas suas variadas escalas, retribuir a demora em cuidar em criar normas de regulação do uso da internet. Responsabilizando esses entes quanto à diminuição da desinformação sobre a utilização da internet.

Não basta apenas conscientizar, é necessário desenvolver meios de aproximar a internet das camadas menos favorecidas, assim como dispor de mecanismos de proteção a essas pessoas que não possuem tanta sabedoria no uso dessa ferramenta.

O Marco Civil foi o grande avanço até hoje desenvolvido pelo governo para tentar regular à ação das pessoas na rede, dando-lhes direitos e deveres quanto ao seu uso. Criando

mecanismos também que visão atribuir tarefas aos Estados, Municípios, Distrito Federal, a sociedade e as empresas em geral. Quanto ao registro das informações dos usuários, Machado (2016) assevera:

Já o ponto controvertido está no art. 15, que tornou obrigatória medida que, até então, nada mais era que uma recomendação do Comitê Gestor da Internet (CGI). Segundo o novo dispositivo legal, os provedores de aplicativos (aqueles que disponibilizam aplicativos ao cliente, como o site de uma *internet banking* ou mesmo uma rede social) deverão armazenar, por seis meses, os registros de acesso de seus usuários (informações como o número do endereço de protocolo de internet, com data, horário e fuso horário do acesso ao aplicativo).

O maior beneficiário do uso da criação do Marco Civil da internet é o usuário, que também poderá ter um papel ativo na decisão de assuntos relacionados à internet, como prevê o texto dessa lei, possibilitando em algumas circunstâncias a realização de debates na internet entre os membros da sociedade visando tomar decisões que melhor garantam a utilização dessa rede mundial no Brasil.

A aplicação do direito no Brasil sempre foi bastante contestada por grande parcela da sociedade. E, isso se refletiu na maneira como o direito brasileiro tratou os casos de crimes virtuais. A demora na tipificação dessas normas deu aos criminosos um campo maior de atuação.

Nesse ponto, o Brasil apresentava um atraso em relação aos demais países na criminalização daqueles que usam a internet com má-fé. Apesar disso, a criação do Marco Civil da Internet é tida como uma das referências a nível global de uso da internet, tornando o Brasil pioneiro na disposição de direitos e deveres dos usuários da rede. Farinaccio (2017) assevera:

Coisas bem sérias também é tema de discussão no Marco Civil da Internet, incluindo crimes e outras práticas extremamente danosas para usuários. Diversos desses projetos tratam de condutas consideradas fora da lei, desde práticas de extorsão, crimes cibernéticos, difamação e calúnia, bullying online, sem contar conteúdo racista e discursos de ódio de todos os tipos. Três desses projetos surgiram apenas nessa recente onda da brincadeira da Baleia Azul.

Embora esteja em vigor a mais de um ano, pois essa norma entrou em vigor em Junho de 2014, o Marco Civil ainda não representou grandes alterações no uso da internet. Os objetivos propostos por essa lei em sua grande maioria não foram colocados em prática, deixando os usuários desprovidos de segurança.

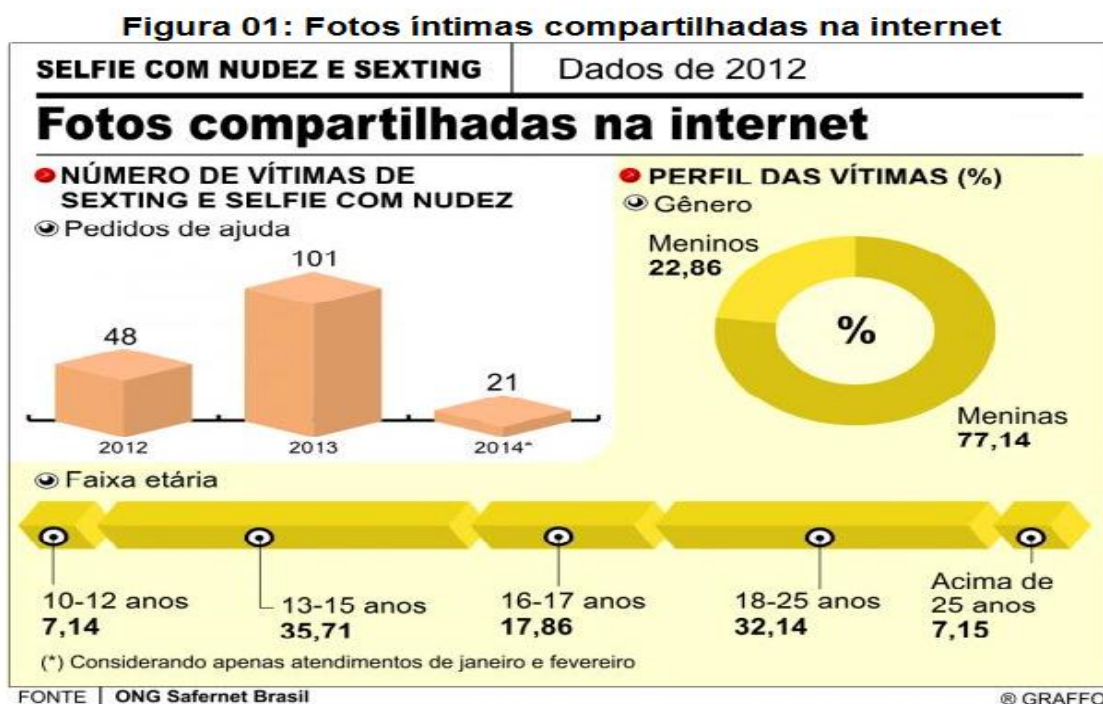
Analisa-se agora a divulgação de imagens íntimas sem a autorização, popularmente conhecido como vazamento de *nudes*, caracterizando uma forma de crime virtual comum e crescente na sociedade brasileira, necessitando de uma atuação mais efetiva do Estado no seu controle e punição.

4.2. A DIVULGAÇÃO DE IMAGENS ÍNTIMAS SEM AUTORIZAÇÃO NA INTERNET

O vazamento de *nudes*, como é conhecido popularmente à divulgação de imagens íntimas sem autorização apresentou um crescimento nos últimos anos, muito devido à positivação de normas no sentido de coibir a ação desses criminosos virtuais, como é a Lei 12.737 de 2012 vindo de forma tardia, quase trinta anos posterior a implementação da internet no Brasil.

Além disso, a punição até certo ponto branda para os infratores passou a ser questionada, principalmente por aqueles que tiveram sua privacidade exposta a partir da ação desses criminosos, que fazem uso desses equipamentos para divulgar essas imagens de cunho íntimo.

A Figura 01 traz uma exposição dos dados referentes ao ano de 2012, pelo SAFERNET, site que analisou a quantidade de casos investigados e denúncias referentes a prática desses crimes virtuais, observando especialmente um crescimento demasiado no ano de 2013, ano posterior à sanção da Lei 12.737 de 2012.



A partir dessa pesquisa, vê-se que em sua maioria as vítimas são do sexo feminino, representando quase oitenta por cento da pesquisa, conforme delimita o gráfico acima. Também se pode expor a partir da análise da figura, que a maior parte das vítimas tem entre treze e quinze anos de idade, revelando com isso uma prática mais comum entre os jovens.

Frisa-se que os casos de vazamento de nudes, embora estejam sendo analisados na esfera criminal nesse estudo, através da tipificação desse crime virtual, também enseja ações no âmbito civil, para reparação dos danos morais causados a vítima pela ação dos criminosos.



Observou-se pelos dados do site Safernet, que analisa o ambiente virtual no Brasil um crescimento considerável e anormal desde o ano de 2012, tendo somente uma leve queda nos casos levados a denúncia no ano de 2016, porém demonstrando-se nesse lapso temporal de vigência da lei um crescimento nas denúncias.

A própria jurisprudência tem considerado essa possibilidade de punição decorrente da divulgação de imagens íntimas, aplicando pelos tribunais a legislação presente no artigo 154-A do Código Penal brasileiro, reconhecendo o prejuízo à vítima da ação dos criminosos virtuais, conforme decisão jurisprudencial acima mencionada.

INVASÃO DE DISPOSITIVO INFORMÁTICO - materialidade – prova oral e documentos acostados aos autos comprovando a invasão do sistema operacional do site da vítima, da obtenção de informações sigilosas e da alteração de dados do

sistema. – réu que não se desincumbiu de atestar o alegado – não acolhimento – declaração de vítima apontando o réu como sendo o autor do delito – validade – versão da vítima confirmada pelos e-mails e pelo restante da prova documental acostada aos autos. CAUSA DE AUMENTO – art. 154-A, § 2º, do CP - e-mail, comprovante de depósito e prova oral indicando o prejuízo econômico suportado pela vítima. (TJ-SP 30036070720138260586 SP 3003607-07.2013.8.26.0586, Relator: Lauro Mens de Mello, Data de Julgamento: 24/08/2017, 6ª Câmara de Direito Criminal, Data de Publicação: 29/08/2017). (BRASIL, 2017)

Na tipificação dos crimes virtuais referentes ao vazamento de nudes, estudasse pelos congressistas a incorporação de dispositivo pela Lei nº 11.340 de 2006, no sentido de trazer uma proteção maior as mulheres, que são as maiores vítimas desses crimes, geralmente divulgadas por seus parceiros na rede de computadores.

Na terceira parte do texto monográfico foi abordada em específico a aplicação desses diplomas legais aos casos de divulgação de imagens íntimas sem autorização, popularmente conhecidas na sociedade como vazamento de nudes, debatendo de forma clara a aplicação jurisprudencial nesses casos e a valorização dos direitos dos usuários da internet a partir dessa lei.

Observa-se ainda que conforme dados expostos na figura, pode-se compreender que a Lei nº 12.737 de 2012 já atingiu um dos sentidos da lei, que é informar as pessoas medidas que devem ser seguidas quando da ocorrência dos casos. Assim, o crescimento do número de denúncias representa a ocorrência de amparos maiores às pessoas, como departamentos especializados na apuração desses crimes no ambiente virtual.

À medida que as pessoas passam a dotar de meios mais efetivos de combate e controle da ação dos criminosos, conseguem ter uma segurança maior para buscar auxílio na justiça. Os artigos 154-A e 154-B estabeleceram amparos legais a essas pessoas, permitindo que elas busquem a reparação dos danos causados a imagem.

5. CONSIDERAÇÕES FINAIS

A internet constituiu uma grande ferramenta para a sociedade brasileira, capaz de ligar pessoas nos mais remotos cantos do mundo em questão de um curto período de tempo, tornando-se uma febre na sociedade e permitindo que as mais variadas pessoas possam ter acesso à essa ferramenta.

Ao mesmo tempo em que representou um avanço considerável na sociedade brasileira, a internet apresentou diversos riscos a sociedade, pois não apresentou legislação que regulasse a atuação das pessoas nessa grande rede mundial de computadores.

Essa ausência de normas direcionadas, a regulação do uso da internet no Brasil, causou o crescimento também de uma ameaça representada pelos crimes virtuais, que cresceram em larga escala no país, impedindo que as pessoas pudessem se relacionar na rede sem serem ameaçadas pela ação de criminosos.

Nesse sentido, foram desenvolvidos, no ambiente virtual diversos crimes, que trouxeram uma insegurança aos usuários e revelaram uma necessidade urgente de atuação do Estado, tanto na elaboração de leis que punissem os infratores, como na apuração e punição dos mesmos.

Dentre os crimes no ambiente virtual, a divulgação de imagens íntimas sem autorização, também chamada de vazamento de nudes representa uma afronta à privacidade das pessoas, consumando o disposto no § 3º do artigo 154-A do Código Penal brasileiro.

Assim, a partir desse artigo, passou-se a punir as pessoas que mal intencionadas tem acesso a imagens íntimas de outras e divulgam, no sentido de vulgarizar a imagem da outra pessoa, passando então a cometer um crime, que embora tenha uma pena branda, deve gerar a responsabilização do infrator.

Constatam-se por meio do trabalho monográfico, que embora represente uma necessidade de garantir aos usuários da internet uma segurança maior no seu uso, as leis 12.737 de 2012 e 12.965 de 2015, foram essenciais para que se possam garantir às pessoas a punição aqueles que infringirem padrões estabelecidos pela lei, ao mesmo tempo, nota-se que os resultados ainda não são os esperados, com uma pequena resolução para grande parte dos casos levados a apreciação.

REFERÊNCIAS

BRASIL. **Lei nº 12.735, de 30 de Novembro de 2012.** Brasília, 2012.

_____. **Lei nº 12.965, de 23 de abril de 2014.** Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 05 de nov. 2017

_____. **Lei nº 12.737, de 30 de Novembro de 2012.** Brasília, 2012.

CARRERA, Mario Sérgio Valadares. **A Pedofilia Virtual e Seus Reflexos no Âmbito Jurídico.** Disponível em:< <http://www.egov.ufsc.br/portal/conteudo/pedofilia-virtual-e-seus-reflexos-no-%C3%A2mbito-jur%C3%ADdico>>. Acesso em 12 de nov. 2017.

CARRILHO, Ulisses. **Carolina Dieckmann, a vizinha famosa de todos nós.** Disponível em:<<http://revistadonna.clicrbs.com.br/moda/carolina-dieckmann-a-vizinha-a-famosa-de-todos-nos/>>. Acesso em: 06 de nov. 2017.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.** Disponível em: <http://www.soci.org.br/files/trajetoria_internet.pdf>. Acesso em: 14 de out. 2017.

CAVALCANTE, Márcio André Lopes. **Primeiros comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático.** Disponível em: [http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.ht ml](http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.ht%20ml). Acesso em: 14 de out. 2017.

DUMAS, Veronique. **A origem da internet.** Disponível em:<<http://revistahistorien.blogspot.com.br/2011/08/origem-da-internet.html>>. Acesso em: 06 de nov. 2017.

CUNHA, Clareane. **Lei de Cibercrimes e Lei Azeredo entram em vigor e o Marco Civil? Nada.** Disponível em: <http://marchamulheres.wordpress.com/2013/04/05/lei-de-cibercrimes-e-lei-azeredo-entram-em-vigor-e-o-marco-civil-nada/>. Acesso em: 14 de out. 2017.

ESTADÃO. **Crimes virtuais afetam 42 milhões de brasileiros.** Disponível em:<<http://economia.estadao.com.br/noticias/releases-ae,crimes-virtuais-afetam-42-milhoes-de-brasileiros,70001644185>>. Acesso em: 11 de nov. 2017

FACHINI, Thiago. **Quais os crimes virtuais e golpes digitais mais comuns?**. Disponível em: <http://tiagofachini.jusbrasil.com.br/artigos/156312969/quais-os-crimes-virtuais-e-golpes-digitais-mais-comuns>. Acesso em: 14 de out. 2017.

FARINACCIO, Rafael. **Marco Civil da Internet faz três anos sendo alvo de 56 propostas de mudança**. Disponível em: <https://www.tecmundo.com.br/internet/116066-marco-civil-internet-tres-anos-sendo-alvo-56-propostas-mudanca.htm>. Acesso em 10 de nov. 2017.

GUSMÃO, Gustavo. **Brasil é o segundo país com mais downloads em ranking de pirataria**. Disponível em: <https://exame.abril.com.br/tecnologia/brasil-e-o-segundo-pais-com-mais-downloads-em-ranking-de-pirataria/> Acesso em 21 de out. 2017.

HUDSON, ALEX. **O Marco Civil da Internet**. Disponível em: <http://rbrj.com.br/tecnologia/>. Acesso em: 14 de out. 2017.

KLEINA, Nilton. **A história da Internet: pré-década de 60 até anos 80**. Disponível em: <http://homepages.dcc.ufmg.br/~mlbc/cursos/internet/historia/Brasil.html>. Acesso em: 14 de out. 2017.

LANDIN, Wikerson. **Conheça a Lei Azeredo, o SOPA brasileiro**. Disponível em: <http://www.tecmundo.com.br/ciencia/18357-conheca-a-lei-azeredo-o-sopa-brasileiro.htm>. Acesso em: 14 de out. 2017.

LOURENÇO, Laura. **Dilma sanciona Marco Civil da Internet**. Disponível em: <http://diariodoaco.com.br/noticias.aspx?cd=80295>. Acesso em 14/10/2015.

MAATSUDA, Sérgio. **Relatório detalha em números explosão de preconceito na internet em 2014**. Disponível em: <https://oglobo.globo.com/sociedade/tecnologia/relatorio-detalha-em-numeros-explosao-de-preconceito-na-internet-em-2014-15299044#ixzz4xfyaEUO3stest>. Acesso em 06 de nov. 2017.

MACHADO, Felipe. **Marco Civil traz efeitos na apuração criminal, mas pode invadir privacidade**. Disponível em: <https://www.conjur.com.br/2014-jul-14/felipe-machado-marco-civil-traz-efeitos-apuracao-criminal>. Acesso em: 30 de out. 2017.

MAGGIO, Vicente de Paula Rodrigues. **Novo crime: invasão de dispositivo informático - CP, Art. 154-A**. Disponível em: <https://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a>. Acesso em 06 de nov. 2017.

MANZEPPI, Eduardo. **A chamada Lei “Carolina Dieckmann” (Lei nº 12.737/2012).** Disponível em: http://www.olhardireto.com.br/jurídico/artigos/exibir.asp?artigo=A_chamada_Lei_Carolina_Dieckmann_Lei_n_127372012&id=296. Acesso em: 14 de out. 2017.

MARTINS, Helena. **Entenda o Marco Civil da Internet.** Disponível em: <http://www.ebc.com.br/noticias/brasil/2014/04/entenda-o-marco-civil-da-internet>. Acesso em: 14 de out. 2017.

MELLO, Tatiane Dias. **Dilma sanciona leis que definem cibercrimes.** Disponível em: <http://link.estadao.com.br/noticias/geral,dilma-sanciona-leis-que-definem-ciber-crimes,10000034487>>. Acesso em: 10 de nov. 2017.

MIECOANSKI, Ellen; TAVARES, Osny. **Em dez anos, usuários de internet no Brasil passaram de 6% para 35%.** Disponível em: <http://www.gazetadopovo.com.br/vida-e-cidadania/em-dez-anos-usuarios-de-internet-no-brasil-passaram-de-6-para-35-2ujy1lqyl2wwc8pytoatetse>. Acesso em: 24 de out. 2017.

MILEN, Marconi Valente Teixeira Asséf. **Vazar “nudes” já é crime, mas poderá ter criminalização específica na lei Maria da Penha.** Disponível em: <http://www.mantenanews.com/#/vazar-nudes-ja-e-crime-mas-podera-ter-criminalizacao-especifica-na-lei-maria-da-penha/>>. Acesso em 08 de nov. 2017.

NASCIMENTO, Unilson Souza Rangel. **Sequestro virtual pode ser evitado com serviços especializados de segurança em TI.** Disponível em: <https://www.linkedin.com/pulse/sequestro-virtual-pode-ser-evitado-com-servi%C3%A7os-de-em-unilson>. Acesso em: 10 de out. 2017.

OLIVEIRA, Adeilson de. **Vazamento de 'nudes' é crime virtual mais comum no Rio, diz delegado.** Disponível em: <https://adeilsonfilosofo.jusbrasil.com.br/artigos/260392266/vazamento-de-nudes-e-crime-virtual-mais-comum-no-rio-diz-delegado>>. Acesso 31 de out. 2017.

OLIVEIRA, Luis Gustavo Caratti de e DANI, Marília Gabriela Silva. **Os crimes virtuais e a impunidade real.** http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963. Acesso em: 19 de out. 2017.

OLIVEIRA, SOLANGE. **Como denunciar um crime virtual.** Disponível em: <http://ecommercegirl.com/uncategorized/como-denunciar-um-crime-virtual/>. Acesso em: 02 de out. 2017.

PEREIRA, Felipe. **Lei melhora combate a crimes cibernéticos, mas apresenta deficiências.** Disponível em: <http://jornaldesantacatarina.clicrbs.com.br/sc/noticia>

/2013/05/lei-melhora-combate-a-crimes-ciberneticos-mas-apresenta-deficiencias-4126522.html>. Acesso em 14 de nov. 2017.

PINHEIRO, Jana. **Lei de crimes virtuais já está em vigor.** Disponível em:<<http://www.tjmt.jus.br/noticias/29323#.Wf8c349SziU>>. Acesso em 07 de nov. 2017.

RODRIGUES, Vinícius. **A origem da Internet.** Disponível em: <http://WWW.grupoescolar.com/pesquisa/a-origem-da-internet.html>. Acesso em: 05 de out. 2017.

SERRA, Amanda. **Mandar nude não é crime:** divulgar fotos sem consento é. Disponível em:<<http://www.compromissoeatitude.org.br/mandar-nude-nao-e-crime-divulgar-fotos-sem-consenso-e-diz-promotora-uol-07072017/>>. Acesso em 06 de nov. 2017.

SIQUEIRA, Ethevaldo, MANCINI, Luciana. 1993, “Rumo ao caos”, In: Siqueira, Ethevaldo. **Telecomunicações: privatização ou caos.** São Paulo, TelePress. Editora Ltda. pp.10-29.

STRINGARI, Gabriel. **A diferença entre hacker e cracker.** Disponível em: <http://www.hiperfree.com/blog/a-diferenca-entre-hackers-e-crackers/>. Acesso em: 14 de out. 2017.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet:** uma lei sem conteúdo normativo. Disponível em:<http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269>. Acesso em 08 de nov. 2017.

TORRES, Lucas. **Entenda o que muda com a lei Carolina Dieckmann.** Disponível em:<<http://www2.sidneyrezende.com/noticia/204758+entenda+o+que+muda+com+a+lei+carolina+dieckmann>>. Acesso em 06 de nov. 2017.

TRISTÃO, Marcos Paulo. **A divulgação de fotos íntimas sem autorização é crime.** Disponível em:<<http://www.folhados.com/noticia/2014/04/18/a-divulgacao-de-fotos-intimas-sem-autorizacao-e-crime.html>>. Acesso em 06 de nov. 2017.

VIANA, André de Paula. **Crimes virtuais e a necessidade de uma legislação específica.** Disponível em:<<http://www.egov.ufsc.br:8080/portal/conteudo/crimes-virtuais-e-necessidade-de-uma-legisla%C3%A7%C3%A3o-especifica>>. Acesso em 12 de nov. 2017.