FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE- FANESE
CURSO DE DIREITO

LEONE RODRIGUES DOS SANTOS

CRIMES CIBERNÉTICOS

ARACAJU
2019

CRIMES CIBERNÉTICOS

CRIMES CIBERNÉTICOS

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Fanese como requisito parcial e obrigatório para a obtenção do Grau de Bacharel em Direito.

Orientador: Prof. Esp. Ivis Melo

ARACAJU
2019

S237c SANTOS, Leone Rodrigues dos

Crimes Cibernéticos / Leone Rodrigues dos Santos; Aracaju, 2019. 44p.

Trabalho de Conclusão de Curso (Graduação) – Faculdade de Administração e Negócios de Sergipe. Coordenação de Direito.

Orientador(a) : Esp.Ivis Melo de Souza.

1. Crimes Cibernéticos 2. Internet 3. Lei 4. Crimes virtuais.
343.98 (813.7)

Elaborada pela bibliotecária Lícia de Oliveira CRB-5/1255

LEONE RODRIGUES DOS SANTOS

CRIMES CIBERNÉTICOS

Monografia apresentada à Faculdade de Administração e Negócios de Sergipe como exigência parcial para obtenção do grau de Bacharel em Direito.

Aprovado em 05/12/2019

BANCA EXAMINADORA

Prof. Esp. Ivis Melo de Souza (Orientador)
Faculdade de Administração e Negócios de Sergipe

Prof. Me. Osvaldo Resende Neto
Faculdade de Administração e Negócios de Sergipe

Prof. Dr. Denival Dias de Souza
Faculdade de Administração e Negócios de Sergipe

Agradecimentos

Gostaria de agradecer primeiro a Deus por toda força dada a mim durante todo esse tempo em que confeccionei o meu TCC.

Aos meus pais, pois sem eles não teria como sentar-me diariamente para poder estudar, pesquisar acerca do meu tema.

Agradeço também ao meu Orientador Ivis Melo, pois sem uma orientação a presente pesquisa nem sequer iniciaria, muito menos seria finalizada como está. Agradeço por todo o conhecimento por ele passado. Ivis, o senhor é um professor incrível!

Agradeço a todos os meus amigos e colegas que me ajudaram em todas as dúvidas que tive durante todo esse tempo, pelo conhecimento compartilhado.

Agradeço ao Professor Eudes, pois sem o auxílio dele referente as questões da formatação do trabalho eu não teria conseguido.

Agradeço também aos professores avaliadores pelas sugestões e dicas para que o meu trabalho fosse depositado da forma mais correta possível.

RESUMO

A presente pesquisa visa mostrar a importância da existência da tipificação de crimes cometidos na Internet, através de estudos que demonstrem os principais crimes cometidos neste meio, pesquisando sobre Crimes Cibernéticos, a fim de analisar alguns dos crimes digitais cometidos por meio de dispositivos informáticos (computador, *tablet*, celular etc.), mais especificamente sobre os crimes contra a honra, racismo, pornografia, *revenge porn* e estelionato. Para tanto, é necessário identificar quais os principais crimes praticados na Internet, quais as principais legislações e quais são as principais ameaças. Realiza-se, então, uma pesquisa frente aos principais autores que discorrem sobre a relação do Direito Penal com os crimes cibernéticos, utilizando o método dedutivo de natureza qualitativa. Com isso, possibilitou o conhecimento acerca das leis que tratam os crimes cibernéticos, em especial a lei 12.737/2012 (Lei Carolina Dieckmann) e a Lei 12.737/2012 (Lei do Marco Civil da Internet) e de como se dá as ameaças deste tipo de crime no Brasil.

Palavras-chave: Crimes Cibernéticos. Internet. Lei. Crimes Virtuais.

ABSTRACT

This research aims to show the importance of the typification of crimes committed on the Internet, through studies that demonstrate the main crimes committed in this environment, researching cybercrimes, an aim to analyze some digital crimes committed through computer devices (computer, tablet, etc.), specifically on crimes against honor, racism, pornography, revenge pornography and estelionate. To this end, it is necessary to identify which are the main crimes committed on the Internet, which are the main legislations and which are the main threats. Then, we conduct a research in front of the main authors who discuss a relationship of criminal law with cybercrimes, using the deductive method of qualitative nature. Thus, it is possible to know about laws that deal with cybercrimes, especially Law 12.737 / 2012 (Carolina Dieckmann Law) and Law 12.737 / 2012 (Internet Civil Marco Law) and how it gives as this type of crime. crime in Brazil.

Keywords: Cybercrime. Internet. Law. Virtuals Crimes.

LISTA DE SIGLAS E ABREVIATURAS

ART. - Artigo

Nº - Numero

CP - Código Penal

LNCC - Laboratório Nacional de Computação Científica

CF/88 – Constituição da República Federativa do Brasil de 1988

CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

SUMÁRIO

1 INTRODUÇÃO

A evolução tecnológica no mundo fez com que o crescimento entre o convívio via equipamentos eletrônicos se tornasse algo muito maior do que o convívio direto, real. Estando conectados a culturas diferenciadas as pessoas passaram a encontrar na internet novas relações sociais, razão pela qual houve a necessidade de o Direito moldar esta nova realidade, podendo assim caminhar junto com a segurança da informação, para que esta sociedade cibernética não se tornasse uma sociedade sem regras.

Como em todo território brasileiro, os direitos e deveres dos cidadãos, bem como das instituições e do meio ambiente passaram a ser preservados pelas legislações em vigor. O não cumprimento delas constitui uma infração ou um crime.

Diante de uma nova modalidade de crime, o crime cibernético teve uma legislação criada em 2012, a lei 12.737/2012, mais conhecida como lei Carolina Dieckmann que promoveu alterações no Código Penal Brasileiro e tipificou tais delitos.

Neste cenário, surge uma questão: Como é tratado os Crimes Cibernéticos no ordenamento brasileiro?

Outras questões surgem para nortear esse problema, quais sejam: a) quais os principais crimes praticados na internet?; b) Como é tratado os crimes perpetuados na internet em outros países?; c) Qual a principal legislação para os Crimes Cibernéticos?; d) Quais são as principais ameaças?

A presente pesquisa visa mostrar a importância da existência da tipificação de crimes cometidos na internet, através de estudos que demonstrem os principais crimes cometidos neste meio.

As brechas nas leis relacionadas aos crimes cometidos no mundo virtual são bastante claras, por isto a grande importância deste estudo demonstrará que o direito apesar de acompanhar a evolução histórica da sociedade, encontra-se neste caso aquém do seu tempo, e por este motivo, este grande número de brechas utilizadas para se esquivar da punição por crimes cometidos na internet.

Assim, de modo a responder o problema supra levantados abro colocar que esta pesquisa tem o seguinte objetivo geral: Analisar alguns dos crimes digitais cometidos por meio de dispositivos informáticos (computador, tablet, celular etc.), mais especificamente sobre o Cyberbullying, racismo, pornografia, apologia ao crime e estelionato.

Outrossim, cabe registrar como escopos objetivos específicos os seguintes:

a) Pontuar os principais crimes ocorridos no mundo cibernético;

b) Analisar a legislação nacional e a internacional em relação aos crimes cibernéticos;

c) Traçar toda a evolução histórica dos crimes virtuais e analisar os seus conceitos;

d) Qualificar os crimes ocorridos no meio digital.

A presente pesquisa trata de um objeto frente aos principais autores que decorrem sobre a relação do Direito Penal com os crimes cibernéticos, utilizando o método dedutivo, discorrendo sobre o surgimento dos crimes virtuais, seus conceitos e os principais crimes que ocorrem no mundo virtual. Ressalta-se que o método dedutivo é uma operação lógica baseada em duas premissas que permitem chegar a uma conclusão.

O estudo se concluirá a partir da natureza qualitativa, levantamentos bibliográficos, revistas eletrônicas, artigos, entre outros recursos a serem explorados. Contudo, também será utilizado o método auxiliar comparativo, vez que serão analisadas as diferenças entre a legislação brasileira e as estrangeiras, comparando as linhas de raciocínios, levando o leitor a entender de uma forma melhor o assunto que será aprofundado.

2 DA INTERNET

2.1 História

Para entender a evolução até os crimes virtuais é necessário o conhecer a história da Internet. Originalmente a internet foi criada nos Estados Unidos, em 1969. Naquela época era chamada de *Arpanet*, tinha como função principal interligar os laboratórios de pesquisa. Neste mesmo ano um professor californiano enviou o primeiro e-mail da história (WERNER, 2001).

No ano de 1973 surgiu a primeira conexão da *Arpanet*, interligando a Inglaterra e a Noruega. No entanto, ela substituiu o seu protocolo de comutação de pacotes, o Protocolo de Controle de Rede para Protocolo de Controle de Transmissão, que é a linguagem básica de comunicação da rede mundial de computadores. Assim, este protocolo traz que a comunicação entre o servidor de internet e computador local só pode ser feita com base na configuração (WENDT; JORGE, 2013, 06).

Nesse contexto, durante a Década de 80 a ARPANET se expandiu pelos Estados Unidos, promovendo então a interligação entre as universidades, órgãos militares e governo. No ano de 1986 aconteceu a implementação da NSFNET - *pela National Science Fundation*-, e a *Arpanet* começou a se chamar Internet (WENDT; JORGE, 2013, 06).

Para que ocorresse um grande salto na utilização da internet surgiu o ‘’World Wide Web’’ houve um enriquecimento deste meio, pois o conteúdo de rede ficou mais atraente, tendo agora a possibilidade de incorporar imagens e sons. Com a implementação de um novo sistema de localização de arquivos cada informação passou a ter um único endereço que pode ser encontrada por qualquer usuário na internet (WENDT; JORGE, 2013, 05).

O site significados conceitua o termo World Wide Web como:

> Rede de alcance mundial, também conhecida como Web ou WWW. World Wide Web é um sistema de documentos em hipermídia que são interligados e executados na Internet. (Significados, 2019)

2.2 Conceito

A internet é um dos maiores e principais meios de comunicação, através dela é possível interligar todos os computadores do mundo através de várias redes interligadas. Nela é possível encontrar um número incontável de conteúdo (WENDT; JORGE, 2013, 09).

Michaelis conceitua Internet como:

> Rede remota internacional de ampla área geográfica, que proporciona transferência de arquivos e dados, juntamente com funções de correio eletrônico para milhões de usuários ao redor do mundo. (Michaelis, 2019).

A internet vem crescendo com o passar dos anos, sendo hoje a maior fonte global de informação, constituindo o maior fórum mundial de corporações e pessoas com interesse recíproco na comunicação entre virtualmente.

Com acesso à internet os usuários estão aptos ao uso de envio de mensagens, comunicação por voz ou vídeo, acesso a qualquer tipo de informação, independente da área desejada.

2.3 A Internet no Brasil

Apenas a partir de 1988 que o Brasil conseguiu fazer o primeiro contato, utilizando-se da tecnologia da rede, tempos depois o Brasil através de iniciativas públicas e privadas foi desenvolvendo sua infraestrutura para tornar possível o acesso à internet. (FERREIRA, 2017).

Em setembro de 1988 iniciaram-se os primeiros acessos à internet, por meio de iniciativa da Universidade Federal do Rio de Janeiro Paulo no LNCC (Laboratório Nacional de Computação Científica), e da comunidade acadêmica de São Paulo (FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo) (FERREIRA, 2017).

No Ano seguinte, foi criada a RNP (Rede Nacional de Pesquisa), destinada a construir uma infraestrutura para ligar as universidades brasileiras, ano este em que se instituiu o domínio ‘’.br’’ que serviu para identificar, através desta terminação, que se tratava de um site brasileiro (FERREIRA, 2017).

3 DO CRIME CIBERNÉTICO

Diante do seu alcance infindável, a internet com o seu avanço tecnológico e científico disponíveis na atualidade, fez com que a sociedade evoluísse de forma mais rápida. A internet vem conquistando milhares de usuários diariamente, atraídos pela diversidade que se pode encontrar com eficiência e praticidade (SCHMIDT, 2014).

No entanto, este grandioso número de usuários serviu também para atrair criminosos, os chamados cibercriminosos que viram no mundo virtual uma forma nova de se cometer crimes, a traídos pela chance do anonimato, a dificuldade de ser identificado, sendo assim acabaram tirando da internet o fim para que ela foi criada (SCHMIDT, 2014).

Neste sentido Rosa (2005) diz:

Com a expansão do uso de computadores e com a difusão da internet, tem-se notado, ultimamente, que o homem está se utilizando dessas facilidades para cometer atos ilícitos, potencializando, cada vez mais, esses abusos cometidos na rede. Como todos os recursos de disponibilidade do ser humano, a informática e a telecomunicação não são utilizadas apenas para agregar valor. O abuso (desvalor), cometido por via, ou com assistência dos meios eletrônicos não tem fronteiras. De um terminal eletrônico instalado num país se poderá manipular dados, cujos resultados fraudulentos poderão ser produzidos noutro terminal, situado em país diverso.

O crime cibernético é um termo utilizado para todo tipo de violações de leis criminais que tenham a conduta típica, antijurídica e culpável perpetrados através do conhecimento de tecnologia de computador. Crimes estes que podem ser cometidos de diversas maneiras, tais como disseminação de vírus, distribuição de conteúdo pornográficos, fraudes, violação de propriedade intelectual (DULLIUS, 2012).

3.1 Classificação dos Crimes Cibernéticos

3.1.1 Crimes Cibernéticos e Crimes Cibernéticos Exclusivamente Cibernético

Segundo os doutrinadores Higor Vinicius Nogueira Jorge (2013) e Emerson Wendt (2013), Os Crimes Cibernéticos subdividem-se em duas espécies, sendo elas: Crimes Cibernéticos abertos e Crimes exclusivamente cibernético.

Os crimes cibernéticos abertos são os que podem ser praticados de forma tradicional ou por intermédio de computadores, deste modo, o crime poderá ser cometido sem o uso do computador, como por exemplo o crime de ameaça e de Racismo (WENDT; JORGE, 2013, p. 19).

Já os Crimes exclusivamente cibernéticos são aqueles que somente podem ser praticados através do computador ou recursos tecnológicos capazes de ter acesso a internet. São exemplos desta a pornografia infantil por meio de sistema de informática e a invasão de computadores com a intenção de obter, adulterar ou excluir conteúdo sem a autorização do proprietário daquele dispositivo (WENDT; JORGE, 2013, p. 19).

3.1.2 Crimes Cibernéticos Puros, mistos e comuns

Segundo SCHMIDT (2014), os crimes cibernéticos puros são:

> Toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.

Neste sentido se verifica a ação dos hackers, que são pessoas com conhecimento elevado de informática que utiliza todo esse conhecimento para ato ilícito. O objetivo é atingir o sistema informático, podendo assim capturar as informações da vítima.

Já os crimes cibernéticos comuns são os crimes em que se utiliza da internet para a sua consumação. Vale ressaltar que são crimes que já tipificados pelo código penal brasileiro, porém a internet passa a ser outro meio de consumação deste crime. Um exemplo bastante comum é o crime de racismo, que já era criminalizado, mudando a forma, mas sem perder a essência do crime (SCHMIDT, 2014).

3.1.3 Crimes Cibernéticos Próprios e Impróprios

Os crimes cibernéticos classificados como próprios são aqueles praticados por meio do sistema informático, ou seja, sem a tecnologia da informática não existirá o crime.

Exemplo para esta classificação são as condutas praticadas por hackers que por meio do computador invade o dispositivo informático de outrem com a intenção de obter dados da vítima, adulterar informações ou até mesmo inserir informações que não pertencem a pessoa naquele dispositivo informático (SCHMIDT, 2014).

Já os crimes cibernéticos impróprios são aqueles que podem ser praticados de diversas formas, não somente através de dispositivos informáticos, mas que utiliza a internet como um novo meio de execução para este crime.

Um exemplo seria o estelionato, crime este já tipificado pelo código penal, porém com o provimento da internet surgiu uma nova forma de se conseguir praticar este tipo de crime.

3.2 Principais Ameaças

3.2.1 Engenharia Social

É o termo utilizado para descrever um conjunto de técnicas cujo a função é ludibriar pessoas, de modo que a partir da confiança ela forneça os seus dados pessoais que mais tarde será utilizado pelos criminosos para obter o acesso não autorizado aos dispositivos da vítima.

Para ganhar a confiança das vítimas os criminosos muito das vezes utilizam de artimanhas como se passar por funcionário de instituições como bancos, lojas e sites. Outro aspecto utilizado é chamar atenção da vítima através de assuntos que estão em alta na mídia.

Neste sentido o Centro de Estudos, respostas e tratamento de incidentes de Seguranças no Brasil (CERT.br) apresenta alguns exemplos desses ataques:

> Exemplo 1: você recebe uma mensagem e-mail, onde o remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de Internet Banking está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso a conta bancária e enviá-la para o atacante.
>
> Exemplo 2: você recebe uma mensagem de e-mail, dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um site da Internet, para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.
>
> Exemplo 3: algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a Internet está apresentando algum problema e, então, pede sua senha para corrigi-lo. Caso você entregue sua senha, este suposto técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso à Internet e, portanto, relacionando tais atividades ao seu nome.

Uma característica da engenharia social é quando utilizada no âmbito criminal. Em alguns casos o policial se infiltra em organizações criminosa utilizando de técnicas de persuasão da engenharia social para obter informações que o criminalizem.

3.2.2 Vírus Comuns

O Vírus de Boot surgiu na década de 80 e é conhecido por ser o percursor de todos os outros vírus existentes. Sua principal característica é se instalar no setor de inicialização do computador, podendo assim causar transtornos ao computador do usuário. A infecção deste

vírus geralmente ocorre quando um usuário ao colocar um pendrive em um computador infectado acaba por colher o vírus, sendo assim, a cada dispositivo em que utilizar o pendrive estará repassando o vírus sem que o mesmo saiba (CERT.br, 2012).

Além do vírus de boot, existe o Vírus time bomb, sendo este uma forma especial do vírus onde ele será ativado em um momento programado por seu programador. É como se fosse uma bomba relógio, pois o usuário terá acesso livre ao seu dispositivo até que o vírus ``exploda``, fazendo com que a vítima sofra com seus efeitos (WENDT; JORGE, 2013, 20).

3.2.3 *Botnet*

Este é um dos principais vírus, e também, um dos mais perigosos. Através deste código malicioso o programador terá acesso remoto ao computador da vítima, podendo controlá-lo a qualquer momento. É bastante utilizado para atacar outros computadores, geralmente a vítima não percebe que o seu computador está infectado, pois este vírus não traz outros problemas ao seu computador, como por exemplo a lentidão.

Positivamente o botnet é utilizado de forma reversa, servindo para capturar informações sobre os cibercriminosos que o utilizam.

3.2.4 Defacement

Este é um tipo de ataque utilizado para alterar, danificar páginas de sites ou redes sociais. Conhecido popularmente como a pichação virtual, vem sido cada vez mais utilizado por criminosos para propagar ideias e convicções políticas, religiosas, etc (CERT.br, 2012).

3.2.5 Spyware

O *Spyware*, conhecido no Brasil como programa espião, foi projetado justamente para espionar o computador em que se é instalado. Ao ser infectado por um *spyware* o computador da vítima passa a enviar as informações do usuário para o seu programador (CERT.br, 2012).

Sua utilização possui duas formas, sendo de forma legítima e de forma maliciosa, tudo isso dependerá do modo em que for utilizada e instalada.

Acerca disso, a Cartilha de segurança conceitua:

> Legítimo: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.
>
> Malicioso: quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes a navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns dos programas *spyware* são:

a) *Keylogger*

Através do *keylogger* o seu programador poderá obter de sua vítima tudo o que ele digitar através do teclado do computador. Ou seja, um usuário que possuir o *keylogger* instalado em seu computador estará sujeito a ter suas informações pessoais, seus dados bancários ou qualquer informação digitada vazada (MACHADO, 2012).

b) *Screenlogger*

É uma forma simular ao *keylogger*, porém existe uma função peculiar que é a de armazenar a foto da tela. Ele é capaz de capturar a tela no momento em que o mouse é clicado, desta forma ele acaba burlando um método de segurança muito utilizado por bancos, por exemplo, que se utilizam de mecanismo sob cliques na hora em que o usuário digita a senha em algum computador (CERT.br, 2012).

3.2.6 Cavalo de Troia

Denominado originalmente por trojan, o cavalo de troia é utilizado por cibercriminosos para ter acesso de forma remota ao computador da vítima, com o fim de obter informações pessoais da vítima (CERT.br, 2012)

Sua contaminação se dá por envio de um arquivo que ao ser executado o computador da vítima passa a ser dominado pelo cibercriminoso. Ele pode ser adquirido em sites da internet que utilizam de propagandas como meio de atrair o clique dos usuários, ao clicar você acaba baixando um arquivo que poderá contaminar alguns de seus aplicativos sem deixar que eles desempenhem as suas funções originais, tornando-se assim um problema silencioso (CERT.br, 2012).

Neste sentido a Cartilha do CERT, diz:

> Cavalo de troia é um programa normalmente recebido como um “presente” (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.) que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário (CERT.br, 2012)

3.2.7 *Hijack*

Através de brechas de segurança este programa invadem o computador do usuário sem que a pessoa perceba. Com isto, o criminoso acaba por conseguindo modificar o navegador da vítima, forçando o aparecimento de propagandas, páginas aleatórias abrindo, tudo isto contra a vontade de quem utiliza o computador (DUARTE, 2015).

3.3 Provas Digitais

Apesar de cometido em meio virtual, onde por muito tempo foi conhecido como "terra sem lei", tudo o que se pratica neste meio também deixa rastros, sendo assim, há a possibilidade de se descobrir tudo o que ocorrer. Toda atividade realizada através de um dispositivo informático poderá ser recuperada em um espaço de tempo, mesmo que tenha sido apagada pelo cibercriminoso.

Para que a perícia forense analise as provas é necessário que as provas captadas no meio digitais sejam admissíveis, ou seja, como qualquer prova a aquisição dela deverá ser lícita. Além disso, será preciso preservar o princípio da ciência computacional que tem como fim garantir a autenticidade e a integridade do que está sendo recolhido (DOMINGOS, 2018, p. 245)

Todas estas características serão analisadas e verificadas pela perícia forense, que dirá sobre a veracidade da mesma. Vale ressaltar que a perícia forense deve acompanhar as ações de busca e apreensão para que a coleta das provas digitais seja feita com responsabilidade e passe credibilidade perante o juiz (DOMINGOS, 2018, p. 245)

Embora deixem rastros e possibilidade de ser recuperada, algumas das provas digitais também são armazenadas em ambiente internacional, através dos diversos provedores existentes. A lei brasileira obriga os servidores a fornecerem as informações devidas, porém no âmbito internacional somente se dará através de acordos entre os países e, como não existem acordos, acaba que na pratica várias empresas proprietárias de provedores se negam a cumprir as determinações judiciais brasileiras (DOMINGOS, 2018, p. 246)

Apesar disso, existem algumas medidas de cooperação entre o Brasil e outros países para a obtenção de provas digitais, sendo elas: a carta rogatória e o auxílio mútuo em matéria penal. No Brasil a competência de executar essa cooperação é da Polícia Federal, na condição de polícia judiciária da União (DOMINGOS, p. 247)

4 OS PRINCIPAIS CRIMES CIBERNÉTICOS

4.1 Racismo

O racismo na internet é uma extensão daquilo que já acontece e sempre aconteceu, apenas migrou para o meio digital. A praticidade que o meio eletrônico oferece acaba levando as pessoas a cometer abuso de liberdade e expressão na ilusão de que o computador não irá revelar a sua identidade. Acontece que o mundo digital não é uma terra sem lei e toda a sua atitude cometida ali deixa rastro, rastro este que poderá ser rastreado a partir do número de IP que cada computador possui, com isto será possível identificar o local de onde foi praticado o crime de racismo virtual e possivelmente quem o cometeu.

Sobre isso, Ferreira (2018, p.145) diz:

> De acordo com a lei 12.965, conhecida como Marco Civil da Internet, o endereço de protocolo de internet (Endereço de IP) é atribuído a um terminal de uma rede para permitir a identificação, definido segundo parâmetros internacionais. Todo computador que acessa a internet possui um identificador, conhecido como endereço de IP.

Assim, com o endereço de IP do criminoso e a data e hora de conexão, poderá ser encontrado o autor do crime praticado na internet. Para isso será necessário que as autoridades entrem em contato com a empresa provedora da internet para que elas forneçam dados que dispõem, e, a partir destes dados iniciarem todo o trâmite para a descoberta do local e quem cometeu o autor do crime (FERREIRA, 2018, p.145)

A constituição Federal em seu artigo 5º, inciso XLII traz que " a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei". No entanto, os crimes de racismo estão previstos na Lei nº 7.716/1989 e o crime de injúria racial, no artigo 140 parágrafo 3º, do Código Penal, conforme pode ser visto:

> **Art. 140** - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> (...)
> **§ 3o** Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:

Acerca das condutas praticadas através da internet a lei nº 7.716/89 traz em seu artigo 20 parágrafo 2º:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
> Pena: reclusão de um a três anos e multa.
> (...)

> § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza: Pena: reclusão de dois a cinco anos e multa.

Para que haja punição ao autor de mensagens racista na internet é preciso que se caracterize o dolo, sendo assim, é preciso que a vítima sofra algum tipo de ofensa em relação a sua raça, cor, sexo, orientação sexual ou por qualquer motivo que indique intolerância ou ódio (FERREIRA, 2018, p.146).

Quem pratica este tipo de crime normalmente utiliza do argumento de que seu comentário não passou de uma brincadeira, porém apenas isso não afastará a sua culpa, o caso deve ser analisado (FERREIRA, 2018, p.146).

Assim, Fábio Medina e Jairo Gilberto Alertam sobre:

> A consciência e a vontade de produzir atos discriminatórios e preconceituoso são incompatíveis com o formado das "brincadeiras". Inadmissível, assim, a publicação de manifestações jocosas, em qualquer de suas formas, versando discriminações e preconceitos vedados na lei penal. Por conseguinte, as charges, o sarcasmo, a ironia, piadas, o deboche, configuram instrumentos idôneos à pratica, ao induzimento e instigação do ato discriminatório e preconceituoso proibido. (OSÓRIO; SCHAFER, 1995, p. 329)

Mesmo que as mensagens de cunho racista sejam apagadas não o exime de um possível processo, pois estas mensagens poderão ser replicadas nas redes sociais por outros usuários (FERREIRA, 2018, p.146).

4.1.1 Caso Maju Coutinho

Um caso bastante repercutido relacionado ao racismo na Internet foi o que ocorreu com a jornalista, a época apresentadora da previsão do tempo do Jornal Nacional da TV Globo. Através de uma publicação via *facebook* na página do Jornal Nacional, da TV Globo, os criminosos disseminaram vários comentários de ódio contra a apresentadora, caracterizando claramente um caso de injúria racial.

Os denunciados, de acordo com os fatos narrados em denúncia feita pelo Ministério Público, possuíam um grupo de ataques voltado a derrubar conta de outros usuários em redes sociais.

Com o intuito de injuriar a apresentadora da TV Globo, Maria Júlia dos Santos Coutinho, a popularmente conhecida como Maju, os criminosos a atacaram através da página do Facebook do Jornal Nacional com os seguintes comentários:

> “A mão do xicote chega a tremer md vê esssa tua cara!!! Negra maldita !!!”
> “Fim de incêndio”.
> “Macaca.”

> “Esqueceram de sequestrar ela (sic) pra voltar a ser escrava.”
> “Meu cachorro foi dar uma ‘cagada’ dentro de um baude (sic) para contribuir para a fome desta mulher!”
> “Pegaram essa mendiga na rua? Essa negra Tizil (sic)?”
> “Quem deixou essa preta sair da gaiola?”
> “Vou levar você para o Nordeste e mostrar para aquele povo que existe coisa mais feia que a fome.”
> “‘Senhoras e senhores nós estamos sofrendo dificuldades técnicas’ – Deve ser esta negra levando chicotada dos cabos da câmera.”
> “Sabonete de Mecânico”
> “Volta pra senzala, resto de placenta carbonizada”
> “Sai café da sua teta”
> “Escrava”
> “Munição de churrasqueira”
> “Tapete de mecânico”
> “Gorila”
> “Papo com ‘vc’ é no xicote (sic) preta maldita!!!

4.2 CyberBullying

O conceito de Bullying está em seu art 1º da Lei 13.185, parágrafo primeiro:

> § 1º No contexto e para os fins desta Lei, considera-se intimidação sistemática (bullying) todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas (Brasil, 2015).

Já o Cyberbullying trás as mesmas ofensas, porém no meio virtual, através de dispositivos informáticos. A potencialidade lesiva dessa conduta é muito maior, visto que se for comparar com uma criança xingando a outra em um colégio toma uma repercussão, já quando isso é compartilhado na internet e fica disponível 24 horas por dia a repercussão é muito maior.

O cyberbullying é uma forma gratuita de violência que fere a dignidade humana e outros valores do indivíduo, como os danos emocionais. O Cyberbullying ocorre mais em crianças e adolescentes e isto poderá afetá-los pelo resto de suas vidas.

A pedagoga e Historiadora Cleo Fante traz um panorama do conceito e principais características do Cyberbullying:

> O bullying é uma forma de violência que ocorre na relação entre pares, sendo sua incidência maior entre os estudantes, no espaço escolar. E caracterizado pela intencionalidade e continuidade das ações agressivas contra a mesma vítima, sem motivos evidentes, resultando danos e sofrimentos e dentro de uma relação desigual de poder, o que possibilita a vitimação. É uma forma de violência gratuita em que a vítima é exposta repetidamente a uma série de abusos, por meio de constrangimento, ameaça,

> intimidação, ridicularização, calúnia, difamação, discriminação, exclusão, dentre outras formas, com o intuito de humilhar, menosprezar, inferiorizar, dominar. Pode ocorrer em diversos espaços da escola ou fora dela, como também em ambientes virtuais, denominado bullying virtual ou cyberbullying, onde os recursos da tecnologia de informação e comunicação são utilizados no assédio (RODER; SILVA, 2018, apud FANTE, p.29).

Dentro das modalidades do Cyberbullying temos as publicações ofensivas em redes sociais, envios de e-mails com ofensas para a vítima, fóruns de discussão. O cyberbullying poderá ser praticado por vários motivos, sendo os mais comuns em relação as diferenças físicas das pessoas, a exemplo de pessoas com obesidade, mas também em casos referentes a sua religião, a sua preferência sexual (WENDT; JORGE, 2013, p.102).

As agressões perpetuadas na internet através dos dispositivos móveis deverão ser analisadas e poderão caracterizar crimes como de calúnia, injúria, difamação, constrangimento ilegal, ameaça e etc (RODER; SILVA, 2018, p.38).

Os atos de cyberbullying também poderão constituir atos ilícitos cíveis, neste caso os responsáveis poderão ser responsabilizados.

Sobre isto, versa o Código Civil Brasileiro em seus artigos:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. (BRASIL, 2002).

Cabe ressaltar que, sendo o crime praticado por menores, os pais podem ser obrigados a reparar o dano causado a vítima, assim como os estabelecimentos pelos atos praticados em seu interior.

Estando isto disposto nos artigos:

> Art. 932. São também responsáveis pela reparação civil:
> I - os pais, pelos filhos menores que estiverem sob sua autoridade e em sua companhia;
> II - o tutor e o curador, pelos pupilos e curatelados, que se acharem nas mesmas condições;
> III - o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele;
> IV - os donos de hotéis, hospedarias, casas ou estabelecimentos onde se albergue por dinheiro, mesmo para fins de educação, pelos seus hóspedes, moradores e educandos;

> V - os que gratuitamente houverem participado nos produtos do crime, até a concorrente quantia.
> Art. 933. As pessoas indicadas nos incisos I a V do artigo antecedente, ainda que não haja culpa de sua parte, responderão pelos atos praticados pelos terceiros ali referidos (BRASIL, 2002)

4.3 Pedofilia e Pornografia Infantojuvenil

A internet facilitou a vida de muita gente, mas trouxe também desafios que a sociedade ainda está aprendendo a lidar. A relação da criança com o mundo virtual, por exemplo é um ponto a se ter muito cuidado. Porém, a responsabilidade do monitoramento na Internet cabe aos pais.

Com a possibilidade de se criar perfis falsos virtuais em diversos sites e aplicativos de troca de mensagens e vídeos, os pedófilos passaram a utilizar da Internet para buscar as suas vítimas. Estes pedófilos entram na Internet com a intenção de encontrar crianças e adolescentes e obter delas fotos e vídeos íntimos e possivelmente atraí-los para o mundo real também.

O Estatuto da Criança e do Adolescente prevê em seus artigos 241-A e 241-B a criminalização da publicação, troca ou divulgação de vídeo ou foto com conteúdo em sites e blogs, onde poderá ser visualizado por outras pessoas. Conforme:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. § 1 o Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2 o As condutas tipificadas nos incisos I e II do § 1 o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo;
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
> Pena - reclusão, de 1 (um) a 4 (quatro) anos, e multa (BRASIL, 2008).

Sobre isso, Silva (2009, p. 305) comenta:

> O crime de divulgar cena de sexo explícito ou pornografia infanto juvenil estará consumado no instante e no local a partir do qual é permitido o acesso ao público que ‘’navega’’ na internet, ou seja, no endereço do responsável pelo site (endereço real, lugar da publicação).

Empresas como o google que hospeda esse tipo de imagem e vídeo só serão responsabilizadas se após a denúncia ou notificação judicial não fizer a retirada do conteúdo publicado em seu domínio. A simples existência de imagens ou vídeos com pornografia não infantil é o necessário para que seja caracterizado o delito, não importando que o material tenha sido acessado por outros usuários da internet, mas sendo essencial a posse de arquivos com determinado conteúdo.

4.4 Estelionato

Estelionato é um dos principais crimes contra o patrimônio do ordenamento brasileiro. Com o surgimento da internet o número de pessoas que tentam obter vantagens através do estelionato cresceu.

O código penal em seu artigo 171 assevera que:

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Através da internet o estelionatário utiliza de várias condutas, tendo como objetivo obter vantagem ilícita. Um dos principais meios de consumação do crime é quando o cibercriminoso utilizando de seus conhecimentos tecnológicos cria sites parecidos com o de bancos e envia um e-mail falso para os usuários. Quando o usuário abre aquele e-mail é redirecionado para a página falsa do criminoso, acreditando estar acessando uma página oficial a vítima insere ali os seus dados pessoas. Com os dados das vítimas, geralmente dados de cartões de créditos, os estelionatários fazem diversas compras pela internet (NAUATA, 2018).

O código penal brasileiro não menciona o estelionato virtual em seu artigo, ou seja, o artigo 171 do código penal apenas fala sobre o estelionato cometido pelos estelionatários nas vias reais, não mencionando o uso de computadores e internet para consumir o delito. Porém, é nítido que o crime de estelionato comum e o praticado na internet possuem apenas a diferença do modo em que ele é executado, sendo um praticado no mundo físico e o outro no mundo virtual com o uso da internet e dispositivo informático (NAUTA, 2018).

Entretanto, a corrente majoritária o resultado do crime de estelionato no mundo virtual se iguala ao cometido no mundo físico, pois o resultado causado à vítima será o mesmo.

Neste sentido Nucci (2017, p. 626) diz:

> Há várias formas de cometimento de estelionato, prevendo-se a genérica no caput. Obter vantagem (benefício, ganho ou lucro) indevida induzindo ou mantendo alguém em erro. Significa conseguir um benefício ou um lucro ilícito em razão do engano provocado na vítima. Esta colabora com o agente sem perceber que está se despojando de seus pertences. Induzir quer dizer incutir ou persuadir e manter significa fazer permanecer ou conservar. Portanto, a obtenção da vantagem indevida deve-se ao fato de o agente conduzir o ofendido ao engano ou quando deixa que a vítima permaneça na situação de erro na qual se envolveu sozinha. É possível, pois, que o autor do estelionato provoque a situação de engano ou apenas dela se aproveite. De qualquer modo, comete a conduta proibida. Os métodos para colocar alguém em erro são fornecidos pelo tipo penal: artifício (astúcia ou esperteza), ardil (também é artifício ou esperteza, embora na forma de armadilha, cilada ou estratagema) ou outro meio fraudulento (trata-se de interpretação analógica, ou seja, após ter mencionado duas modalidades de meios enganosos, o tipo penal faz referência a qualquer outro semelhante ao artifício e ao ardil, que possa, igualmente, ludibriar a vítima). A utilização de mecanismos grosseiros de engodo não configura o crime, pois é exigível que o artifício, ardil ou outro meio fraudulento seja apto a ludibriar alguém. A pena é de reclusão, de um a cinco anos, e multa (NUCCI, 2017, p. 626).

Cabe ressaltar que, o crime de estelionato virtual não será apenas praticado por quem possuir conhecimento específico em informática. A base deste crime está na confiança que o criminoso consegue sob a vítima, portanto, mesmo que não utilize de artifícios tecnológicos uma pessoa poderá conquistar a confiança da mesma e enganá-la para obter seus dados de forma ilícita.

4.5 Crimes Contra a Honra

As redes sociais ampliam as formas de interação, através dela as pessoas podem fazer comentários, compartilhar histórias, opiniões, fotos, vídeos e trocar informações. Apesar de encurtar tempo e distância facilitando a comunicação, a cautela do que se posta deve ser constante.

Muitos utilizam as redes sociais para praticar de crimes contra honra. Qualquer tipo de manifestação na internet que prejudique a imagem de outra pessoa e essa pessoa se sinta ofendida de alguma maneira é passivo de crime. Dependendo do conteúdo postado sobre outra pessoa poderá ser configurado como calúnia, injúria ou difamação.

O crime contra a honra praticado no ambiente virtual poderá ser julgado tanto em âmbito penal como em âmbito civil. Tudo dependerá da gravidade do dano causado à vítima.

A previsão da honra está prevista na constituição federal, conforme pode ser visto:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988).

Acerca disso, Uadi Lammêgo Bulo (2001, p. 105) diz:

Tutelando a honra, o constituinte de 1988 defende muito mais o interesse social do que o interesse individual, *uti singuli*, porque não está, apenas, evitando vinditas e afrontes à imagem física do indivíduo. Muito mais do que isso, está evitando que se frustre o justo empenho da pessoa física em merecer boa reputação pelo seu comportamento zeloso, voltado ao cumprimento de deveres socialmente úteis.

4.5.1 Calúnia

O crime de calúnia se dá ao atribuir a outra pessoa falsamente um crime que não cometeu. Tendo uma terceira pessoa ciência da notícia falsa, estará aí configurado o crime. Neste ponto nota-se que não será configurado o crime se apenas a pessoa tiver a honra ferida. Neste crime também estará caracterizado quem espalhar a calúnia (SARAIVA, 2015).

> O crime de calúnia está previsto no art. 138 do CP:
> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos.
> Exceção da verdade
> § 3º - Admite-se a prova da verdade, salvo:
> I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
> II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
> III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível (BRASIL, 1949).

A respeito do crime de calúnia, Damásio Jesus diz:

Constitui crime formal, porque a definição legal descreve o comportamento e o resultado visado pelo sujeito, mas não exige sua produção para que exista crime, não é necessário que o sujeito consiga obter o resultado visado, que é o dano a honra objetiva do agente (JESUS, 2007, p. 219).

4.5.2 Injúria

O crime de injúria consiste no ato de afronta, ofensa, insulto contra a honra subjetiva, neste ponto o sentimento da vítima referente aos seus atributos é o que irá pesar. Este crime, basicamente, afeta a autoestima da vítima (SARAIVA, 2015).

Acerca disso, Greco (2015, p. 435) diz:

> De todas as infrações penais tipificadas no Código Penal que visam proteger a honra, a injúria, na sua modalidade fundamental, é a considerada menos grave. Entretanto, por mais paradoxal que possa parecer, a injúria se transforma na mais grave infração Penal contra a honra quando consiste na utilização de elementos referente a raça, cor, etnia, religião, origem ou condição de pessoa idosa ou portadora de deficiência, sendo denominado aqui de injúria preconceituosa.

O crime de Injúria está prevista no artigo 140 do Código Penal, que diz:

> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - no caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
> § 3o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:
> Pena - reclusão de um a três anos e multa (BRASIL, 1940).

4.5.3 Difamação

A difamação é um crime previsto no artigo 139 do Código Penal que diz “Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa”.

O crime de difamação irá caracterizar-se quando alguém imputa a outrem algo que lhe ofenda, que manche a sua honra perante a sociedade. No crime de difamação não é necessário que a ofensa destinada à vítima seja definida como crime, também não importa se é verdade ou não, sendo necessário apenas que a vítima se sinta ofendida (SARAIVA, 2015).

Um exemplo bastante comum de difamação ocorrido na internet é quando uma pessoa ao ver outra usufruindo de luxo, comenta nas redes sociais dizendo que a vítima está se prostituindo para poder manter a vida luxuosa.

Acerca da difamação Damásio comenta:

> Não se cuida de atribuir à pessoa jurídica a prática de um crime ou uma qualidade injuriosa. É certo que a definição legal do art. 139 do Código penal fala em alguém; mas alguém significa alguma pessoa, em face do que se pode entender que o tipo cuida de toda espécie de pessoa, seja física ou jurídica” (JESUS, 2007, p. 179).

4.6 Revenge Porn

O *Revenge Porn*, chamado de Pornografia de Vingança no Brasil, é um novo comportamento que toma a sociedade, fruto do progresso da informática e das relações sociais virtuais. O *Revenge Porn* é uma forma de humilhação, através de vingança contra quem, em um momento de confiança, envia foto ou vídeo íntimo e ao fim do relacionamento por motivo de vingança a pessoa divulga este conteúdo (DIEZ, 2016).

Neste sentido Diez (2016) comenta:

> Na era digital, os compartilhamentos ocorrem sem nenhum critério por parte dos usuários, ainda que sejam de cunho nitidamente íntimo e de pessoas conhecidas. Há a sensação do anonimato e da impunidade, como se fosse uma terra sem lei.

Quando se espalha as fotos e vídeos íntimos o criminoso poderá atingir a honra subjetiva, a intimidade, autoestima, a dignidade ou decoro da vítima. A dificuldade para que se exclua do mundo virtual acabara por angustiar todas essas vítimas, aumentando o número de suicídios após terem suas fotos ou vídeos divulgados.

Normalmente quando se há uma infração de conteúdo a pessoa vai ao judiciário para que ele decida se aquilo deve permanecer ou não, isso garante mais liberdade de expressão, pois se cada um tirasse o que não gosta poderia causar uma censura indireta, então o marco civil privilegiou o poder judiciário para como decisor se há um crime envolvido ou não.

Existem dois casos em qual o judiciário não precisa ser consultado toda vez ou pelo menos apenas em segunda instancia. Sendo eles, direito autoral e *porn revenge*, a chamada Pornografia de Vingança. Na pornografia de vingança a vítima ou o terceiro poderá notificar o provedor que disponibiliza o conteúdo que lhe ofende para que ele seja removido imediatamente.

Acerca disso, o Marco Civil afirma em seu artigo:

> Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo (BRASIL, 2015).

Acerca do assunto, o artigo 218-C do código penal discorre sobre a transmissão, venda ou troca de fotografia ou vídeo de nudez ou pornografia íntima, com uma causa de aumento pertinente ao tema do *Revenge Porn.*

> **Art. 218**-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: (Incluído pela Lei nº 13.718, de 2018).
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave. (Incluído pela Lei nº 13.718, de 2018).

O parágrafo primeiro do artigo 218-C discorre acerca o aumento de pena referente ao crime praticado por agente que mantém ou tenha mantido relação de afeto com a vítima e utiliza do crime como forma de vingança, e com base no estudo exposto no texto acima, caracteriza-se então o *Revenge Porn.*

> **§ 1º** A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação. (Incluído pela Lei nº 13.718, de 2018).
> Exclusão de ilicitude (Incluído pela Lei nº 13.718, de 2018).

Quando o agente que praticar este tipo de conduta em publicações de natureza jornalísticas, científicas, cultural ou acadêmica e com a autorização da outra parte, em caso desta ser maior de idade, não haverá crime, conforme descrito no Artigo 218-C, parágrafo segundo. Conforme pode ser visualizado abaixo:

> **§ 2º** Não há crime quando o agente pratica as condutas descritas no caput deste artigo em publicação de natureza jornalística, científica, cultural ou acadêmica com a adoção de recurso que impossibilite a identificação da vítima, ressalvada sua prévia autorização, caso seja maior de 18 (dezoito) anos. (Incluído pela Lei nº 13.718, de 2018).

5 LEGISLAÇÕES

5.1 Lei Carolina Dieckmann

No ano de 2012 aconteceu um fato notório na vida da atriz Carolina Dieckmann, famosa por diversos papeis em séries e novelas da maior rede de televisão brasileira, a rede Globo. A atriz se viu comentada em todas as redes sociais não pelo seu trabalho, mas por causa do vazamento de suas fotos íntimas, caso este que já havia acontecido com milhares de pessoas e não havia tipificação para este crime.

Acerca da repercussão do caso Romoni comenta:

> Em cinco dias, as fotos vazadas na internet em que a atriz Carolina Dieckmann aparece nua tiveram pelo menos 8 milhões de acessos únicos. Os números podem ser maiores. A pesquisa foi feita só na web, sem contar compartilhadas por e-mail e serviços P2P, como o BitTorrent. Também ficaram de fora mídias físicas, como CDs e DVDs, pen drives e HDs externos para os quais as imagens podem ter sido copiadas (ROMONI, Bruno, 2012).

O fato ocorreu devido terem enviado um e-mail com um programa espião instalado ao ser aberto. Com o vírus espião instalado os hackers tiveram acesso a tudo o que Carolina Dieckmann digitava, sendo assim, conseguiu invadir todas as suas redes sociais. Todo este fato ocorreu devido a atriz juntamente com seu marido, ambos em seu momento íntimo, tiraram fotos e trocaram via e-mail, e com o acesso ao e-mail, os hackers puderam copiar todo o conteúdo em questão (G1, 2012).

Sendo assim, os criminosos com o material recolhido do computador da atriz global Carolina Dieckmann decidiram então usar este fato para chantagear o casal de divulgar na rede mundial de computadores as imagens de nudez da atriz, chegando a enviar parte das fotos para a empresária da atriz e a fazer telefonemas para a casa de Carolina pedindo o valor de dez mil reais para que não a divulgasse na internet. O que não imaginavam é que mesmo com as ameaças a atriz decidiu procurar a autoridade policias para denunciar o crime que estava sofrendo (G1, 2012).

Diante de toda a visibilidade do crime e pelo fato da atriz ter abraçado a causa, um projeto de lei que tramitava no congresso fez com que este projeto adiantasse, tornando-se a lei de número 12.737/2012, e como de costume brasileiro de dar nome a toda e qualquer lei, foi denominada de Lei Carolina Dieckmann (G1, 2012; G1 2013).

> O bem jurídico tutelado é a liberdade individual do usuário do dispositivo informático, haja vista, cumpre dizer, que o tipo está inserido no capítulo do Código Penal que dispõe sobre os crimes contra a liberdade individual. Além disso, pode-se afirmar também que o tipo busca tutelar a privacidade do

> indivíduo, na qual estão inseridas a intimidade e a vida privada (NUCLEO DE CRIMES/MP-SP, 2017).

Esta lei alterou o código penal, passando a tipificar os crimes cibernéticos puros ou propriamente ditos, ou seja, aqueles cujo fim é o próprio sistema informático, bem como seus dados e informações, o crime contra o computador. A intenção da lei é tutelar a privacidade de todos os usuários da grande rede virtual (NUCLEO DE CRIMES/MP-SP, 2017).

A nova lei 12.737/2012 inseriu os Artigos 154-A e 154-B sendo que o primeiro artigo descrito abaixo:

> 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 (BRASIL, 2012)

O artigo demonstra que o crime é praticado contra o dispositivo informático, que só há crime se o computador da vítima tiver dispositivo de segurança, não havendo segurança o fato será atípico. Ou seja, o simples fato de deixar o seu computador sem um antivírus ou até mesmo sem senha e este for utilizado por outra pessoa com intenção de cometer crime, não haverá tipificação na lei, pois de acordo com o artigo é necessário que haja violação do mecanismo de segurança para que se consuma o crime informático.

Acerca da classificação Nucci (2014) é sucinto:

> Trata-se de crime comum (pode ser cometido por qualquer pessoa); formal(delito que não exige resultado naturalístico, consistente na efetiva lesão à intimidade ou vida privada da vítima, embora possa ocorrer); de forma livre (pode ser cometido por qualquer meio eleito pelo agente); comissivo (as condutas implicam ações); instantâneo (o resultado se dá de maneira determinada na linha do tempo), podendo assumir a forma de instantâneo de efeitos permanentes, quando a invasão ou a instalação de vulnerabilidade perpetua-se no tempo, como rastro da conduta; uni subjetivo (pode ser cometido por uma só pessoa); plurissubsistente (cometido por vários atos); admite tentativa.

No momento da invasão do dispositivo dá-se a consumação do crime, mesmo que não haja destruição, adulteração de dados, ou até mesmo a obtenção de vantagem ilícita, visto que a tentativa é admitida. Qualquer pessoa poderá ser o sujeito ativo deste crime, sendo o passivo o usuário que tiver o seu dispositivo invadido (NUCLEO DE CRIMES/MP-SP, 2017)

Em caso de falha na proteção pelo usuário o autor Afonso de Oliva orienta:

> A partir do momento que a pessoa também não se protege, ela fica descoberta da lei federal. Caso haja algum tipo de roubo de informações pessoais, a orientação é abrir um boletim de ocorrência na Delegacia especializada e buscar ajuda com algum profissional. ” (OLIVA, 2013).

A lei 12.737/2012 também acrescentou o artigo Art. 154-**B**, que afirma que o artigo 154-A trata a ação pública condicionada, ou seja, é necessário que por vontade própria a vítima denuncie o crime. O Art 154-B traz uma exceção que será quando o crime informático for praticado contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos, nestes casos não haverá a necessidade de representação, pois a ação será pública e incondicionada.

5.1.1 Penalidade Imposta

Como forma de castigo imposto pela lei será a Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. Trata-se de uma pena básica, conduta de médio potencial ofensivo. Somente será aplicada a pena de detenção mediante o trânsito em julgado da sentença condenatória pela prática do delito.

De acordo com o art. 44 do Código Penal, **§ 2º**: [...]se superior a um ano, a pena privativa de liberdade pode ser substituída por uma pena restritiva de direitos e multa ou por duas restritivas de direitos[...].

O primeiro parágrafo do artigo 154-A, prescreve:

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput (BRASIL, 2012).

Este parágrafo busca explicar que a pena do artigo 154-A também servirá para o usuário que apenas criar, distribuir ou difundir dispositivo ou programa de computador de forma ilícita. Ou seja, desta forma, o crime ocorrerá também por quem produzir o material ilícito utilizado. Um exemplo disso é o vírus de um e-mail que mesmo sendo enviado por outra pessoa, aquele que foi o criador deste vírus elaborado para obtenção de dados de quem abri-lo será punido da mesma forma.

5.1.2 Aumento de pena

O artigo 154-A traz quatro elementos de caso de aumento de pena, ou seja, casos em que a pena será agravada devido ao delito cometido. Sendo os casos:

> **§ 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) Vigência
> **§ 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) Vigência 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
> **§ 4º** Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. (Incluído pela Lei nº 12.737, de 2012) Vigência
> **§ 5º** Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) Vigência
> **I** - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência
> **II** - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência
> **III** - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012) Vigência
> **IV** - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 2012).

5.2 Convenção de Budapeste

Trata-se do principal tratado internacional sobre Crimes Cibernéticos. Criado no ano de 2001 pelo conselho europeu, entrando em vigor a partir de 2004 com a ratificação de países como Estados Unidos, Canada, Austrália e Japão (DOMINGOS, 2018, p. 246).

A Convenção de Budapeste trouxe como principal objetivo a tipificação de crimes cometidos na internet, bem como a cooperação entre os países participantes, e que estes crimes sejam devidamente investigados e punidos.

Segundo Fernandes (2013, p. 145), a Convenção de Budapeste veio tipificar as seguintes condutas:

> 1) Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos:
> a) acesso doloso e ilegal a um sistema de informática;
> b) interceptação ilegal de dados ou comunicações telemáticas;
> c) atentado à integridade dos dados (conduta própria de um subgrupo *hacker*, conhecido como *cracket)*;
> d) atentado à integridade de um sistema.

O Brasil não participa da convenção de Budapeste, no entanto atende boa parte de seus requisitos. A não adesão a convenção é alvo de bastante críticas, pois através dela o Brasil teria acesso as principais formas de cooperação entre os países relacionados aos crimes cibernéticos, o que facilitaria nas investigações para punir quem pratica esse tipo de crime (DOMINGOS, 2018, p. 246).

Neste sentido o Ministério Público Federal se pronuncia:

> O Brasil ainda não é signatário da Convenção de Budapeste, mas o MPF apoia a adesão do país, uma vez que, como integrante, poderá participar ativamente da discussão do protocolo adicional que será finalizado em novembro deste ano. A procuradora-geral da República, Raquel Dodge, enviou ao Ministério das Relações Exteriores ofício no qual defende a adesão do Brasil à Convenção. O assunto também foi tratado em reuniões no Departamento de Assuntos de Defesa e Segurança do MRE (Grossmann Apud Ministério Público Federal, 2018).

5.3 Marco Civil da Internet

A lei nº Lei 12.965/2014, conhecida como Marco Civil da Internet estabelece diretrizes para o uso da internet no Brasil. A lei tem como objetivo disciplinar a relação entre as operadoras de internet e os seus usuários. Para isso, o Marco Civil traz três pilares como base, sendo eles: A liberdade, a privacidade e a neutralidade.

A Liberdade na rede garante a possibilidade de produção, acesso e compartilhamento de qualquer conteúdo. Somente a justiça poderá intervir, a única exceção será o revenge porn que nesse caso o Google, Facebook ou qualquer empresa será punida se não retirar após notificação da vítima ou seu representante legal.

Neste sentido, alguns artigos versam sobre:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da **liberdade** de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> 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;
> 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, grifo nosso).

Quanto à privacidade, ela garante a confidencialidade sobre os dados e mensagens dos usuários da internet. As empresas são obrigadas a manter o histórico durante 6 meses, mas o acesso a ele somente por decisão judicial.

Acerca da Privacidade estão dispostos os artigos abaixo:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> (...)
> II - proteção da privacidade;
> 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;
> Art. 11º Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por

> provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à **privacidade**, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros;
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à **privacidade** e ao sigilo de comunicações. (BRASIL, 2014, grifo nosso).

Já a neutralidade garante que as empresas de internet não cobrem valores diferente de acordo com os conteúdos que você acessa. Neste caso ficará proibido, por exemplo, cobrar mais de quem joga on-line do que de quem apenas acessa páginas de notícias. A regra é que os dados contratados sejam utilizados da maneira que se desejar.

> O Marco Civil da Internet dispõe sobre a Neutralidade em seu artigo 9º, conforme pode ser conferido:
> Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
> § 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
> I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
> II - priorização de serviços de emergência.
> § 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º , o responsável mencionado no caput deve:
> I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;
> II - agir com proporcionalidade, transparência e isonomia;
> III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e
> IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.
> § 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo. (BRASIL, 2014).

5.4 Legislações em outros países

É relevante verificar como outros países tratam os crimes cibernéticos, desta forma é possível visualizar o quanto o Brasil pode avançar neste quesito. Visto que o Brasil é um dos países que mais cometem crimes virtuais, ainda não há legislações suficientes para suprir toda essa demanda de crimes. Acerca destes países, este subcapítulo trará de forma sucinta o direito comparado em relação as legislações de outros países.

5.4.1 Alemanha

Logo após a segunda guerra mundial, a Alemanha já demonstrou preocupação com a criminalidade no meio digital, mais especificadamente com crimes contra a economia que eram cometidos por meio dos computadores.

No ano de 1986 a Alemanha passou a criminalizar diversos crimes através da chamada lei de informática.

Conforme TORRES, a Lei contempla os seguintes itens:

> a) Espionagem de dados (202 a);
> b) Extorsão informática (263 a);
> c) Falsificação de elementos probatórios (269), aí incluindo a falsificação ideológica, o uso de documentos falsos (270, 271, 273);
> d) Alteração de dados (303 a), considerando ilícito cancelar, inutilizar ou alterar dados, penalizando ainda a tentativa;
> e) Sabotagem informática (303 b), punindo a destruição de dados relevantes por qualquer meio (deterioração, inutilização, eliminação ou alteração de um sistema de dados), punindo também a tentativa;
> f) Utilização abusiva de cheques ou cartões de crédito (266 b).

5.4.2 Espanha

Na Espanha a intenção era coibir as condutas criminosas dos hackers, alterando o código penal para a inserção de artigos referente aos acessos ilegítimos e disseminação dos códigos malicioso, conhecidos popularmente como vírus e toda a gama de delitos cibernéticos (TORRE, 2015, p. 121).

Torre (2015, p. 121) elenca entre as condutas puníveis pelo ordenamento espanhol:

> a) ficam equiparadas, para fins penais, as mensagens de correio eletrônico às cartas de papéis privados (art. 197);
> b) é responsabilizado penalmente quem, sem a devida autorização, se aproprie, utilize ou modifique, em prejuízo de terceiros, dados pessoais de outros, que se achem registrados em suportes informáticos (art. 197);
> c) reprime-se o delito de ameaça feito por qualquer meio de comunicação (art. 169);
> d) castigam-se calúnias e injúrias difundidas por qualquer meio (art. 211);
> e) inclui-se o uso de chaves falsas como qualificadora do delito de roubo, entendendo que são também chaves os cartões magnéticos ou perfurados, e os comandos e instrumentos de abertura a distância de sistemas (arts. 238-239);
> f) modifica o art. 248 que tipifica o delito de fraude, incluindo aqueles que, com ânimo de lucro e valendo-se de alguma manipulação informática ou artifício semelhante, consigam a transferência não consentida de qualquer ativo patrimonial em prejuízo de terceiro;
> g) penaliza a conduta de quem faça uso de qualquer equipamento ou terminal de telecomunicação sem consentimento de seu titular, ocasionando a este um prejuízo de mais de cinquenta mil pesetas;
> h) protege-se o software, ao castigar quem danifica os dados, programas ou documentos eletrônicos alheios contidos em redes, suportes, ou sistemas

> informáticos (art. 264), assim como a fabricação, posta em circulação e posse de qualquer meio destinado a facilitar a supressão não-autorizada de qualquer dispositivo utilizado para proteger programas de ordenador (art. 270);
> i) é punida a fabricação ou posse de programas de ordenador, entre outros, especificamente destinados à falsificação de todo tipo de documento (art. 400).

5.4.4 França

A França previu bem as condutas criminosas praticadas por computadores, tendo previsões acerca de acesso fraudulento de acesso aos sistemas de dados, sabotagem informática, destruição de dados, e falsificação de documentos informatizados (SILVA, 2015).

Apesar da França acreditar que o seu ordenamento é bastante moderno e capaz de compreender todo tipo de situação, seu código penal teve de ser alterado, incluindo um capítulo especial na lei n 88-19 que trouxe novas previsões acerca do tema de crimes cibernéticos (SILVA, 2015).

Crespo neste sentido elenca as mudanças:

> a) Acesso fraudulento a sistema de elaboração de dados (462-2), sendo considerados delitos tanto o acesso ao sistema coo nele manter-se ilegalmente. Caso haja supressão ou modificação dos dados ou, ainda, alteração no funcionamento do sistema, a pena é aumentada;
> b) Sabotagem informática (462-3), que pune a conduta de quem apaga ou falseia o funcionamento de sistema eletrônico;
> c) Destruição de dados (462-4), que responsabiliza aquele que, dolosamente, introduz dados em sistema ou, de qualquer forma, suprime ou modifica dados;
> d) Falsificação de documentos informatizados (462-5), que busca punir quem falsificar documentos informatizados com a intenção de causar prejuízo a outrem;
> e) Uso de documentos informatizados (462-6), que pune quem faz uso dos documentos falsos retro mencionados. (Crespo, 2011, p. 28)

5.4.5 Estados Unidos

Os Estados Unidos têm como modelo o sistema judiciário chamado *Commom Law*, sistema este que se baseia em precedentes judiciais. Os Estados Unidos possuem uma política de federalismo, ou seja, cada estado pode criar as suas próprias regras, pode escolher o seu modelo de justiça (SILVA, 2015).

Em relação aos crimes cibernéticos a primeira manifestação dos Estados Unidos aconteceu após um estudante criar um vírus capaz de se expandir em outros computadores. A ideia deste estudante era apenas demonstrar a insegurança das redes de computadores

existentes, no entanto te vírus criado por ele passou a se reproduzir e infectar vários outros computadores (SILVA, 2015).

A partir deste caso, os Estados Unidos passaram a lutar contra a criminalidade virtual, sendo que para isto foi necessário lutar em âmbito estadual e federal. A nível federal veio a Lei de Proteção aos Sistemas Computacionais com a intenção de incriminar as condutas praticadas pelo computador de fraude, apropriação indébita e furto (SILVA, 2015; CRESPO, 2011. p.30)

No ano de 1986 surgiu a primeira lei para responsabilizar as condutas ilícitas no âmbito informático, a Lei de Fraude e Abuso Computacional que visa proteger a acessibilidade dos sistemas para a obtenção de segredos nacionais ou com a intenção de se obter vantagens econômicas (CRESPO, 2011,p.30)

Segundo a legislação americana são coibidas condutas que de certa forma:

> a) atentem contra o sigilo de informação eletrônica de defesa nacional, de assuntos exteriores, de energia atômica ou qualquer outra informação restrita de caráter estratégico;
> b) envolvam a um ordenador pertencente a departamentos ou agências do governo dos Estados Unidos;
> c) envolvam banco ou qualquer outra classe de instituição financeira;
> d) envolvam comunicações interestaduais ou internacionais;
> e) afetem pessoas ou ordenadores em outros países ou Estados.

6 CONSIDERAÇÕES FINAIS

Como foi explanado, a Internet trouxe vários benefícios para a sociedade, em qualquer área que seja. Ocorre que com o surgimento da Internet não só coisas boas foram inseridas, mas também aconteceu a proliferação dos conhecidos como crimes cibernéticos, crimes como: Racismo, estelionato, crimes contra a honra, ganharam outro meio de se consumar.

Portanto, é possível visualizar a necessidade de a sociedade receber informações legais sobre o limite do que se pode fazer na Internet. Para isso, no Brasil algumas leis foram criadas para tentar inibir os problemas ocorridos no mundo digital.

As principais legislações surgiram com a finalidade de impedir o crescimento das ilicitudes ocorridas em âmbito virtual, porém ainda estão longe de serem perfeitas e de inibirem de forma total os crimes ocorridos na Internet.

A lei nº 12.737/2012 (Lei Carolina Dieckmann), criada para alterar o código penal, passando a tipificar os crimes cibernéticos ocorridos contra o computador. No entanto esta lei não trouxe a solução para todos os problemas ocorridos na Internet, visto que o crime tipificado nesta lei são apenas os crimes praticados contra dispositivo informático, sendo assim, será tipificado apenas se houver uma quebra de segurança para obtenção do ilícito.

Cabe ressaltar que, A lei nº Lei 12.965/2014 (Marco Civil da Internet) é outro ponto a se destacar nas legislações criadas no mundo digital. Esta lei trouxe diretrizes para o uso da Internet no Brasil. Através dela é possível disciplinar acerca da liberdade, da privacidade e neutralidade no meio digital.

Conclui-se que, estas legislações não são o suficiente para combater todos os crimes cibernéticos, pois ainda há pontos que não estão detalhados e ocasiona uma dificuldade na hora de criminalizar determinado delito. Sendo assim, a criminalidade no âmbito virtual só tende a aumentar, visto que os avanços no mundo tecnológico não param de crescer e é preciso que a justiça acompanhe essa evolução.

REFERÊNCIAS

ARNAUDO, Daniel. **O Brasil e o Marco Civil da Internet. Instituto Igarapé**. 2017. Disponível em: https://igarape.org.br/marcocivil/assets/downloads/igarape_o-brasil-e-o-marco-civil-da-internet.pdf. Acesso em: 13 ago. 2019.

BORGES, Abimael. **Lei Carolina Dieckmann - Lei nº. 12.737/12, art. 154-a do Código Penal**. JusBrasil, 2012. Disponível em: https://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal). Acesso em: 7 ago. 2019.

BRASIL ESCOLA. **Internet no Brasil e sua Administração. Brasil Escola**, 2019 Disponível em: https://brasilescola.uol.com.br/informatica/internet-no-brasil.html. Acesso em: 21 ago. 2019.

BRASIL. Decreto-lei nº 2.848, de 07 de dezembro de 1940 (Código Penal). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 14

BRASIL.Escola de Magistrados Investigação e prova nos crimes cibernéticos. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 22 ago. 2019.

BRASIL. Lei 12.965 de 23 de Abril de 2014. Disponível em: http://www.Planalto.Gov.Br/ccivil_03/_ato2011-2014/2014/lei/l12965.Html. Acesso em: 01 jun. 2019.

_____. Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckman). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em:

_____. Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14

_____. Lei nº 3.689, de 03 de outubro de 1941 (Codigo de Processo Penal Brasileiro). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 19 de set. 2019.

_____. Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8069.htm. Acesso em: 19 de set. 2019.

_____. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Acesso em: 19 de set. 2019. http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 19 ago. 2019.

BULOS, Uadi Lammêgo, Constituição Federal anotada, 2.ed., São Paulo, Editora Saraiva, 2001, p.105

CARTILHA. Cartilha de segurança pela internet. Cert.Br, 2011. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 10 set. 2019.

COSTA, Marco Aurélio Rodrigues. Crimes de informática. Disponível em: Revista Eletrônica Jus Navigandi. Site: http://www.jus.com.br/doutrina/crinfo.html. -- SOBRE MISTOS E PURO

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.48

DAVID, H. DR2 - Nascimento e evolução dos computadores/internet. CINEL - Centro Formação Profissional da Indústria Eletrónica. Disponível em: http://efaredesinformaticas01.cinel.org/site_files/formandos/jose/dr2.pdf. Acesso em: 15 jul. 2019.

DIEZ, Valéria. Revenge Porn: o feminicídio virtual na internet. Carta Forense, 2016. Disponível em: <http://www.cartaforense.com.br/conteudo/artigos/revenge-porn--o-feminicidio-virtual-na-internet/16400>. Acesso em: 30 jun. 2019.

DOMINGOS, Fernanda Teixeira. A obtenção das provas digitais. In: SILVA, Angelo Roberto Ilha da. (Org.), Crimes Cibernéticos. 2 ed. Porto Alegre: Livraria do advogado, 2018, p. 235-247.

DORIGON.Crimes cibernéticos. Disponível em: https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade. Acesso em: 8 ago. 2019.

DUARTE, Henrique. O que são hijacker e como eles podem colocar o seu pc em risco,2015. Disponível em: http://www.techtudo.com.br/noticias/noticia/2014/02/o-que-saohijackers-e-como-eles-podem-colocar-o-seu-pc-em-risco.html. Acesso em: 15 set. 2019.

DULLIUS, A.; HIPLLER, A.; FRANCO, E. Dos Crimes Praticados em Ambientes Virtuais. Conteúdo Jurídico, 2012. Disponível em: http://www.conteudojuridico.com.br/consulta/Artigos/30441/dos-crimes-praticados-em-ambientes-virtuais. Acesso em: 22 ago. 2019.

FERREIRA, Jonas. A HISTÓRIA DA INTERNET. Adlogados, 2017. Disponível em: https://www.adlogados.com/artigos/visualizar/a-historia-da-internet21#_ftnref8. Acesso em: 22 ago. 2019.

FERREIRA, Paulo Gomes. Mensagens Racistas postadas na Internet. In: SILVA, Angelo Roberto Ilha da. (Org.), Crimes Cibernéticos. 2 ed. Porto Alegre: Livraria do advogado, 2018, p. 131-146.

G1. Lei 'Carolina Dieckmann', que pune invasão de PCs, entra em vigor. Disponível em: http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html. Acesso em: 7 ago. 2019.

GRECO, Rogério. **Curso de direito penal:** parte especial - v. 3. 12. ed. Niterói: Impetus, 2015.

JESUS, Damásio Evangelista de. **Direito Penal 2° volume parte especial**: dos crimes contra a pessoa e dos crimes contra o patrimônio / Damásio E. de Jesus – 28 ed. Ver e atual, São Paulo: Saraiva, 2007, p.179-219.

MACHADO, Jonathan. **O que é um keylogger?**, 2012. Disponível em: https://www.tecmundo.com.br/spyware/1016-o-que-e-keylogger-.htm. Acesso em: 15 setembro. 2019.

MICHAELIS. Dicionário. **Dicionário de Lingua Portuguesa**, 2019. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/internet%20/ Acesso em: 08 ago. 2019.

NAUATA, Felipe. **Crimes virtuais**: Estelionato. Disponível em: https://jus.com.br/artigos/65242/crimes-virtuais-estelionato. Acesso em: 1 out. 2019.

NUCCI, Guilherme de Souza. **Código penal comentado**: estudo integrado com processo e execução, 14. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2014, p.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 13. ed. Rio de Janeiro: Forense, 2017. 626 p.

NUCLEO DE CRIMES, Mp. Visão geral sobre a Lei 12.737/2012. **Justiça de Saia**, 2017. Disponível em: http://www.justicadesaia.com.br/wp-content/uploads/2017/06/Cartilha-Lei-Carolina-Dieckmann.pdf. Acesso em: 04 ago. 2019.

OLIVA, Afonso. **Especialista em Direito Eletrônico explica Lei Carolina Dieckmann**. G1 Sergipe, 2012. Disponível em: http://g1.globo.com/se/sergipe/noticia/2013/04/especialista-em-direito-eletronico-explica-lei-carolina-dieckmann.html. Acesso em: 7 ago. 2019.

PINHEIRO. **Os cybercrimes na esfera jurídica brasileira**. 2000. Disponível em: https://jus.com.br/artigos/1830/os-cybercrimes-na-esfera-juridica-brasileira. Acesso em: 12 set. 2019.

RODER, P.; SILVA, H. CyberBullying: Uma agressão virtual com consequências reais para a vítima e a sociedade. In: SILVA, Angelo Roberto Ilha da. (Org.), **Crimes Cibernéticos**. 2 ed. Porto Alegre: Livraria do advogado, 2018, p. 27-40.

ROMONI. **Fotos de Dieckmann nua tiveram 8 milhões de acessos**. Folha Uol, 2012. Disponível em: https://www1.folha.uol.com.br/tec/2012/05/1089392-fotos-de-dieckmann-nua-tiveram-8-milhoes-de-acessos-saiba-como-proteger-as-suas.shtml . Acesso em: 7 ago. 2019.

SARAIVA, Adevan. **Dos crimes contra a honra: breves comentários**. 2015. Disponível em: https://jus.com.br/artigos/39929/dos-crimes-contra-a-honra-breves-comentarios. Acesso em: 18 set. 2019.

SCHMIDT, Guilherme. **Crimes Cibernéticos**. JusBrasil, 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos . Acesso em: 22 ago. 2019.

SIGNIFICADOS. **Significado de World Wide Web.** Significados, 2019. Disponível em: https://www.significados.com.br/world-wide-web/ . Acesso em: 7 ago. 2019.

SILVA, Amaury; SILVA, Artur Carlos. **Crimes de Racismo**, 1 ed. Leme. Editora JH Mizuno, 2012, p.23.

SILVA, Ana Carolina Calado da. O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira, 2015. Disponível em: http://www.egov.ufsc.br/portal/conteudo/o-estudo-comparado-dos-crimes-cibern%C3%A9ticos-uma-abordagem-instrumentalista-constitucional Acesso em: 19 de set. 2019.

SILVA, Angelo Roberto Ilha da. (Org.), **Crimes Cibernéticos**. 2 ed. Porto Alegre: Livraria do advogado, 2018. p. 11-255.

TORRE, Marina Giantomassi della. **Aspectos Processuais e Penais dos Crimes de Computador**, 2009. Dissertação de Mestrado (Mestrado em Direito Processual Penal)-Pontifícia Universidade Católica de São Paulo. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp0 Acesso em: 19 de set. 2019.

TURNER, David; MUÑOZ, Jesus. **Para os filhos dos filhos de nossos filhos**: uma visão da sociedade internet. São Paulo: Summus, 2002.

VIANA, Marco Túlio apud CARNEIRO, Adeneele Garcia. **Fundamentos de direito penal informático**. Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003, p. 13-26.

WENDT, E.; JORGE, H. V. N. **Crimes Cibernéticos**. São Paulo: BRASPORT, 2013, p. 03-200.

WERNER, Leonardo. **Internet foi criada em 1969 com o nome de "Arpanet" nos EUA**. 2000. Disponível em: https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml. Acesso em: 12 set. 2019.