UNIVERSIDADE DE SANTA CRUZ DO SUL
CURSO DE DIREITO

Jean Kilian

CRIMES CIBERNÉTICOS UMA ABORDAGEM JURÍDICA DIANTE DA EFICÁCIA NA LEGISLAÇÃO BRASILEIRA

Santa Cruz do Sul
2020

Jean Kilian

CRIMES CIBERNÉTICOS UMA ABORDAGEM JURÍDICA DIANTE DA EFICÁCIA NA LEGISLAÇÃO BRASILEIRA

Trabalho de Conclusão apresentado ao Curso de Direito da Universidade de Santa Cruz do Sul para obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Vinícius Ferreira Laner

Santa Cruz do Sul
2020

Dedico a presente monografia aos meus familiares, orientador e aos professores que sempre de prontidão auxiliaram para que pudesse chegar até esse momento.

AGRADECIMENTOS

Primeiramente, agradeço a Deus.

Agradeço aos meus pais pelo apoio e dedicação.

Quero agradecer também ao orientador Prof. Vinícius Ferreira Laner, e a todos professores da Universidade que sempre auxiliam para concretização desse sonho.

RESUMO

A presente monografia visa analisar a temática dos crimes cibernéticos no Brasil, identificando a eficácia na legislação brasileira, consistindo no problema de pesquisa. Utiliza-se o método dedutivo e pesquisa bibliográfica, trazendo os crimes cibernéticos praticados na atualidade brasileira, desde o surgimento da internet, nossa legislação penal não é compatível com a prática delituosa de hoje no Brasil, sendo esta legislação de 1940, ascensão e o crescimento é mais rápido que nossa legislação atual, não acompanhando ao meio virtual, sendo que é demasiada branda e ineficaz, popularmente conhecida como a Lei Carolina Dieckmann. Lei 12.737/2012, modificando nosso ordenamento jurídico mas que ainda é insuficiente, visto ao crescimento exponencial, desde o surgimento e expansão da internet, hoje utilizando-se recursos da Deep Web e Dark Web, muitos usuários escondem informações e dificultam as investigações, expondo a real eficácia e comprometimento de todos os poderes ao combate e prevenção dos crimes cibernéticos, ainda assim houve significativas mudanças no tocante das garantias e direitos dos usuários com a chegada da Lei 12.965 de 2014 (Marco Civil) e Lei de Proteção de Dados Pessoais 13.709/2018, lembrando sempre da educação digital e da cooperação internacional dos países para prevenção dos crimes cibernéticos.

Palavras-chave: Combate. Crimes Cibernéticos. Educação Digital. Eficácia. Legislação Penal.

ABSTRACT

The present study analyzes the theme of cybercrimes in Brazil, identifying the effectiveness in Brazilian legislation, consisting of the research problem. Using the deductive method and bibliographic research, introducing the cybercrimes practiced currently in Brazil, since the rise of the internet, Brazilian criminal law is not compatible with current criminal practice, the Brazilian legislation of 1940, the growth is faster than our current legislation, not following the virtual environment, and penalties so small and ineffective, popularly called the Carolina Dieckmann Law. The Law 12.737/2012 changed our legal order, but which is still insufficient, front the exponential growth of the internet technology, since the emergence and expansion of the internet, now using Deep Web and Dark Web resources, have many possibilities hide information and hinder investigations, exposing the real importance the commitment and effectiveness of the all powers to combatting cybercrimes, there were significant changes regarding the guarantees and rights of users with the arrival of Law 12,965 of 2014 (Marco Civil) and Law 13.709/2018, always remembering digital education and searching international cooperation between countries to prevent cybercrimes.

Keywords: Combat. Cyber Crimes. Digital Education. Effectiness. Penal Law.

SUMÁRIO

1 INTRODUÇÃO

É notório que os crimes aconteciam muito antes da criação da internet, e com o avanço tecnológico, o direito teve que adequar-se para combater essas infrações no âmbito penal cibernético. Mas realmente não foi o que ocorreu, pois estamos cada vez mais suscetíveis a estes crimes na atualidade, pois nossa legislação permite com que estas infrações sejam cometidas e muitas vezes acabam por ficar impunes ou com penas relativamente brandas.

Visto que o Código Penal de 1940, tem que lidar com crimes cibernéticos da atualidade, pelo fato do agente praticar e consolidar esses crimes em âmbito virtual, não necessitando ir para o mundo físico para cometer estes crimes. Havendo assim necessidade do Poder Judiciário regulamentar leis que protegessem os usuários que estão vulneráveis navegando nas redes sociais, utilizando de seus recursos virtuais smartphone ou notebook, em busca de vítimas, vulneráveis ou suscetíveis a sofrerem diversos crimes.

Em meados de 1960, surgiu a internet, e com isso, os criminosos migraram para ciberespaço, em virtude da facilidade de acesso, surgia um grande negócio e muito lucrativo. Visto que nosso Código penal é de 1940, é de fato necessário uma atualização da legislação para combater e auxiliar o Direito dos cidadãos, visto que a internet cresce a cada dia mais, alcançando um número cada vez maior de usuários deve ser tutelado seus direitos e deveres e uma tipificação penal da criminalidade cibernética.

Diante da análise do objetivo geral do trabalho de curso, que está inteiramente ligado a eficácia da legislação pertinente aos crimes cibernéticos, avaliando a eficácia ao final, consistindo no problema de pesquisa que trata diretamente da eficácia no que tange os crimes cibernéticos no Brasil.

O método utilizado para execução do trabalho é o dedutivo, com base na pesquisa bibliográfica partindo do pressuposto da revisão da literatura, livros e obras científicas e jurídicas para abarcar a temática principal da monografia.

Serão abordados no primeiro capítulo os aspectos gerais da internet, as camadas da DeepWeb, e DarkWeb, onde ocorrem diversos tipos de crimes, a diferença entre Cracker e Hacker, que utilizam dos recursos virtuais de software ou

hardware de um computador, também os tipos de vírus que todos estão suscetíveis no âmbito virtual.

No segundo capítulo trataremos dos crimes cibernéticos, conceitos básicos, análise dos tipos penais mais recorrentes em virtude dos crimes virtuais, que são os crimes contra honra, cyberbullyng estelionato, racismo e pornografia virtual contra crianças e adolescentes que são comercializados e expostos na rede virtual de computadores.

Após análise do primeiro e segundo capítulo, partindo para o terceiro e último capítulo, no qual verificaremos a legislação vigente em decorrência dos crimes cibernéticos, que é a Lei 12.737/2012, também conhecida como Lei Carolina Dieckmann, no qual tipifica novos tipos penais referente ao mundo cibernético, também o Marco Civil da Internet que trata dos direitos e deveres dos internautas no ciberespaço Lei 12.965/14, no qual, efetivamente inovou estes tipos penais no ramo cibernético, mas devemos levar em consideração a crescente ascensão da criminalidade virtual, no qual deve-se dar maior suporte e autonomia para as autoridades, investigarem e provarem os fatos pertinentes a sua aplicação.

Também será exposto a legislação internacional, cooperação dos países em combate a cibercriminalidade, convenção de Budapeste (2001), em relevância aos crimes cibernéticos internacionais, meios de provas e procedimentos de investigação e também a nova Lei de Proteção de Dados 13.709/2018, tratando dos crimes virtuais especialmente cibernéticos no Brasil, além da importância fundamental do tema para conscientização e prevenção e repressão dos crimes virtuais no Brasil.

2 CONCEITOS E ASPECTOS GERAIS DA INTERNET

As origens da internet podem ser encontradas na Advanced Research Projects Agency Network (ARPANET), uma rede de computadores criada em setembro de 1969, foi formada em 1958 pelo Departamento de Defesa dos Estados Unidos, como missão e objetivo de superioridade teológica frente a União Soviética. A ARPANET não passava de um pequeno programa fundado em 1962 com base em uma unidade preexistente, tinha como objetivo definido estimulação da pesquisa e por justificativa a concentração de vários centros de computadores e também grupos de pesquisas que trabalhavam para agência, reunindo como compartilhar tempo de computação online (CASTELLS, 2003).

A ideia básica da criação da rede mundial de computadores, saiu das mãos de um órgão dos Estados Unidos, no ano de 1969, na Guerra Fria, foi criado por motivações bélicas por meio de um projeto designado como ARPANET da agencia de pesquisa em projetos avançados do departamento de defesa Americano através da colaboração da Rand Corporation, capaz de sobreviver a um ataque nuclear soviético, consistindo em computadores ligados a rede locais, também ligavam-se entre si, formando em conjunto uma grande rede, essa foi a ideia base, que hoje chamamos de internet, seu uso era exclusivo das Forças Armadas (RIBEIRO, 2013).

A criação e o desenvolvimento do computador estavam diretamente vinculados as atividades bélicas das forças armadas e dos departamentos de defesas dos países desenvolvidos como Estados Unidos, Rússia e a Inglaterra, em razão da militarização demorou algum tempo para popularização dessa máquina, que veio à mão dos civis apenas em meados dos anos 1960, com finalidade de executar tarefas de cálculos pesados e gerenciamento de grandes empresas. A população em geral estava fora do uso dos computadores, até a invenção dos microprocessadores, conseguindo operar com números maiores de operações, diante da evolutiva, também do desenvolvimento dessas técnicas, e da popularização e elevado capital gerado com a venda desses computadores, no final dos anos 1970, foi desenvolvido por um grupo de estudantes californianos anonimamente resultando no projeto do primeiro computador de cunho pessoal, dando o passo inicial para ascensão da cultura da informação (RIBEIRO, 2013).

Em 1975 a ARPANET, foi transferida para Defense Communication Agency (DCA), tornando a comunicação dos computadores para diferentes ramos das forças armadas, criando várias redes sobre o seu controle, estabelecendo a chamada Defense Data Network, operando com protocolos TCP/IP. Já em meados de 1983 o Departamento de defesa preocupado com a segurança resolveu criar a MILNET, uma rede independe para usos militares, sendo em 1984 a National Science Foundation (NSF), acabava por monta sua própria rede de comunicação entre computadores a NSFNET, usando em 1988 a ARPA-INTERNET como backbone[1], já em 1990 a ARPANET, tornava-se obsoleta, pois a maioria dos computadores nos Estados Unidos tinham capacidade de entrar em rede, sendo que na década de 1990, muitos provedores de serviços montaram suas próprias redes estabelecendo assim suas portas de comunicação com base comercial (CASTELLS, 2003).

A internet é conhecida no mundo todo, devido ao fato do desenvolvimento do www, esta aplicação de compartilhamento de informação foi desenvolvida na década de 1990, por um programador inglês Tim Berners-Lee (CASTELLS, 2003).

> No início da década de 1990 muitos provedores de serviços da Internet montaram suas próprias redes e estabeleceram suas próprias portas de comunicação em bases comerciais. A partir de então, a Internet cresceu rapidamente como uma rede global de redes de computadores. O que tornou isso possível foi o projeto original da Arpanet, baseado numa arquitetura em múltiplas camadas, descentralizada, e protocolos de comunicação abertos. Nessas condições a Net pôde se expandir pela adição de novos nós e a reconfiguração infinita da rede para acomodar necessidades de comunicação (CASTELLS, 2003, p. 18).

Com isso ainda na década de 1990, a internet popularizou-se ainda mais entre as universidades norte-americanas e logo para o mundo todo, revolucionando as trocas de conhecimentos e informações, criando um ambiente virtual, paralelo ao real, sendo chamado de ciberespaço (BARRETO; BRASIL, 2016). ”A Internet é uma rede de computadores interligados mundialmente, capaz de eliminar distâncias. É a informação a apenas um clique de distância” (BARRETO; WEDNT; CASELLI, 2017, p. 58).

> Com o passar dos anos se consolidou a importância de criar uma rede capaz de integrar computadores que estivessem distantes e que por

[1] Backbone significa espinha dorsal (MARTINS, 2009, https://www.tecmundo.com.br).

> intermédio dela fosse permitida a comunicação de dados. Sob esse ponto de vista foi criada a ARPANET, inicialmente interligando a Universidade da Califórnia (Los Angeles e Santa Bárbara), a Universidade de Stanford (Santa Cruz) e a Universidade de Utah (Salt Lake City (WEDNT; JORGE, 2013, p. 18).

Tendo assim, uma troca de informações, e-mails, noticiais, implementado no Brasil em meados de 1991, com transmissão de alguns pacotes TCP/ITP para os Estados Unidos, considerado revolução da época. A evolução da comunicação contribui com muita celeridade dos dados, aonde estes devem chegar (BARRETO; WEDNT; CASELLI, 2017).

Diante do sucesso imediato da internet, o número de pessoas que buscavam informações crescia avassaladoramente, com isso as informações não eram claras, estavam confusas, eram postas nas redes como se fosse uma biblioteca desorganizada, sendo o acesso a informação privilégio de poucos. Tempo atrás a internet não permitia pesquisas e buscas de uma forma precisa e organizada com isso houve a inovação dos promissores eruditos David Filo e Jerry Yang, estudantes da Universidade de Stanford, dos Estados Unidos, acabaram por ganhar um concurso e os futuros fundadores do Yahoo desenvolviam uma ideia e uma oportunidade de ganhar dinheiro e inovar com capacidade de filtrar as pesquisas de forma que seriam mais precisas (BARRETO; WEDNT, 2020).

O sucesso imediato desses jovens crescia assustadoramente e nisso gerava custos para empresa, sendo necessária mantê-la deveria ganhar dinheiro com a internet, até o momento não estava introduzida, nesse ponto surgiu a publicidade, empresas investiam dinheiro em banners na página do Yahoo, passando a ter lucros milionários, fortalecendo muito esta ferramenta de busca (BARRETO; WEDNT, 2020).

2.1 Internet no Brasil

No Brasil, o IBGE (Instituto Brasileiro de Geografia e Estatística), passou a utilizar um computador no ano de 1964, foi criado o Centro Eletrônico de Processamento de Dados do Estado do Paraná. Em 1965 foi criado o serviço Federal de Processamento de Dados, e com isso o Brasil associou-se ao consórcio internacional de telecomunicação via satélite, estava vinculado ao Ministério das

Comunicações. No ano de 1972 foi fabricado o primeiro computador brasileiro pela Universidade Federal de São Paulo (USP), sendo dois anos depois criado o Computadores S.A, 1979 criou-se a Secretaria Especial de Informática, sendo um passo importante da consolidação da internet brasileira em 1988 com a conexão à bitnet da Fundação de Amparo à pesquisa do Estado de São Paulo (FAPESP), Laboratório Nacional de Computação Cientifica (LNCC), e da Universidade Federal do Rio de Janeiro (WEDNT; JORGE, 2013).

A Secretaria Especial de Informática foi extinta em 1992, treze anos após sua criação e para o seu lugar foi criada a Secretaria de Política de Informática, entretanto nesse ano foi implementado a primeira rede conecta a internet, interligava as principais universidades brasileiras, diferentemente da internet de hoje, não existia interface gráfica os usuários conectados na rede poderiam apenas trocar e-mails, mas no ano de 1995, com o uso comercial da internet no país com velocidade máxima de conexão era 9,6Kpbs. Neste mesmo ano houve a criação do Comitê Gestor da Internet no Brasil com a finalidade de integrar e coordenar todas as iniciativas e serviços de internet envolvidos no país, havendo qualidade técnica e inovação e propagação dos serviços ofertados (WEDNT; JORGE, 2013).

O Brasil integra o grupo de 79 países onde mais de 50% da população tem acesso à Internet. No país, 57,6% das pessoas estão conectadas. A forma de acesso, porém, apresenta variações. A cada 100 brasileiros, apenas 11,5 possuem uma assinatura de banda larga fixa, quando avaliados as assinaturas de banda larga móvel esse valor sobe para 78,1, ainda segundo o relato da UIT, 48% dos domicílios do Brasil não possuem conexões a internet, sendo os resultados da Pesquisa Nacional por Amostra de domicilio de 2013 (PNAD), divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE). Segundo a ONU houve avanços referentes a evolução tecnologia nas residências, mas estes avanços foram totalmente desiguais pois em países como Noruega, Dinamarca e Islândia o número de pessoas conectadas ultrapassa os 90%, e em países em desenvolvimento a média de conexão da internet é de apenas 35%, ainda segundo a ONU esses avanços desiguais se deram no ano de 2014 para 2015 em que 300 milhões de pessoas conquistaram o acesso à rede mundial de computadores somando 3,2 bilhões, sendo que metade da comunidade mundial não está conectada (NAÇÕES UNIDAS BRASIL, 2015).

2.2 Crescimento tecnológico

Quando estamos falando de internet, logo analisamos um mundo virtual com vasto e incontável número de informações, podendo estar organizados ou desorganizadas em decorrência da quantidade de informações colocadas na rede e que estão à disposição de todos nós, podendo ser utilizados contra ou a favor das pessoas, dependendo claro do ponto de vista, e os meios utilizados por esses recursos (BARRETO; WEDNT, 2020).

Já em meados de 1998, surge a Google Inc. foi fundada e revolucionou os sites e formas de pesquisas na web, fundadores da Google Sergey Brin e Larry Page, priorizava nas pesquisas buscas pela quantidade de links, no qual o termo buscado possuía, ou seja, se determinada palavra tinha sido buscava mais vezes por determinados sites, seriam colocados como prioridade, trazendo dados úteis e mais precisos, foi a revolução de internet, tornando a Google a maior empresa do setor, inovando e trazendo a busca mais atrativa para o público (BARRETO; WEDNT, 2020).

Com o avanço tecnológico trouxe vários benefícios, a comunicação, os negócios, relações sociais, tornando nossa rotina cotidiana mais fácil, e com isso, os usuários com intenções de causar danos, aproveitando-se destes serviços para suas práticas criminosas (BARRETO; WEDNT, 2020). “O uso da internet como sistema de comunicação e forma de organização explodiu nos últimos anos do segundo milênio” (CASTELLS, 2003, p. 8). “De acordo com a Internet World Stats, em junho de 2019 chegamos ao impressionante volume de 4,536 bilhões de pessoas com acesso à Internet” (BARRETO; WEDNT, 2020, p. 13).

A internet hoje, é de suma importância para nossas vidas, hoje a tecnologia da informação é a eletricidade da era industrial, a internet passou a ser uma base tecnológica de uma forma organizacional da era da informação, conhecida como rede. Sendo esta rede, todos nós interligados, uma pratica muito antiga da civilização, mas que ganharam numa sobrevida em nosso tempo, transformando-se em redes de informações (CASTELLS, 2003).

De acordo com o crescimento da internet temos o entendimento de Jesus e Milagre (2016, p. 15):

> A convergência tecnológica, a dinâmica industrial e a queda dos preços dos equipamentos, aliados ao vertiginoso crescimento da internet, são molas propulsoras das recentes transformações sociais locais. O Brasil ultrapassa pela primeira vez 100 milhões de usuários de internet. A evolução rápida, eis que duas décadas atrás utilizávamos redes Fidonet, conectando-se com pessoas através de BBSs (Bulleting Board Systems) e modems que nos permitiam o acesso discado, muitas vezes em não mais que 56kpb (kilobyts por segundo).

A internet tem seu aumento exponencial maior a cada ano, sendo relativo a evolução tecnológica, entrelaçado ao barateamento dos dispositivos tecnológicos, tornando-se assim mais acessível a grande parcela da sociedade (WEDNT; JORGE, 2013).

2.3 Internet em relação ao direito

Disciplina o Lei 12.965/14 (Marco Civil da Internet), em que dispõe do acesso à internet, considerando o acesso à internet como direito essencial a todos ao exercício da cidadania Conforme o Artigo 4° da referida Lei:

> Art. 4º - A disciplina do uso da internet no Brasil tem por objetivo a promoção:
> I - do direito de acesso à internet a todos;
> II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
> III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
> IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados (BRASIL, 2014, http://www.planalto.gov.br).

Também no tocante dessas conexões da internet em relação ao direito, se dão em modo de estarem em fontes que são classificadas como abertas e fechadas de acordo com seu conteúdo. Podendo definir-se a fonte como dado ou conhecimento da inteligência de investigação, produzindo assim conhecimento e provas, sendo admitidas no âmbito do direito (BARRETO; WEDNT; CASELLI, 2017).

Visto o conceito das fontes, deve ser classificada, portando as chamadas fontes abertas são aqueles que tem livre acesso ao público, sem obstáculos ou empecilhos para ter acesos a informação, já dado as fontes fechadas são aquelas

protegidas para o acesso, onde o público é seleto e restrito (BARRETO; WEDNT; CASELLI, 2017).

Todos os dias pessoas são ofendidas em redes sociais, também outras são cobradas por produtos que nunca fizeram a compra, inúmeras contas são saqueadas e muitas vítimas desses golpes nunca recebem os produtos que compram na internet, diante desse cenário, é evidente que nada é 100% seguro ou mesmo qualquer um está suscetível a ser uma vítima desses golpes virtuais (CASSANTI, 2014). Pelo fato da internet ter esta instabilidade, abre brechas e possibilidades. “Os recursos tecnológicos permitem que cibercriminosos, espalhados por diversas localidades, comuniquem-se e realizem ações criminosas em parceria e organizadamente” (WEDNT; JORGE, 2013, p. 168).

> No Brasil, os crimes de informática superam até o narcotráfico. Somos o terceiro país no ranking mundial neste tipo de crime. A Federação Brasileira dos Bancos (Febraban) divulgou que o internet banking é utilizado por 46% das contas ativas no país e 24% dos 66 bilhões de operações bancárias realizadas em 2011 foram feitas pela internet. E, no mesmo ano, as instituições pagaram cerca de R$ 1,2 bilhão a clientes que tiveram problemas em suas contas bancárias, como transferências e saques indevido por meio eletrônico. (CASSANTI, 2014, p. 18).

Também como vulnerabilidade da internet trata que os desenvolvedores não queriam que ela fosse controlada pelos governos, sendo individualmente ou coletivamente, assim projetaram para que o sistema tivesse prioridade na descentralização e não na segurança (CLARKE; KNAKE, 2015).

A internet pode comunicar-se com qualquer computador através de uma rede de internet, sendo assim o ciberespaço, inclui a internet que está presente em todas as redes, algumas dessas redes são privadas que estão teoricamente separadas, devendo o usuário conecta-la, são redes transacionais que fazem coisas, como enviar dados de fluxos de dinheiro, mercado de ações, dados de cartão de credito, sendo algumas dessas redes sistemas que controlam máquinas que apenas podem comunicam-se com outras máquinas, no caso de elevadores, painel de controle de conferencia de bombas hidráulicas, geradores que são controladas dessa forma (CLARKE; KNAKE, 2015).

Significando assim diversidade de informação, todas trafegando, sendo e-mails, notícias que hoje chegam em qualquer parte do mundo com apenas um

clique, e que estão circulando, podendo ser de grande utilidade na produção de conhecimento e também na tomada de decisões governamentais. (BARRETO; WEDNT; CASELLI, 2017).

2.4 A internet Deep Web e Dark Web

A internet desenvolveu-se na década de 1960, primeiramente para emprego militar, tendo como ideia central a reunião de computadores mundialmente interconectados, comunicando-se através de protocolos, inicialmente TCP/IP, considerados organizadores de mensagens de dados que circulavam entre essas maquinas. Este protocolo é composto por um conjunto de regras, no qual se divide em mensagem em pacote que irá trafegar pela internet, podendo assim seguir caminhos diferentes na rede. Com isso ocorreu a possibilidade de troca de informações entre inúmeros computadores e outros dispositivos, utilizando-se várias conexões diferentes. (BOMFATI; KOLBE JUNIOR, 2020).

A conexão entre os inúmeros dispositivos pode dar-se por diferentes tecnologias, antigamente essas conexões utilizavam-se do uso de modens, foram substituídos pelo uso da banda larga, que tem como principal forma a conexão A DSL, o cabo, o rádio, 3G, 4G, o satélite e recentemente a fibra ótica. Para que ocorra o envio, requisição para a internet devemos ter instalado no computador um browser ou aplicativo de acesso, podendo ser feito através de um modem ligado a linha telefônica ou a um cabo, também temos conexões via Wi-Fi, e Bluetooth, que acessarão um provedor, e com isso entrar nos servidores de todos os lugares do mundo conectados entre cabos ou satélites. (BOMFATI; KOLBE JUNIOR, 2020).

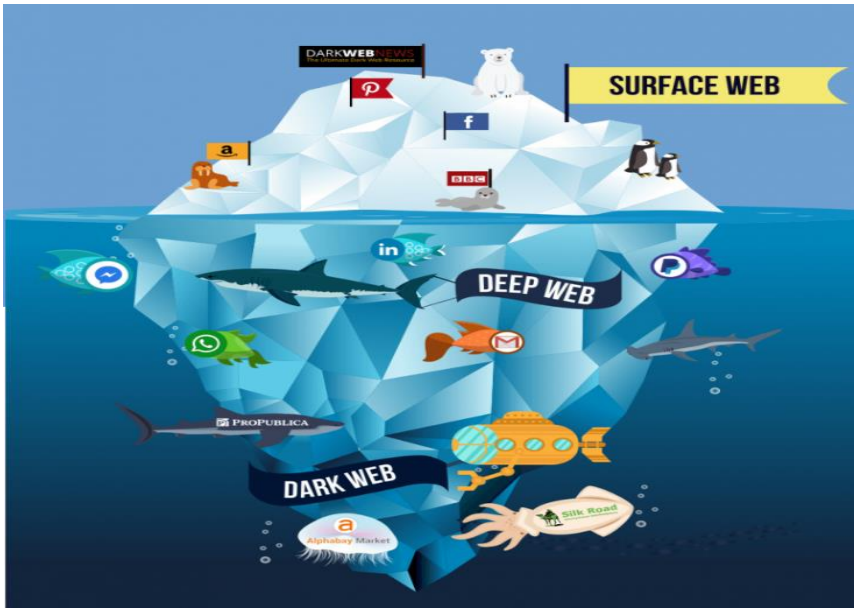
Tratando da Deep Web, também conhecida como internet profunda, ou seja, o lado obscuro da internet. Uma informação impressionante é que essa rede detém 90% das informações contidas na web, mas não podem ser acessadas com navegador comum. Normalmente os usuários que entram nessa rede não querem ser identificados, ou seja, encontrados, entre os usuários que acessam são traficante de drogas, terroristas, traficantes de órgãos humanos de crianças entre outros criminosos (BOMFATI; KOLBE JUNIOR, 2020).

A Deep Web surgiu também com a intenção de ter uma rede independente, fora do padrão www, para ser utilizada no caso de ocorrer uma catástrofe mundial.

Consequentemente surgiu a Dark Web ela é denominada uma camada ainda mais obscura, profunda e oculta da rede teve como origem as análises dos Laboratórios da Marinha dos Estados Unidos, no qual tinha desenvolvido o The Onion Routing – TOR (roteamento em cebola, uma rede em anonimato no qual o acesso está ligado em adentrar as camadas da web, como se fossem uma cebola) (BOMFATI; KOLBE JUNIOR, 2020).

Conforme ilustrado na imagem, verifica-se as camadas referidas ao estudo, sendo ilustrada por um iceberg no mar, representado pela superfície (Surface Web), sendo ela nossa World Wide Web, a internet usual, com isso o mar representa bem o contexto, pois nele verifica-se a Deep Web, que está localizada abaixo da superfície, contudo não é visto livremente na internet, o seu uso não está ligado ao crime, pois a pessoa pode estar conectando-se para não ser rastreada zelando pela sua segurança e privacidade. A Dark Web trata apenas de uma pequena parcela da Deep Web, também com sites e redes não indexadas pelos mecanismos de busca, onde nesta parte está voltada para práticas criminosas de todos os tipos, está elencada na parte inferior do gráfico (GOGONI, 2019).

Figura 1 – Imagem representado Surface Web, Deep Web e a Dark Web (GOGONI, 2019, https://tecnoblog.net).



“A Deep Web é, portanto, composta por redes de computadores que têm como características o anonimato, a criptografia, a descentralização e a codificação aberta, e cujo o conteúdo não é “visível” pelas ferramentas de buscas convencionais” (BARRETO; SANTOS, 2019, p. 17).

A criptografia está ligada a confidencialidade, sendo um conjunto de técnicas visando proteger uma informação entre o emitente da mensagem e o receptor, para que estes consigam compreendê-la, a criptografia, de cunho relacionado a guerra, mas comerciantes e os governantes utilizam como recurso e meio para que as pessoas não autorizadas descubram informações e estratégias indevidas. A criptografia funciona de forma que o emissor da mensagem usa um protocolo que protege essa mensagem, sendo transmitido ao destinatário que possuía uma chave que resolvera esse protocolo para poder acessar seu conteúdo. Com o surgimento dos meios digitais principalmente da internet os métodos de criptografia ficaram mais avançados usando chaves para criptografar e de descriptografar os conteúdos (FIORIM, 2015).

Uma das vulnerabilidades também da Internet é o fato de que quase tudo o que funciona é aberto, ou seja, sem criptografia. Quando você está navegando pela web, a maioria das informações é enviada sem a devida proteção, o que significa que não é criptografada deixando suscetível a sofrer as consequências no tocante dos cibercriminosos (CLARKE; KNAKE, 2015). “A dificuldade ocorre quando o investigador se depara com o tráfego de pacotes que estão encriptados ou protegidos pelos provedores de conteúdo” (WEDNT; JORGE, 2013, p. 168).

Realmente com o universo da Deep Web e Dark Web, fica de fato evidenciado, o grande avanço tecnológico frente ao nosso Direito, os criminosos utilizam-se desses mecanismos para evadir-se e dificultar as investigações, mostrando perícia e destreza nos crimes praticados na internet.

2.5 Origem da rede Tor

O Tor é um programa que protege a identidade e a privacidade dos seus usuários enquanto estão usufruindo do uso da internet, também chamado de “The Onion Router” foi a ideia inicial do Laboratório de Pesquisa Naval dos Estados Unidos, esse projeto recebeu o apoio da Eletronic Frontier Foundation, que é uma

das organizações que dedica-se a defesa dos direitos da internet mais conhecida do mundo, sendo um software de código aberto e está constantemente associado a Deep Web, que é parte da internet associada a conteúdos suspeitos. O Tor foi lançado em Setembro de 2002, elaborado para que as pessoas mantenham o anonimato navegando na rede, mantendo suas informações protegidas, instalando esse software ele oculta a sua identidade na rede, dificultando assim qualquer pessoa de acessar suas informações utilizando uma rede de transmissão de dados que passa por diversas máquinas até chegar nas informações buscadas, confundindo assim aos terceiros mantendo sua privacidade e segurança, além disso o Tor também é capaz de mascarar seu endereço de IP, bloqueando assim que hackers acessem seus dados, pois não permite que as páginas tenham acesso aos dados pessoais dos usuários, mas todo cuidado é pouco, nada é 100% na internet, O Tor é uma opção para proteção na internet muito útil para pessoas bem intencionadas que desejam buscar privacidade e proteção dos seus dados (PEREIRA, 2020)

“Essa rede é constituída por computadores disponibilizados por voluntários ao redor do mundo, permitindo que seus usuários melhorem sua privacidade e segurança na internet” (BARRETO; SANTOS, 2019, p. 24).

> Em 1996, Paul Syverson e outros militares do Laboratório Central da Marinha dos Estados Unidos para Segurança de Computadores, com a ajuda da Darpa (www.darpa.mil), desenvolveram um software livre de rede aberta capaz de estabelecer uma comunicação resistente a ataques e análises dos pacotes de dados trafegados e, ainda, que não permitisse ser descoberta a origem do acesso. Assim nascia o projeto Tor. Sua aplicação baseia-se na utilização de diversos servidores que roteiam todo o tráfego das informações através do que denomina de nós. Para cada novo salto de conexão estabelecido com esse novo servidor, novos nós são criados, até finalmente chegar ao destino pretendido (BARRETO; WENDT; CASELLI, 2017, p. 165).

Diante disso, os criminosos que atuavam no âmbito da realidade física, no qual vivenciamos, passaram a migrar para o ambiente virtual, visando ampliar os horizontes de atuação, afim de passar por cima das autoridades policiais (BARRETO; WENDT; CASELLI, 2017).

“Podemos afirmar, então, que a tendência mundial, no que se refere ao ciberespaço, é instauração de um sistema digital base de toda a tecnologia humana,

que se aplique a todos os ramos de atividade, social ou individual” (RIBEIRO, 2013, p. 27).

2.6 Cracker e Hacker

No ambiente virtual deve-se distinguir a figura do cracker e do hacker. O hacker utiliza-se dos seus conhecimentos de informática para e segurança da rede para proteção e atualização atuando em favor dos menos favorecidos, conhecidos também como white hats (chapéus brancos), quanto aos crackers, conhecidos como black hats (chapéus pretos) para práticas delituosas e condutas antiéticas (BARRETO; BRASIL, 2016).

Apesar dos hackers muitas vezes serem associados a roubo de dados e invasão de sistemas, conforme especialistas os verdadeiros criminosos são os crackers, palavra que deriva do inglês “to crack”, que significa quebrar. O termo hacker descreve a figura de um programador com conhecimento vasto em computação sobre sistemas, mas sem a intenção de causar danos a terceiros, ambos são especialistas em programação e sistemas por isso muitas vezes são confundidos (CASSANTI, 2014).

“Muitas técnicas utilizadas por crackers descaracterizam o pretenso tipo penal. Muitas técnicas, ainda desviam a conduta da descrita no tipo. Muitas condutas protegidas pela tutela penal, não abrangem determinadas técnicas” (JESUS; MILAGRE, 2016, p. 29)

Algumas características dos crackers os definem como criminosos, sendo suas habilidades conhecidas como Carder que trata de um especialista em roubar dados bancários e números de cartão de crédito, contas em banco. O cracker Defacer é um especialista em pichar sites, ou seja deixando mensagem de protesto contra sites, tem também o Spammer que acaba por disseminar correntes de vírus via e-mails, visando roubar e danificar informações dos usuários, já o Phisher é o especialista em aplicar golpes, são conhecedores das falhas dos sistemas, o Phreaker é o especialista que utiliza-se de técnicas para burlar os sistemas de segurança de telefonia, sendo estas algumas das habilidades de um cracker, cujo a finalidade estar em causar danos (CASSANTI, 2014).

Um mundo onde os crackers são mais fortes, a tecnologia revela o poder desses programadores, profissionais, onde utilizam seus poderes para finalidades de causar danos, onde no Brasil, a educação digital passa longe das escolas (JESUS; MILAGRE, 2016).

Em meados de 2013, o Brasil perderia cerca de U$$ 8 bilhões com ataques crackers, roubo de senhas, cartões, além da pirataria, espionagem e claro outros crimes cibernéticos que ainda em 2013 custariam cerca de U$$ 500 bilhões para toda a economia mundial, sendo o Brasil em termos da macrocriminalidade destacando-se como um dos principais alvos dos crackers, sendo o quarto principal alvo, figurando entre os cincos países que tem as empresas hackeadas, cerca de 38 milhões de usuários lesados (JESUS; MILAGRE, 2016).

“Pesquisas sempre revelaram que o Brasil está na rota dos crimes cibernéticos. De acordo com a Polícia Federal, em notícia do ano de 2004, de cada dez hackers ativos no mundo, oito vivem no Brasil” (JESUS; MILAGRE, 2016, p. 23).

Diante do avanço significativo da internet e da tecnologia, vivenciamos o grande avanço dos Crackers e Hackers, sendo o Brasil, um dos principais alvos para prática criminosa virtual, fato pelo qual, nossa legislação está crescendo de velocidade evidentemente inferior ao crescimento criminoso.

2.7 Vírus, Malware e Trojan

O vírus de computador não é uma conduta incriminável, sendo por muitos classificados como condutas incriminàveis na esfera criminal, na verdade está inserido na conduta de provocar ou tentar fazer algum dano a um dispositivo ou fazê-lo funcionar de forma inesperada, logo o vírus não é um comportamento ou conduta com a finalidade de causar danos, sendo técnicas de um sistema como trojan, worm visam comprometer um sistema informático. O phishing scam, a pescaria de senhas, consiste na técnica do agente obtenha vantagem ilícita, induzindo alguém ao erro proporcionando a entrega confidencial de dados da vítima (JESUS; MILAGRE, 2016). “Os vírus são pequenos programas capazes de produzir cópias de si mesmos, porém não podem se autoexecutarem; para começar a agir, precisam que alguém ou algo ou execute” (CASSANTI, 2014, p. 8).

“Em março de 2013, foi revelado um golpe que atingiu 120 mil computadores pessoais gerando um prejuízo de US$ 6 milhões (quase R$ 12 milhões) por mês. O golpe foi identificado como Chameleon botnet” (CASSANTI, 2014, p. 34).

> Vírus, worms e phishing scams são conhecidos coletivamente como malware (código malicioso). Eles se aproveitam tanto de falhas em softwares quanto de deslizes dos usuários, como entrar em sites infectados ou abrir anexos de e-mail. Os vírus são programas que são passados de usuário para usuário (através da Internet ou através de uma mídia portátil, como um pendrive) e que levam algum tipo de carregamento para comprometer o funcionamento normal de um computador, fornecer um ponto de acesso oculto ao sistema, ou copiar e roubar informações pessoais. Os worms não exigem que o usuário passe o programa para outro usuário, eles podem se autorreplicar por meio de vulnerabilidades conhecidas e se propagam pela Internet sozinhos. Os phishing scams tentam enganar um usuário da Internet para que ele forneça informações, como números de contas bancárias e códigos de acesso, criando mensagens de e-mail e sites falsos que fingem estar relacionados a negócios legítimos, como o seu banco, por exemplo (CLARKE; KNAKE, 2015, p. 85).

A respeito do Cavalo de Tróia, também conhecido como Trojan, seu nome surgiu devido à história da guerra de troia e fulminou na destruição desta, um grande cavalo de madeira, oferecido supostamente como pedido de paz por parte dos gregos, sendo presente para o rei, os troianos levam para dentro das muralhas da cidade, sendo a noite enquanto todos dormiam revelou-se uma armadilha e os soldados gregos esconderam-se dentro da escultura de madeira, saindo todo o exército para dentro da cidade, referente ao Trojan, simula alguma funcionalidade útil, e pode conter um programa escondido que danifique os computadores, consistindo na abertura de portas pelo usuário possibilitando invasão ou roubo de senhas, onde são práticas comum na internet. Os dois tipos mais comuns de Trojans, são os Keyloggers, que são utilizados para roubar senhas, e os Backdoors são arquivos que possibilitam aberta de portas para invasão, diferente dos Vírus e Worms, eles não se autocopiam, não necessitam infectar outros programas para executarem suas tarefas, são autônomos necessitando apenas serem executados, instalam-se juntamente com os arquivos, são potencialmente mais perigosos e arquivos podem não ser identificados pelo antivírus como ameaças ou de origem duvidosa, devem ser vistos com cautela, pois esse trojan visa causar grandes danos (PEREIRA, 2008).

“No mundo virtual a ideia é a mesma: um cavalo de troia é um arquivo aparentemente inocente entregue pela porta da frente, mas que contém um elemento malicioso escondido em algum lugar dentro dele” (CASSANTI, 2014, p. 32).

Um rootkit, também é um trojan, busca esconder softwares de segurança dos usuários utilizando de diversas técnicas avançadas de programação, o cracker utiliza-se dessas técnicas com a finalidade dos usuários não saberem que estão com seu sistema comprometido, podendo ser instalado tanto localmente como remotamente, boa parte dos antivírus não conseguem detecta-los e os usuários seguem com esses programas maliciosos de forma camuflada nas máquinas (CASSANTI, 2014).

Ransomware, é um tipo de malware que bloqueia o sistema e geralmente depois de instalado exige resgate, o programa conseguirá criptogragar o disco do computador ou bloquear o acesso a vítima ao sistema, são instaladas através de uma vulnerabilidade, quanto abertura de e-mails de phishing ou pelo acesso de sites maliciosos, são detectados facilmente por antivírus (CASSANTI, 2014).

“Spyware são programas espiões cuja função é coletar informações sobre o usuário e seus costumes na internet com ou sem o seu conhecimento” (CASSANTI, 2014, p. 30).

Um malware pode não ser um vírus que cause algum dano ou capture informações, malware pode significar gênero, código malicioso, mas, contudo, não significa que é uma conduta penalmente imputável (MILAGRE; JESUS, 2016). Sendo “O termo malware é a contração de malicious software (programa malicioso) e identifica qualquer programa desenvolvido com o propósito de causar dano a um computador, sistema ou redes de computadores” (CASSANTI, 2014, p. 29).

“Um worm é um programa similar a um vírus, com a diferença de que ele se autopropaga através de uma rede de computadores, sem ajuda de uma pessoa” (CASSANTI, 2014, p. 36). O Worm é um malware mais perigoso que um vírus comum, pois ele tem uma propagação de maneira muito rápida, assim que acaba por contaminar um computador, o programa malicioso acaba por tirar cópias de si mesmo em diferentes locais do sistema e, portanto, acaba por se espalhar por outras máquinas, sendo através da internet, mensagens, conexões locais ou portas USB, sendo o objetivo principal roubar os dados ou senhas dos usuários. Os Worms

infectam os computadores através de brechas do sistema podendo ser transmitidos em segundo plano na forma de um arquivo corrompido ou acessar uma página suspeita, enquanto não for neutralizado esse Worm se espalhará atingindo grandes empresas ou roubar dados confidencias e sigilosos dos usuários (STIVANI, 2018).

Os vírus de computadores são engenhosos, são diversos tipos de vírus espalhados pela rede e que tem avançado significativamente, assim como os crackers e hackers, que utilizam desses mecanismos como evidenciamos, fato pelo qual, devemos estar em uma evolução gradual com nossa legislação penal, buscando adequação virtual, trataremos desse assunto em específico no terceiro capítulo, onde aprofundaremos essa análise.

No próximo capítulo serão analisados os tipos penais e os crimes cibernéticos recorrentes em nossa sociedade aplicando nosso Código Penal Brasileiro, aproximando então a tecnologia da informação com relação ao direito na era de crimes digitais.

3 DOS CRIMES CIBERNETICOS

Os crimes tecnológicos são aqueles que estão relacionados com o uso de tecnologia, sendo por computador, internet, caixa eletrônicos, cujo sua forma inovadora apesar de estar relacionado aos crimes virtuais, cibernéticos, praticados pela internet, usufruem da esfera digital, mas concretizados os delitos trazem efeitos para o mundo real (BARRETO; BRASIL, 2016).

Nosso Código Penal 1940, é dividido em duas partes, sendo a primeira denominada parte geral, e a segunda parte do Código, é denominada como parte especial e define e os crimes propriamente ditos, tratando os específicos de crimes contra o patrimônio, crimes contra a dignidade sexual. (BRASIL, 1940).

O crime, então, é uma conduta não permitida legalmente, cuja a punição é a mais severa de todas, pois afeta diretamente a liberdade do indivíduo. Trata de uma contravenção penal, uma infração de natureza penal, porém não tão grave, também chamada de infrações penais de menor lesividade, tais punidas com menos rigor (BOMFATI; KOLBE JUNIOR, 2020).

Os crimes cibernéticos também são conhecidos como cibercrimes, crimes de informática, crimes eletrônicos. Trata-se de condutas ilícitas no qual os criminosos através de um equipamento eletrônico, podendo ser via telefone, notebook, tablet usando meios ilegais para alcançar seus objetivos (BOMFATI; KOLBE JUNIOR, 2020). O crime, então é uma conduta não tipificada legalmente, cuja punição é a mais severa, pois está diretamente ligada a liberdade do indivíduo, por sua vez uma contravenção penal, porem por não ser tão grave, são infrações penais de menor lesividade, ou seja, punidas com menos rigor:

> Art 1º Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente (BRASIL, 1941, http://www.planalto.gov.br).

Assim, entende-se que o crime se trata de uma conduta, ação ou omissão, cuja a punibilidade afeta diretamente a liberdade do infrator.

3.1 Classificação

Os crimes cibernéticos são classificados e conceituados como “próprios, impróprios, mistos e mediato ou indireto. Considerando que virtual é algo que não existe na realidade, sendo algo em potencial, cibernético refere-se à teoria de mensagens e dos sistemas de processamento de mensagens, sendo que os crimes digitais são todas as condutas previstas em lei, que sejam punidas com pena na esfera criminal e que nesta prática, envolva os meios tecnológicos, seja porque a conduta destina-se contra os sistemas de informatização e dados por isso são dois tipos de classificações dos crimes digitais, sendo os próprios e os impróprios. Crimes digitais próprios ou puros trata-se de condutas proibidas por lei em que estão sujeitas a pena criminal no qual se voltam para os sistemas informáticos e de dados, também conhecidos como delitos de riscos, exemplos desses delitos próprios são o hacking, cujo acesso não é autorizado, a disseminação de vírus e a complicação do funcionamento de sistemas. A respeito dos crimes impróprios também chamados de mistos, são também condutas proibidas por lei que estão sujeitas as penas criminais que se voltam contra os bens jurídicos que não sejam tecnológicos, tais protegidos pela legislação, como a vida, liberdade, patrimônio. São exemplos de crimes impróprios os contra honra praticada na internet, troca ou armazenamento de imagens com conteúdo com pornografia infantil, estelionato até o homicídio (CRESPO, 2015).

Impuros ou próprios são aqueles que o dispositivo tecnológico é utilizado como meio para a prática delituosa, operando a sua execução ou resultado, apenas o veículo que está o crime praticado diretamente ligado a tecnologia, sendo totalmente adequado as figuras típicas do Código Penal e leis penais especificas. Os puros que usam os meios informatizados, banco de dados ou arquivos são atacados pelos criminosos após descobertas as vulnerabilidades, pode ser que a vítima baixe um Cavalo de Tróia e nesse caso, aproveitam-se das falhas de segurança para conseguirem atacar (BARRETO; BRASIL, 2016).

Visto a situação dos cibercriminosos no Brasil é extremamente preocupante, pois uma vez que no campo virtual os lucros das atividades ilícitas são altíssimos, ressaltando-se o fato que nossa legislação, não é suficiente eficaz para combater esses criminosos e também contra a impunidade que se espalha cada vez mais na

rede, condutas ilícitas na internet estão atraindo quadrilhas que antes atuavam em crimes como roubo a bancos e tráfico de drogas (BARRETO; BRASIL, 2016).

Os criminosos estão usando informações no âmbito virtual para praticar delitos, aproveitando-se das fotografias das vítimas, parentes, telefones, locais frequentados, hábitos como fonte de informação para auxiliar na pratica delitiva como é o caso do Facebook por exemplo, uma rede social que permite aos usuários divulgarem o local certo em que se encontram, fotos, vídeos e informações pessoais, endereço, números de telefones facilitando as ações criminosas, tais quais podem utilizar-se dessas informações verídicas para formatar documentos falsos, cadastros falsos em lojas virtuais (BARRETO; WEDNT; CASELLI, 2017).

Portanto os crimes cibernéticos, abertos ou crimes digitais impróprios, crimes contra honra, racismo, furto mediante fraude, entre outros que os criminosos utilizam dos recursos virtuais para pratica-los, a respeito dos crimes exclusivamente cibernéticos, ou digitais próprios, pode-se citar os tipos penais previstos nos Estatuto da Criança e do Adolescente, meio a pornografia infantil por via do sistema informático (WEDNT; LOPES, 2014).

Visto que os crimes cibernéticos abrangem os ramos próprios e impróprios verificaremos as tipificações e as leis pertinentes a estes crimes neste capítulo.

3.2 Estelionato

Os crimes cibernéticos atingiram um marco de 77 mil brasileiros, com prejuízo anual de mais de R$ 104 bilhões, segundo levantamento da Norton, mas deve ser visto com cautela, pois são variáveis de empresa para empresa. De acordo com Symantec, os crimes cibernéticos geraram um prejuízo de R$ 1,5 bilhões, sendo R$ 900 milhões em fraudes bancárias. Entre os crimes mais comuns na internet estão o estelionato, pornografia infantil, sendo praticada por meio de vírus de computador ou malware, invasão de perfis de redes sócias, como o crime informático, o Direito Penal já protege certos bens jurídicos, fato que dados de segurança e sistemas e rede informáticos necessitam de uma proteção especifica (JESUS; MILAGRE, 2016).

No crime de estelionato, a fraude é utilizada como meio de obter o consentimento da vítima, que conforme iludida pelo infrator e por sua ingenuidade acaba por entregar de forma voluntaria os bens sediados para o agente, utilizar-se

dos dados bancários das vítimas sem a devida autorização afim de fazer empréstimos, também configura-se o crime de estelionato, causa de fraude no e-commerce, ou seja, a venda pela internet, diante aos bens que de fato são inexistentes, consumando-se pela obtenção de vantagem indevida por parte do criminoso, após ser realizado um pagamento ao bem que a vítima pensava existir, o crime é consumado na agência bancária do suspeito (BARRETO; BRASIL, 2016).

Dentre os crimes informáticos impróprios praticados na Internet, um dos destaques e maior incidência é o crime de estelionato (art. 171, do Código Penal):

> 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 um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155 (BRASIL, 1940, http://www.planalto.gov.br).

O estelionato difere-se do furto mediante fraude, previsto no Art. 155, parágrafo 4°, inciso II, do Código Penal (1940), o furto mediante fraude nos meios tecnológicos ocorre de duas maneiras falsificação e clonagem de cartão bancário ou pela invasão de contas bancárias na internet, havendo a subtração de valores, no estelionato a vítima com sua vontade ludibriada entrega o bem ao criminoso, e já no furto há diminuição do monitoramento, descuido, mediante técnicas fraudulentas, possibilitando o suspeito subtração do bem (BARRETO; BRASIL, 2016).

Se alguém invade um dispositivo informático de um banco e transfere indevidamente dinheiro para sua conta, estará cometendo dois delitos distintos: o de invasão de dispositivo informático e o furto; o primeiro, crime informático, o segundo, patrimonial. Como visto o mundo virtual da internet tem seus prós e contras, e com isso abre possibilidade de muitos criminosos praticarem as fraudes, referente a crimes dessa natureza, por tratar de baixa incidência da eficácia na legislação referente a estes delitos, temos um número recorrente e cada vez maior de crimes desta espécie no Brasil.

3.3 Cyberbullyng

Sendo o cyberbullyng nada mais que uma condição da disposição humana, seu exame deve vir por meio das ciências que tratam do agir humano, pode-se definir então cyberbullyng, como um conjunto de atos agressivos, ocorridos em espaços virtuais de interação e dispositivos de tecnologia, praticados por um ou mais indivíduos contra alguém que está em posição de certa inferioridade em relação ao agressor. O foco que está no bully, aproveita-se de uma suposta “superioridade” para dirigir ataque à honra e à imagem de outrem. Dentro do espaço amplo e diversificado da internet, sendo na maioria das vezes atrelado a jovens, e estudantes sendo uma relação conflituosa (RIBEIRO, 2013).

O caráter de interconexão entre os grupos formados numa rede social, possibilita que indivíduos de grupos diferenciados, tenham acesso, sendo suscetível e mais fácil a invasão de intimidade para formação de um elo de poder, sendo o bullyng e o cyberbullyng, necessário uma motivação, que deve ser analisado caso a caso, podendo ser impopularidade no meio virtual, como tantos outros motivos, sempre há uma exclusão interpretada como um tipo de inferioridade e o agressor por uma suposta “superioridade”. Entendido assim o cyberbullyng como ato ilícito que fere aos direitos porque representa uma conduta contraria a da lei (RIBEIRO, 2013).

Nesse sentido, a Constituição da República, (1988) consagrou-o no art. 5º, inciso XXXIX, que traduz: “não haverá crime sem lei anterior que o defina, nem pena sem prévia cominação legal” (princípio da legalidade e princípio da anterioridade (BRASIL, 1988, http://www.planalto.gov.br).

Partindo desse ponto, os crimes existentes no cyberbullyng, como modelo de condutas praticadas estão a injúria, difamação, calúnia, ameaça, constrangimento ilegal, extorsão, falsa identidade entre outros, quanto aos meios das ações são remotamente virtuais, principalmente ligada à troca de mensagens, diante dessas formas penais dos cyberbullyng em que será elencado. O cyberbullyng, é um conjunto de agressões nas quais a vítima é considerada de um estrato inferior ao do ofensor, em que os meios usados podem ser a violência, a ameaça, como ocorrência do constrangimento, trazendo o crime da esfera virtual para a esfera concreta os danos praticados (RIBEIRO, 2013).

Visto a condição valorativa do homem, e da maneira que esta é sentida pelo ser humano, no qual traduz honra, dignidade como um todo, conforme a Constituição Federal:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
> III - a dignidade da pessoa humana;
> Também devemos tomar nota dessa dignidade que deve ser posta esse valor como objetivo da República Federativa do Brasil (BRASIL, 1988, http://www.planalto.gov.br).

Temos assim um rol de proteção e direitos, mas nada de uma legislação específica para tipificação dos crimes de cyberbullyng, sendo a conduta característica no ataque à honra e à imagem, no qual verificaremos a seguir no próximo subcapítulo a ser aprofundado.

3.4 Crimes contra honra

Com decorrer do tempo e da evolução da internet é indiscutível crescimento dos meios de comunicação neste aspecto os usuários acabam se expondo de alguma forma. Essa modalidade de crimes é mais recorrente nos dias atuais, pois os criminosos são incentivados pela grande possibilidade de anonimato das redes sociais e sites que estão sempre em constante mudança, dificultando as investigações e as provas relacionadas a estes crimes, além disso a possibilidade de criar perfis falsos e as possibilidades de não identificar-se, facilitam os criminosos para estas práticas, portanto diante dos crimes contra a honra, sendo na esfera virtual ou não, resta o Código Civil o dever de reparar o dano e o Direito Penal, investigação e punição dos devidos infratores e cumprimento do devido processo legal (CHIMENEZ, 2017).

O Art. 953 do Código Civil, prevê que a indenização por injuria, difamação ou calunia, consistirá na reparação do dano, resultado ao ofendido, não podendo provar o prejuízo dano material, caberá ao juiz fixar o valor equitativamente, conforme caso a caso, nesse sentido a Constituição Federal (1988), no artigo 5°, inciso X, assegura o direito a indenização por dano material ou moral ao determinar que 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 (WEDNT; JORGE, 2013).

Também temos a Calúnia, escrita e tipificada no Artigo 138 do Código Penal (1940):

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa
> Crime, tipicamente comum no meio virtual, com atenção ao parágrafo primeiro
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga
> § 2º - É punível a calúnia contra os mortos (BRASIL, 1940, http://www.planalto.gov.br).

O significado da honra está diretamente ligado com o princípio e o valor da dignidade humana da pessoa humana, consiste em atributos morais, físicos ou intelectuais da pessoa, que está atrelado a autoestima e reputação, a honra pode ser subjetiva e objetiva, quando tratamos da autoestima a honra é subjetiva e quando falamos da reputação está ligada a honra objetiva. A honra objetiva é compreendida como o juízo que terceiros fazem a respeitos dos atributos de alguém e a honra subjetiva do juízo que determinada pessoa faz a respeito de seus próprios atributos (LATIF, 2007).

O crime de difamação é o fato de imputar a alguém qualquer adjetivo que ofenda a reputação do indivíduo determinado, sendo este crime está ligado diretamente com a honra objetiva, por meio de um terceiro que é o sujeito ativo do crime desonrando, diante da reputação do indivíduo perante a sociedade (CHIMENEZ, 2017).

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

O crime de injuria busca defender a honra subjetiva, trata de imputação de qualidade negativa a alguém, contem fatos genéricos e vagos para ser configurada o crime de injuria, o sujeito passivo deve ter a capacidade de fazer o juízo de valor sobre si mesmo, a injúria qualificada se existe elementos a raça, cor, etnia, religião

ou condição de pessoa idosa ou portadora de deficiência conforme parágrafo § 3, já a injuria real que trata o parágrafo § 2, quando a injúria consiste em violência ou vias de fatos, que por sua natureza ou meio empregado, se considerem aviltantes, a constatação que as atitudes foram aviltantes pode decorrer da natureza um tapa no rosto ou do meio empregado arremesso de excrementos. No caso de injúria real, será pública e incondicionada se a lesão for grave ou gravíssima, e condicionada à representação, se for leve (LATIF, 2007).

Já a injúria trata de crime contra a honra, Código Penal de 1940:

> 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, http://www.planalto.gov.br).

Os crimes contra a honra são intimamente ligados a propagação da informação pela internet e outros meios digitais, um comentário pejorativo, discussão ou xingamento, podem passar despercebidos no calor do momento, mas que trazem aspectos do meio digital para o mundo real. Esse xingamento ficará registrado indefinitivamente na rede, até mesmo após ser retirado do local onde foi posto, nada impedindo que um terceiro capture e espalhe essa postagem novamente, sendo crime muito comum, diante das redes socais e que fere a honra da pessoa atingida (BOMFATI; KOLBE JUNIOR, 2020).

Os crimes contra honra, calunia, difamação e injúria, no qual verificamos, deverá ser oferecido mediante representação da vítima ofendida, de acordo com o Art. 145 do Código Penal de 1940, pois trata de crime de ação penal condicionada à representação da vítima, sendo sua manifestação imprescindível para seguimento da ação penal.

3.5 Crimes contra a dignidade sexual

O termo sexting, é a união de duas palavras em inglês “sex” (sexo) e texting (envio de mensagens), no qual consiste em envio de conteúdos sexuais, envolvendo principalmente fotos ou vídeos, produzida pela própria pessoa, no qual consente em seus atos, assim enviando esses conteúdos para terceiros, ou seja, outras pessoas através de celular ou para grupos, redes sociais, e-mails, foi criado por jovens americanos, ganhando cada vez mais popularidade entre os jovens no Brasil, na medida que a tecnologia avança, as redes sociais e aplicativos acabam por colaborar para estas práticas (CASSANTI, 2014).

Hoje com a convivência com a internet, a admiração do corpo, onde as pessoas estão frequentemente expondo-se, além da invasão de privacidade, que um problema sério, neste caso em tela, as pessoas estão se exibindo de maneira, no qual estão revelando toda sua intimidade, acontecendo a chamada “pornografia por vingança”, no qual é enviada foto de nudez ou vídeo, utilizados para ofender a reputação, onde pode ser armazenados em nuvens, podendo ser alvo de crackers, vindo a ser roubado, deve-se proteger as informações intimas e pessoas evitando assim ser alvo de criminosos cibernéticos (BARRETO; BRASIL, 2016).

Diante da infiltração do agente, obedecerá a Lei, exigindo-se prévia e circunstanciada autorização judicial, e será estabelecido os limites de investigação, com essa nova Lei 13.441/17, ainda que no exercício do agente, não possui caráter voluntario, pois decorre dos meios virtuais, não expondo-se fisicamente e integralmente a risco eminente, sendo que esta Lei, tipifica que a filtração do agente deve-se dar apenas se não houver outros meios de obtenção de provas disponíveis, esta Lei, altera o Estatuto da Criança e do Adolescente, criando a figura do agente infiltrado na internet, investigando crimes contra a liberdade e dignidade sexual de crianças e adolescentes, sendo uma infiltração cibernética, trazendo significativas mudanças no mundo real na parte de investigação, especialmente por não colocar a integridade dos agentes em risco (JORGE, 2018).

Diante da infiltração do agente no meio virtual, este não corre riscos da sua integridade física, uma vez que desenvolve essa infiltração por meio da internet. Conforme a Lei 13.441/17, nos termos do inciso II, do artigo 190-A, da Lei nova, o procedimento poderá ser provocado pelo Ministério Público, por meio de

requerimento, ou pelo delegado de polícia, através de representação (BRASIL, 2017, http://www.planalto.gov.br).

> Artigo 190-A, inserido no ECA pela nova Lei, a infiltração virtual de agentes só poderá ser utilizada como técnica investigativa para a apuração dos crimes descritos no dispositivo em questão, ou seja, aqueles previstos nos artigos 240, 241, 241-A, 241-B, 241-C e 241-D, todos do Estatuto protetor da criança e adolescente, e artigos 154-A, 217-A, 218, 218-A e 218-B do Código Penal. Tendo em vista o caráter excepcional do procedimento, entendemos que estamos diante de um rol taxativo de crimes que autorizam esta medida (JORGE, 2018, p. 39).

Como forma de aumentar a celeridade e eficácia das investigações foi criada a figura do agente infiltrado, sendo importante ao delegado responsável esteja frente ao inquérito policial, para que o poder Judiciário possa cooperar conjuntamente com as operadoras de telefonia com a finalidade de permitir em tempo real, pesquisa cadastrais e aos bancos de dados, também que ao magistrado autorize esse agente a proceder com apreensão de documentos de qualquer natureza e realizar filmagens, escutas, tratando-se assim de uma ação controlada no qual a justificativa é a busca de evidências e provas sobre um interesse maior (JORGE, 2018).

A respeito da utilização de criança ou adolescente em cena pornografia ou de sexo explícito, o sujeito ativo seria qualquer pessoa de acordo com o parágrafo § 1º, cuja a pena é aumentada em até 1/3, se o sujeito ativo estiver se enquadrando nas condições estabelecidas no § 2º. Já o sujeito passivo seria a criança ou adolescente que se enquadraria neste rol estabelecido (ANDREUCCI, 2018).

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
> § 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
> I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
> II– prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
> III– prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento (BRASIL, 1990, http://www.planalto.gov.br).

Compreende com o uso da internet, pessoas com a finalidade de aliciar as crianças ou adolescentes para realizarem atividades sexuais ou de forma que exponham estas de uma forma pornografia. Os casos de pornografia infantil no Brasil, dominam as denúncias feitas na internet, pois só de janeiro de 2006 a outubro de 2012, cerca de 40,5% das denúncias postas, foram supostamente encontrados arquivos com dispositivos desse conteúdo pejorativo (CASSANTI, 2014).

A consumação do ato ilícito previsto no Art. 241 do Estatuto da Criança e do Adolescente, conforme exposto pelos autores Barreto e Brasil afirmam (2016, p. 167) “ocorre no ato de publicação das imagens pedófilo-pornográficas, sendo indiferente a localização do provedor de acesso onde tais imagens encontram-se armazenadas, ou a sua efetiva visualização pelos usuários”.

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> Sujeito ativo: qualquer pessoa (BRASIL, 1990, http://www.planalto.gov.br).

A pedofilia é uma forma doentia de satisfação sexual, tratando de uma perversão, um desvio sexual que leva o indivíduo adulto sentir atração sexualmente por crianças, tem como base a Classificação de Doenças da Organização mundial de Saúde, definindo a pedofilia como preferência sexual entre meninos ou meninas ainda na fase pré-pubere ou início da puberdade. Sendo assim, os pedófilos podem se transformarem em agressores, assim em trocarem suas fantasias sexuais por atos reais, porém não são todos que chegam a essa atitude, pois nem todos que agridem sexualmente as crianças ou adolescentes são necessariamente pedófilos, todavia no âmbito jurídico a pedofilia é conceituada como abuso sexual de crianças e adolescentes, tendo um rol de crimes no Estatuto da Criança e do Adolescente e no Código Penal (COUTO, 2015).

Quanto a pornografia infanto-juvenil na internet, o Estatuto da Criança e do Adolescente é bem específica em seus Art. 240 a 241-E, mesmo quando imagens são trocadas ou disponibilizadas, gratuitamente, em grupos como WhatsApp, há crime, está tipificado no Art. 241-A, em seus parágrafos traz a tipificação penal de representante de provedor de internet (BARRETO; BRASIL, 2016).

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (BRASIL, 1990, http://www.planalto.gov.br).

Conforme a Lei 11.829/08, no qual alterou o Estatuto da Criança e do Adolescente, conforme o artigo 241-B, representou grande avanço, pois definiu algumas condutas referentes aos crimes de pornografia infantil em âmbito virtual, e também criou condutas que antes não estavam tipificadas, como armazenar fotografia ou vídeo, registros que contenham cena de sexo explícito ou pornografia com crianças ou adolescentes, sendo os possuidores destes arquivos não podiam ser penalizados em razão da inexistência de figura típica, visto que é fundamentalmente importante as figuras típicas penais para que seja possível penalizar estes criminosos (WEDNT; JORGE, 2013).

> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
> § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
> I – agente público no exercício de suas funções;
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
> § 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido (BRASIL, 1990, http://www.planalto.gov.br).

Temos assim no código penal os crimes contra a dignidade sexual, possuindo assim um capítulo específico acerca dos crimes sexuais contra vulneráveis, O

legislador trouxe assim um conceito de cena de sexo explícito ou pornográfica, compreendendo qualquer situação que envolva crianças ou adolescentes em atividades sexuais. É típica a conduta de fotografar cena pornografia enquadrando-se o Art. 241-B do ECA, e o armazenamento envolvendo criança ou adolescente em seu Art. 240 do Estatuto da Criança e do Adolescente, tendo um rol de proteção do Art. 227 da Constituição Federal estabelece o dever não sendo apenas da família mas da sociedade e também do Estado, ainda no parágrafo 4° do mesmo dispositivo constitucional “a lei punirá severamente o abuso, a violência e a exploração sexual da criança e do adolescente” (COUTO, 2015).

Ainda no que tange o Estatuto da Criança e do Adolescente (1990), nos termos de simulação de pedofilia consta em seu Art. 241-C.

> Art.241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual.
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, pública ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo. (BRASIL, 1990, www.planalto.gov.br).

Também referente aos crimes exclusivamente cibernéticos temos o Art. 241-D, do ECA da Lei 8.069/90, que trata segundo Wednt e Jorge (2013, p. 38) “Um exemplo é o crime de aliciamento de crianças praticado por intermédio de salas de bate papo na internet, previsto no art. 241-D do Estatuto da Criança e Adolescente”.

O Art. 241-E, trata de forma explicativa os crimes previstos nos Art. 240, Art. 241, Art. 241-A a Art 241-D do ECA, trazendo esse dispositivo de uma forma mais extensiva, não podendo ser interpretado de forma restritiva, não limitou a extensão ao conceito de cena de sexo explícito ou pornográfico, compreendendo qualquer situação que envolva crianças e adolescentes (COUTO, 2015).

> O Art. 241-E. define que a expressão “cena de sexo explícito ou pornográfica” compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais, ou seja, deve haver o dolo específico (BRASIL, 1990, www.planalto.gov.br).

Diante da análise da investigação da pornografia infantil, não se dá apenas baseada em fotos, disponíveis na internet, mas sim com seu conteúdo, pois o usuários tem por vezes dezenas de arquivos com estes conteúdos, armazenados em seus computadores, ou dispositivos informáticos, repassando por sites, ou e-mails anexados, protegidos com senha, devendo a investigação em curso ser precisa, e para isso deve dar cumprimento à apreensão desses conteúdos sendo imprescindível o exame pericial, verificando os dispositivos de histórico, navegação e pesquisa, compartilhamento de pastas ou arquivos até mesmo armazenamento remoto ou virtual (BARRETO; BRASIL, 2016).

A requisição de ordem judicial para obtenção de qualquer informação relativa a um crime cibernético é uma questão que atrasa e representa excesso de burocracia, acabando prejudicando e retardando os esclarecimentos desses tipos de delitos (WEDNT; JORGE, 2013). Trazendo assim, maiores complicações e dificuldades para deixar o processo mais célere e eficaz no tocante dos crimes cibernéticos.

Trazendo os crimes de importunação sexual e divulgação de cena de estupro com a Lei 13.718/2018, alteramos o nosso Código Penal, importante de ser ressaltado com advento do Art. 218-C, com a divulgação de cena de estupro e cena de estupro de vulnerável em cena de sexo ou pornografia.

> 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 (BRASIL, 1940, http://www.planalto.gov.br).

Mas de fato, a legislação pertinente aos crimes de dignidade sexual, avançou de forma significativa, a figura do agente infiltrado é fundamental para os procedimentos investigatórios, mesmo assim, os crimes sexuais de pornografia de crianças e adolescentes tem avançado na sociedade, a legislação atende de forma regular e adequada a esta criminalidade, pois realmente tem uma tipificação penal própria para combate de forma eficaz, devendo assim, a eficácia ser complementada com um procedimento célere de investigação, e autonomia, também quanto aos meios de provas deve ser buscada de maneira rígida e incessante, sempre na forma

da lei, buscando assim, com rigor a devida punição desses criminosos que ainda, tem números altíssimos no Brasil, sendo um dos crimes mais praticados na internet.

3.6 Racismo Virtual

A principal diferença consiste no crime de racismo em ofensa a toda coletividade indeterminada, sendo considera inafiançável e imprescindível está previsto na Lei 7.716/89, o crime de injúria racial está prevista no Código Penal no parágrafo §3 do art. 140, que consiste na utilização de elementos referentes a raça cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência com pena de reclusão de um a três anos e multa (BRASIL, 1940, http://www.planalto.gov.br).

Conforme a Constituição Federal (1988), temos tipificado no inciso XLII, a respeito da pratica do crime de racismo:

> 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:
> XLII - a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei (BRASIL, 1988, http://www.planalto.gov.br).

Também no tocante constitucional, temos a tutela no Art. 3, inciso IV, que no qual elenca sobre as formas de discriminação “promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação”. (BRASIL, 1988, http://www.planalto.gov.br).

A internet possibilita as mais variadas possibilidades crimes, uma manifestação racista verbal nem sempre é compartilhada por muitas pessoas mas em razão disso quando é ocorre na internet a repercussão é muito maior, deve-se investigar se o criminoso está agindo de maneira individual ou participa de um grupo de organização criminosa, esse tipo de crime em específico envolve imagens, comentários ou vídeos que atinjam a cor, raça, religião conforme a Lei 9.459/1997, além disso o crime de racismo é inafiançável, imprescritível e sujeito a reclusão. Ocorrendo essa discriminação em uma rede social ou um blog, site, fica mais fácil identificar e localizar os computadores desses criminosos (WEDNT; JORGE, 2013).

Sendo o crime de injuria ligado diretamente a honra da pessoa determinada, sendo prescritível em um prazo de oito anos. Injuriar é ofender a dignidade de alguém em virtude de sua raça, cor ou religião por deficiência ou idade avançada, trata-se de ação penal pública condicionada à representação do ofendido. No crime de racismo ação penal é publica incondicionada, cabendo sua iniciativa exclusiva ao Ministério Público, pois se houve a ofensa direcionada a coletividade e não a uma pessoa determinada (D'URSO, 2016).

Obviamente, o racismo está disseminado em nossa sociedade, alastrando-se cada vez mais a pratica do racismo, é uma prática de menosprezar, de denigrir a imagem das pessoas, pela sua cor, raça, cultura, religião uma discriminação pelas características raciais, sendo extremamente importante, fazer as denúncias pertinentes a essa criminalização, e certamente a penalização das pessoas que ainda praticam esse tipo de crime.

Conforme o Art. 1 da Lei 7.716 (1989), "Serão punidos, na forma desta Lei, os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional". (BRASIL, 1989, http://www.planalto.gov.br).

No próximo capítulo, será abordado a eficácia dos procedimentos de investigação e meios de provas para combater os crimes cibernéticos, e também tratar legislação exclusivamente cibernética, diante do avanço da nossa atual legislação para combate dos crimes virtuais.

4 INVESTIGAÇÃO E PROVAS DOS CRIMES CIBERNÉTICOS

No presente capítulo será abordado a legislação específica dos crimes cibernéticos, visando os mecanismos de investigação e provas, direitos e garantias dos usuários na internet e também análise da legislação jurídica para amparo, proteção de dados destes usuários, além da cooperação internacional entre países para colaboração dos crimes virtuais.

Diante da relação da perícia computacional, sendo de suma importância para investigações do âmbito criminal cibernético com objetivo de compreender os fatos que ocorreram, utiliza-se as técnicas de aplicação das principais etapas no qual já são tratadas da forma forense como identificação, coleta, exame, análise e resultados que foram obtidos, sendo a principal ideia buscar indícios que o cibercriminoso possa ter deixado para trás, ou seja rastros no sistema, podendo ser um computador, um pen-drive, sendo a coleta de informações fundamental para o reconhecimento das evidências, também é muito importante a forense computacional nas investigações de vários crimes como tráfico de drogas e homicídios, sendo ao final encaminhamento dos quesitos que foram investigados pelo perito (WEDNT; JORGE, 2013).

Uma das dificuldades da perícia é em relação de um computador utilizado pelo criminoso, encontrar-se em um servidor que está localizado em outro país, sendo que o papel da investigação da pericial forense computacional é dificultada em virtude desses fatos e também da demora que e diante da impossibilidade de obter informações para investigação criminal, e tratando que o Brasil não assinou a convenção de Budapeste, além da dificuldade que encontramos para tirar do ar sites relacionados aos provedores estrangeiros ou que preste as devidas informações, prejudicando as investigações que deviam ser totalmente céleres, para que os criminosos respondam pelos crimes praticados, mas muitas vezes acabam beneficiado o cibercriminoso, que sabe das dificuldades da legislação no tocante a estes crimes em relação a impunidade acabam aproveitando-se para pratica desses delitos cibernéticos (WEDNT; JORGE, 2013).

De fato, é necessário uma legislação pertinente aos crimes cibernéticos, condizendo com a realidade atual que vivenciamos, a Justiça brasileira tem conseguido ainda que a passos lentos, avançar nesse quesito, diante do vasto e

exponencial crescimento e a diversidade do mundo da internet, em que muitos visam obter ou ganhar alguma vantagem cometendo crimes, sendo na realidade um problema de alcance mundial, colocando a liberdade e a segurança em uma linha tênue, infelizmente é tratada como terra sem lei, e de difícil investigação e responsabilização pelos delitos praticados nesse mundo cibernético (BOMFATI; KOLBE JUNIOR, 2020).

Os órgãos investigativos e Judiciários ainda carecem de uma preparação adequada para lidar com essa criminalidade, pois como a tecnologia e a internet avançaram de forma acelerada nas últimas décadas, frete ao franco desenvolvimento investigativo dos órgãos federais, estaduais e municipais, ainda existem agentes despreparados, sem conhecimento sobre o desenvolvimento dessas novas tecnologias, desconhecimento relacionado ao cibercrime da internet, falhas que acabam deixando a sociedade mais vulnerável. A preparação desses agentes deve-se dar de forma urgente para que possa lidar com essa nova tecnologia, principalmente envolvendo essa área jurídica ou pelo menos noções básicas de tecnologia, prestando assim maior contribuição e colaborar de forma produtiva para o combate do mundo organizado de crimes que ocorrem na internet, devendo estruturar-se as polícias frente a esta persistente luta que ainda tem muito para evoluirmos e avançarmos (BOMFATI; KOLBE JUNIOR, 2020).

Conforme visto, a capacitação policial deixa a desejar, mas também o Ministério Público e o Judiciário, representando grande desafio para todos nós, pois na medida que impede a punição desses cibercriminosos, consequentemente causando a impunidade desses agentes (WEDNT; JORGE, 2013).

> Nestes termos evolutivos e preocupantes, essas novas formas de praticar crimes representam um grande desafio para os órgãos da persecução penal, que devem ser instrumentalizados para esse enfrentamento. Necessariamente, no Brasil deverá ser traçado um planejamento e uma preparação para todos os problemas penais relacionados com o tema, existentes e os que ainda surgirão. Nestes moldes, podemos ressaltar as principais questões consideradas desafiadoras para a segurança pública e, em especial, para a investigação dos crimes cibernéticos (WEDNT; JORGE, 2013, p. 163).

Como podemos notar, a legislação pertinente a estes crimes é bastante tímida, devendo aprimorar e avançar em diversos pontos, relacionadas a regulamentação do uso da internet e como os problemas das fake news. Essa timidez de fato acaba

incidindo com o aumento gradativo da criminalidade e prejudicando e também inviabilizando as investigações desses crimes (BOMFATI; KOLBE JUNIOR, 2020).

Diante da evolução constante de tecnologia, acaba viabilizando cada vez mais possibilidades de recursos para seus usuários. A cloud computing também conhecida como computador nas nuvens, é uma ferramenta possibilidade o acesso aos dados em qualquer lugar e de qualquer dispositivo, que possa conectar-se com a internet. Esses serviços, programas e arquivos, ficam disponibilizados na nuvem, ou seja, em servidores, que tem como função principal função de hospedar as funcionalidades da internet, o problema é que grande parte destes servidores não estão localizados no Brasil, estão localizados em outros países, são de fácil acesso, via de forma remota, o sistema funciona como um disco rígido em que o internauta não está em seu dispositivo, localizado em lugares que o usuário não conhece na nuvem, sendo um exemplo deste ferramenta é o Dropbox, os dados ficam duplicados no dispositivo hospedeiro. É utilizado por diferentes usuários, mas que pode se tornar muito difícil de investigar por tratar de servidores estrangeiros, extremamente difícil apreender um servidor de outro país, ou mesmo uma demasiada demora nas investigações e diligências necessárias para o procedimento investigativo, além disso estes servidores são morosos no tocante em retirar os sites solicitados, dificultando ainda mais as investigações, sendo uma ameaça à segurança (BOMFATI; KOLBE JUNIOR, 2020).

Já em termos de prova e investigação pode-se, ainda que de forma excepcional atendendo aos requisitos constitucionais para interceptação das comunicações, conforme o exposto.

> A atual Constituição Brasileira, no Art. 5, inciso XII, dispõe que: é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. A Lei n o 9.296/1996 regulamenta a matéria, disciplinando que é cabível a interceptação de comunicações telefônicas e do fluxo de comunicações em sistemas de informática e telemática, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, desde que respeitado o disposto nela, sempre mediante ordem do juiz competente da ação principal, sob segredo de justiça, após requerimento da autoridade policial, na investigação criminal, ou, ainda, do representante do Ministério Público, na investigação criminal e na instrução processual penal (BARRETO; BRASIL, 2016, p. 169).

No tocante das provas, temos o printscreen ou captura de tela, muito utilizada para registrar um momento ou fato ocorrido na internet, no qual tem-se gerado muitas dúvidas, pois é fácil de ser modificado ou alterado para ter validade jurídica, podendo com um simples editor fazer transformações nessa captura de tela, que podem transpor outros dados que não condizem com os reais, muito utilizado nas redes sociais como Facebook e Whatsapp, mas que tem vários metadados que devem ser levado em consideração para ter valor probatório, o que não ocorre com uma simples captura de tela, perdendo dados propriedade de criação, e localização por exemplo. Também temos outra maneira de preservar os dados disponibilizados na internet, que é utilizado através de software específicos, fazendo o download da página investigada, como HTTRACK, que é um software que permite a cópia de sites inteiros para o computador ou pasta específica, podendo ser visualizado mesmo ser estar conectado na internet, recomendando-se passar para uma mídia e enviá-la imediatamente este conteúdo para perícia, fundamentando os quesitos pertinentes, sendo em muitos casos a mera captura de tela não tendo valor como prova por não submeter-se ao contraditório e ampla defesa (BARRETO; BRASIL, 2016).

Importante tratar no caso da ata notarial, diante dos documentos que formados perante a um oficial público serão de cunho público, conforme dispositivo do Art. 405 do CPC, faz prova não só da formação, mas dos fatos que o escrivão ou chefe de secretaria, tabelião ou o servidor autorizado declarar, a ata notarial tem por finalidade determinar a existência de um fato relevante no âmbito jurídico, sendo lavrado por um notário, dotada de fé pública, no qual não poderá emitir nenhum juízo sobre o que está vendo e sim tratar dos fatos narrados em que está se observando, sem nenhuma alteração dos conteúdos, sendo um importante meio de preservação de provas utilizado pelos fatos ocorridos na internet (BARRETO; BRASIL, 2016).

Outro caso, além da ata notarial para materialidade e evidências das validades digitais, considera-se a certidão de servidor público dotado de fé pública, sendo que igual valor probatório na coleta de evidências na unidade policial, trazido pela Carta Magna de 1988, uma vez que é gratuita sendo de acesso de todos nós, permitindo justiça e acesso a democracia a todos cidadãos vítimas de crimes cibernéticos apurando-se a coleta probatória, diferentemente da ata notarial em que se pese, para o registro do delito cibernético está em seu custo, que não é acessível a todos,

fazendo com que a demanda dos registros seja reprimida, levando em conta que este registro da certidão policial cabe apenas em crimes cibernéticos, tratando de ilicitudes civis ou administrativas deve-se recorrer a via da ata notarial, devendo o policial anotar todos os fatos afim de individualizar as condutas como exposição da pessoa de conteúdo íntimo, pessoas que compartilharam, ou postaram e elementos essenciais para investigação, preservando as evidências o mais rápido possível por parte da vítima e policial, solicitando ao provedor que preserve o conteúdo das investigações, pois a conduta poderá repercutir na esfera cível e criminal (BARRETO; BRASIL, 2016).

Conforme a Lei 12.735 de 2012, deve-se dar total autonomia e dispor a polícia judiciária total efetividade no combate e repressão dos cibercrimes, como dispõe o respectivo Artigo 4°.

> Art. 4° Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado (BRASIL, 2012, http://www.planalto.gov.br).

Diante da teoria do resultado, que trata em regra que a competência seja pelo lugar em que consumar-se o crime, ou seja, na pratica desse delito, ou na tentativa, pelo fato do último lugar que foram executados os atos dos criminosos, sendo imprescindível a interpretação do Código de Processo Penal, fazendo jus a busca de provas e produção probatória nos crimes cibernéticos (BARRETO; BRASIL, 2016).

Visto a materialidade, dos meios investigativos e de provas, diante dos avanços tecnológicos que reunimos em nossa legislação para combate eficaz dos crimes no meio virtual, passaremos para nova legislação pertinente aos crimes puramente cibernéticos.

4.1 Lei Carolina Dieckmann

Analisado a abordagem jurídica a despeito dos crimes cibernéticos no segundo capítulo, e legislação penal pertinentes a estes crimes, aprofundaremos nesse capítulo sobre a nova legislação Carolina Dieckmann 12.737/12 e a Lei do Marco Civil da Internet 12.965/14, no qual tipificam e tutelam sobre os crimes cibernéticos na internet, sendo fundamentalmente importantes para nosso estudo, pois um

complementa o outro, e funcionam de maneira que reúnam uma legislação específica e harmônica, no qual é objeto deste estudo.

No dia 16 de maio de 2012, fato pelo qual houve a divulgação das fotos da atriz Carolina Dieckamnn, o plenário da Câmara dos Deputados aprovou o projeto do deputado Paulo Teixeira, tipificando a invasão de dispositivo informático, sendo levado para o Senado para análise, com o projeto Azeredo, que também foi aprovado. Sendo no dia 30 de novembro de 2012, sancionada a Lei 12.737, denominada socialmente pela mídia como Lei Carolina Dieckamnn, sendo de avanço significativo para o ordenamento jurídico, mas que deixa alguns pontos de interrogação em relação as suas penas consideradas relativamente brandas (WEDNT; JORGE, 2013).

A lei 12.737/12, criminaliza as condutas cometidas pela internet, como invasão de dispositivo, roubo ou furto de senhas, conteúdos, e-mails, derrubar sites de forma intencional, além das críticas das punições previstas serem demasiadamente brandas, pois no Brasil, as penas com até quatro anos de reclusão para crimes que não utilizam da violência transformam-se em restrição de direitos, portanto não sofrerá perda da liberdade, pois a nova lei prevê no máximo um ano de detenção (CASSANTI, 2014).

A conduta de invadir equipamentos eletrônicos até então não era considerada crime em nosso Código de Direito Penal Brasileiro, posteriormente alteração e a criação da Lei Carolina Dieckmann (Lei 12.737/2012), que acabou tipificando os crimes cibernéticos, no qual está elencada no Art. 154-A do referido código:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput .
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (BRASIL, 2014, http://www.planalto.gov.br).

No tocante aos crimes informáticos, temos a Lei 12.735/12, tipificando as condutas que utilizam o uso de sistemas eletrônicos, digitais ou similares, que sejam praticados contra sistemas informatizados e similares, além dos policiais civis possam criar setores especializados no combate os crimes virtuais, devendo assim os policiais civis de todo o Brasil, readaptar essa nova realidade, no qual não estão efetivamente estruturadas e treinadas para o combate desses delitos, justamente estão extinguindo os serviços que já possuem, sendo assim uma realidade crescente e evolutiva que conhecemos, no tocante dos crimes virtuais (CASSANTI, 2014).

O presente tipo penal foi amplamente criticado, pois ressalta uma pena ínfima, sendo desproporcional em relação a gravidade que pode ser atingida e, portanto, causando prejuízos às vítimas, sendo violada a privacidade e intimidade, criminosos sabendo dessa pena branda, já visam praticar novamente crimes e propagar programas maliciosos (BARRETO; BRASIL, 2016).

A Lei Carolina Dieckmann aponta que o crime de invasão de dispositivo informativo é exclusivamente cibernético, pois é praticado unicamente com o uso de computadores e outros dispositivos que tem acesso à internet (BRASIL, 2012).

Tratando dos crimes de invasão de dispositivos informáticos, considerando-se a pena inferior a dois anos, será processada no Juizado Especial Criminal, analisando a complexidade probatória, podendo ser deslocada para Justiça Comum (JESUS; MILAGRE, 2016).

A lei 12.737/12 trouxe uma alteração no Código Penal, que consta no Art. 298 do Código Penal, que trata da falsificação de documento particular, onde está prevendo a equiparação de documento particular o cartão de crédito ou débito, sendo elemento indispensável para a conduta de falsificação, diante disso, o

legislador, foi específico no objeto, mas não resolveu a questão interpretativa, veiculando os diversos tipos de documentos que não estão sobre um suporte material, sendo assim o estudo dos crimes cibernéticos, não está sobre análise de uma técnica ou dos tipos penais que merecem a consideração do Direito Penal, e sim analisando condutas incriminàveis que podem ser realizadas por diversas maneiras e técnicas, uma técnica pode considerar uma ou mais condutas penalmente relevantes o Cavalo Tróia, pode se referir a uma invasão e permitir o dano e comportamento inesperado do sistema informático, nem toda técnica se enquadra em um comportamento incriminável, por exemplo o vírus de computador não está em uma conduta incriminável (MILAGRE; JESUS, 2016).

Como visto antes da legislação pertinente da Lei Carolina Dieckmann, não poderia prever e consequentemente punir os crimes cibernéticos exclusivamente oriundos da internet.

> Cabe esclarecer que é possível realizar o enquadramento típico da maioria das atividades que causem prejuízos ou transtornos aos usuários. Porém, para atender àqueles casos em que não existe a referida previsão penal para promover um enquadramento específico que se amolde perfeitamente aos referidos crimes, de forma a evitar questionamentos jurídicos como, por exemplo, a alegação de que a conduta não é criminosa porque não há previsão legal, e também com o objetivo de oferecer mais condições para a punição dos crimes cibernéticos estabelecendo inclusive prazo mínimo para a preservação dos logs (WEDNT; JORGE, 2013, p. 164).

O dano informático, a interferência de dados sendo realizado por um ou mais agentes, com ato intencional de causar o dano, danificar, deteriorar, alterar, apagar qualquer desses dados informáticos, no caso de incidência de dano temos o Art. 154-B do Código Penal, nos termos da nova lei 12.737/12, contudo se o agente não invade, mas apenas causa o dano informático ainda responderá perante ao crime de dano, que trata o Art. 163 do Código Penal. Tratando da interferência de sistemas, no qual sua causa está ligada diretamente dolosamente causando de forma intencional e ilegítima ao funcionamento de um sistema informático, com isso passou a ser tipificado o delito de interrupção ou perturbação do serviço telegráfico, telefônico, informático, telemático, ou de informação de utilidade pública, sendo sua pena dobrada se cometidas em estado de calamidade pública (MILAGRE; JESUS, 2016).

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1 º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2 º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública (BRASIL, 2012, http://www.planalto.gov.br).

Sendo que o Art. 266 do Código Penal, não tratava das possibilidades do objeto dos sistemas de informáticos serem atacados envolvendo a interrupção, sendo essa lacuna suprimida pela referida lei, buscando proteger com esse tipo penal a regularidade dos serviços telegráficos, radiotelegráficos e telefônicos, deste modo sendo acaba sendo protegido o próprio serviço de informação, devendo destacar que o §1 do Art. 266 do Código Penal, protege só o serviço telemático ou de informação que seja de utilidade pública, critério de difícil entendimento, devendo ser analisado caso a caso, sendo conduta criminosa também impedir ou dificultar o restabelecimento dos serviços telemáticos ou de informação e de acordo com o caput a mera perturbação, também considera-se conduta punível (JESUS; MILAGRE, 2016).

4.2 Marco Civil da Internet

Os direitos dos usuários originaram-se com a Lei 12.965/2014, conhecida como Marco Civil da Internet no qual uma sociedade não está preparada para entender o que pode ou não caracterizar um crime informático, que já está tipificado. Após 15 anos de discussões foi promulgada a Lei 12.735/12 e 12.737/12, passando a expor algumas condutas no âmbito cibernético, no qual é necessário cautela para entendimento pois é uma legislação nova, precisando ser esclarecida quais condutas devem ser reprendidas e punidas consequentemente. Com isso a Lei 12.735/2012, surgiu prevendo que os órgãos de polícia judiciária poderão estruturar nos termos de regulamentação, setores e equipes especializadas no combate a sistemas de informatização (JESUS; MILAGRE, 2016).

A Lei 12.737/12 está longe de ser uma legislação que resolva todos os problemas relativos aos crimes cibernéticos, a solução não está só em editar leis e mais leis, mas também da educação digital, politicas criminais e uma base

investigativa eficaz. O Marco Civil da Internet é considera a Constituição da Internet, assim garantido os direitos e deveres inerentes a todos usuários da internet no Brasil, surgindo de um projeto inicialmente em 29 de outubro de 2009 da Secretaria de Assuntos Legislativos do Ministério da Justiça com parceria da Escola de Direito da Fundação Getúlio Vargas do Rio de Janeiro, após essa fase foi levada para a participação popular no Congresso, em 24 de agosto de 2011, por meio de projeto de Lei, n° 2.126, de iniciativa do Poder Executivo, projeto no qual viabilizava estabelecer princípios, direitos e garantias para seus usuários na internet, sendo sancionada pelo Presidente da República em 23 de abril de 2014, surgindo a Lei 12.965 (JESUS; MILAGRE, 2016).

> Alguns pontos foram bem polêmicos na discussão do projeto, entre eles a neutralidade da rede e a obrigação de empresas de sediarem os “data centers” (centros de processamento de dados) no Brasil, a fim de garantir que os dados fossem armazenados no país. Em 12 de setembro de 2013, o Poder Executivo solicitou que o projeto de lei fosse incluído no regime de urgência, através da Mensagem nº 391 de 2013, conferindo o prazo de 45 dias para apreciação na Câmara dos Deputados. Depois, ao ser enviado ao Senado, o projeto do Marco Civil foi aprovado por unanimidade (BARRETO; BRASIL, 2016, p. 20).

Conforme exposto, a era antes da promulgação da Lei do Marco Civil, era a ausência de regulamentação civil na internet no Brasil, causando grande insegurança jurídica, também temos sua aplicação no Direito Penal e Direito Processual Penal, uma vez que estabelece princípios e conceitos fundamentais, bem como também trata da obtenção de provas e quanto à materialidade e identificação da autoria desses delitos (BARRETO; BRASIL, 2016)

Segundo o Art. 1º da Lei nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, determinando suas diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. (BRASIL, 2014).

Diante dos fundamentos do Marco Civil, é norma especifica a regulamentar os fundamentos do uso da Internet, com isso teve inspiração seu de seus fundamentos do texto constitucional, colocando como ideias centrais a preservação da liberdade de expressão conforme disposto em seu Artigo 2° da referida Lei (BARRETO; BRASIL, 2016).

No qual tange os princípios do Marco Civil da Internet estão especificados nos incisos do Art. 3º da sua lei, como veremos a seguir:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II – Proteção da privacidade;
> III – proteção dos dados pessoais, na forma da lei;
> IV – Preservação e garantia da neutralidade de rede;
> V – Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI – Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII – preservação da natureza participativa da rede;
> VIII – liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte (BRASIL, 2014, http://www.planalto.gov.br).

O Marco Civil da Internet, possibilita que a autoridade policial e o Ministério Público, façam o requerimento de preservação dos registros de conexão, também no tocante dos acessos de aplicações na internet, sendo mantidos por um ano podendo ser prorrogado, desde que haja a devida solicitação da autoridade mencionada, nos casos dos registros devem ser feitos a manutenção no período de seis meses, também podendo haver prorrogação, a preservação do registro perderá a eficácia se não houver protocolo de representação judicial no prazo de sessenta dias a contar do requerimento, evidência ou indeferimento, tendo conhecimento o delegado deverá expedir o ofício ao provedor de conexão ou de internet, indicando assim a forma de localização quanto ao suposto perfil do ilícito e dos dados pertinentes aos indícios de autoria. O Marco Civil diferencia o registro de conexão do registro de aplicação na internet, sendo que no primeiro trata-se de informações referentes à data e hora, início e termino de uma conexão à internet, também a sua duração e endereço de IP. Já o segundo é o conjunto de funcionalidades que se referem a data e hora, mas de uma forma determinada a aplicação da internet, partindo de um determinado endereço de IP. Sendo que tudo deve ocorrer sob sigilo com ambiente controlado e seguro, no caso dos provedores de conexão não é possível a transferência e manutenção dos registros a terceiros (BARRETO; BRASIL, 2016).

Sendo que ambos dispositivos estão elencados na Lei do Marco Civil, especificamente no Artigo 5°. Respectivamente nos Incisos VI, que trata dos registros de conexão do Inciso VIII, dos registros de acesso, que foram elencados (BRASIL, 2014, http://www.planalto.gov.br).

Também nos termos do inciso I, do Artigo 7° da Lei do Marco Civil, passa a tratar da inviolabilidade e sigilo das comunicações na internet, exceto por ordem judicial, sendo utilizada para fins de investigações criminais ou instrução processual penal, sendo no inciso V, o usuário não fornecerá a terceiros seus registros de conexão e acesso a aplicações na internet salvo se esta pessoa consentir ou nas hipóteses que estão previstas em lei (JESUS; MILAGRE, 2016).

Temos também a neutralidade da rede, elencada no Art. 9 da lei referida, tem um acesso igualitário à internet:

> 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 (BRASIL, 2014, http://www.planalto.gov.br).

Sendo, portanto qualquer conteúdo vinculado será removido via meio judicial, sendo obrigados os provedores a disponibilizar os registros pertinentes e as informações de identificação do usuário, sendo cabível diante de um mandado, exceto nos casos envolvendo nudez em que a notificação extrajudicial deverá ser atendida pelos provedores. Nos moldes do Artigo 18° da referida lei, o provedor de conexão a internet, não será responsabilizado civilmente pelos danos gerados decorrente dos conteúdos de terceiros, poderá ser responsabilizada por atos de terceiros se após ordem judicial específica não tomar as devidas providências no âmbito de seu serviço dentro do prazo, para remoção de conteúdos infringentes e violadores, contudo não há impedimento para eventual responsabilização criminal de diretores ou sócios de provedor de acesso, desde que tenha sua participação comprovada por intermédio do uso informático (JESUS; MILAGRE, 2016).

Fundamentalmente, ninguém é obrigado a fazer ou deixar de fazer algo se não em virtude de lei, conforme o princípio da legalidade, nesse contexto, temos a Lei do Marco Civil da Internet efetivamente tutelando garantias e direitos aos usuários que utilizam-se dos meios virtuais, antes da referida lei, era inexistente qualquer lei que

obrigasse os provedores de internet ou de serviços a registrarem logs das atividades dos seus usuários, havendo apenas a recomendação do Comitê Gestor Internet do Brasil, sendo que a maioria das vítimas dos crimes virtuais, não é administradora do ativo informático, para que apure a autoria do delito, sendo indispensável cooperação de terceiros que administram ou oferecem serviços, aplicações ou hosts para pratica dos crimes cibernéticos (JESUS; MILAGRE, 2016).

Como visto, os principais direitos e garantias, previstas na Lei do Marco Civil da Internet estão na remoção do conteúdo, sigilo das comunicações, salvo os casos de ordem judicial, proteção dos dados pessoais, direito da não suspensão da conexão, manutenção da qualidade contratada e a neutralidade da rede tratando de forma igual, sem distinção dos conteúdos dos destinos e da origem (CASSANTI, 2014).

Com o surgimento da do Marco Civil da Internet Lei 12.965 de 2014, temos alguns direitos e garantias assegurados como visto, garantindo aos usuários que provém dos seus recursos uma tutela jurídica na qual não havia anteriormente, sendo que o Marco Civil da Internet, é uma espécie de complementação da Lei 12.737, a famosa Lei Carolina Dieckmann, no qual analisamos nesse capítulo.

4.3 Lei de Proteção de Dados Pessoais

A Lei de Proteção de Dados Pessoais 13.709/18, conhecida como LGPD, foi promulgada pelo presidente Michel Temer no dia 14 de agosto de 2018, sendo uma legislação técnica e busca assegurar uma gama de garantias previstas nos direitos fundamentais, proteção dos direitos humanos de liberdade e privacidade, é um novo marco para nossa legislação atual, impactando tanto as instituições privadas como públicas, qualquer relação que envolva o tratamento de informações que utilizem os dados pessoais, sendo por qualquer meio, regulando princípios, direitos e garantias para uma sociedade digital relacionada com as bases dos dados pessoais (PINHEIRO, 2020).

A LGPD, é uma legislação bem recente, passando por algumas atualizações, foi essencialmente inspirada para sua criação, a Autoridade Nacional de Proteção de Dados (ANPD), uma figura típica que representa a garantia de eficácia e aplicação das normas trazidas com a regulamentação, trazendo a regulação de proteção de dados no Brasil, também da ampliação do prazo para sua entrada em vigor. A

criação da ANPD, além das polêmicas que a envolvem, foi criada com intuito de trazer maior segurança e estabilidade (PINHEIRO, 2020).

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização (PINHEIRO, 2020, p. 14).

Inspirada na Lei Europeia de proteção de dados, também conhecida como General Data Protection Regulation (GDPR), a LGPD tem como objetivo geral de proteger os dados pessoais das pessoas naturais ou físicas, sendo que estas pessoas físicas são o foco principal, não tendo como escopo dados de pessoas jurídicas, mas sim dos dados que as empresas têm das pessoas físicas, sendo funcionários, terceiros ou clientes (GARCIA *et al*, 2020).

A proteção dos dados, é garantia das plataformas e aplicativos, mas que existe muitas violações pertinentes ao uso indevido dos dados pessoais, isso é fato, no entanto a Lei 13.709/18, vem para proteção e sigilo destes dados em todo o território nacional, regulamentando o direito à privacidade e proteção dos dados, assegurando os direitos fundamentais, inclusive no meio digital, por pessoa física ou jurídica, sendo indevido, sem a permissão da pessoa a publicação de informações a terceiro, infringindo a nova Lei. Também identifica o tratamento de dados sensíveis, sendo toda aquelas informações que podem ser utilizadas de forma discriminatória, portanto carecendo de proteção especial que está abarcada, implicando sobre origem racial, étnica, religiosa, opinião política, dados referentes as pessoas naturais. Outro fato importante, são os dados tutelados e protegidos pela LGPD, vinculando todos os dados pessoais dos funcionários por exemplo das empresas, que são detentoras da proteção desses dados, sob pena de responsabilização civil, no entanto não tem um órgão federal que realize a fiscalização de tais regras, sendo instituído a ANPD, que é responsável pela devida aplicação e mediadora de eventuais conflitos, empresas, usuários e da própria legislação (FREITAS, 2020).

Além da complementação do Marco Civil da Internet, a LGPD, tem como relevância o fato de ser mais específica e acaba inovando por trazer sanções direcionadas e incluindo um novo órgão de governança da presidência da República,

precisando empresas públicas e privadas adaptar-se à nova realidade, tratando essa sanção administrativa aplicada pela autoridade nacional podendo chegar a 2% do faturamento da pessoa jurídica de direito privado (GARCIA *et al,* 2020).

A Lei de dados pessoais, vem em um momento crucial e fundamental em que estamos vivenciando, realmente sendo promissora, tendo em vista a vanguarda a defesa e proteção dos direitos pessoais dos cidadãos, no momento onde há muitos vazamentos de dados e exposição no âmbito virtual. A fiscalização e proteção desses dados é primordial sendo uma Lei, para complementação do Marco Civil da Internet.

4.4 Cooperação Internacional

A internet é uma rede global, colocando parâmetros para que haja cooperação internacional, envolvendo tanto polícias quanto os judiciários, de diversos países e culturas sendo sua finalidade principal o combate à criminalidade cibernética, hoje temos a internacionalização da troca de informações, tornando-se a rede mundial, sendo a vinculação dessas pessoas em grande massa, necessidade de levar plataforma a todos os cantos do planeta, sendo resultado a globalização da rede, sendo capaz a troca de informação de países em todo o mundo, sendo a rede internacional as ameaças também são. Com o avanço significativo da internet, gerou um aumento dos usuários influenciando na ampliação dos provedores de serviços, assim com as novas tecnologias devem ser feitas novas ações para enfrentamento desse contexto criminal que desconhece fronteiras, sendo praticado em todo o mundo, sendo cada país organizado politicamente e com as leis e estruturas do governo de maneira diversa de outra, sendo imprescindível a cooperação internacional para combate ao cibercrimes, sendo que ainda é muito burocrática havendo necessidade de urgência no aperfeiçoamento da colaboração entre os países para repressão dos crimes acometidos na rede mundial de computadores, sendo imprescindível a existência de um canal aberto para atendimentos às vítimas entre os órgãos judiciários e a polícia na mesma velocidade que ocorrem os crimes que utilizam fibra ótica (BOMFATI; KOLBE JUNIOR, 2020).

A dificuldade da investigação depara-se quando está à frente de um provedor estrangeiro e este não possui escritório de representação no Brasil, assim nos casos

de e-mails ou sites de responsabilidade de provedor estrangeiro deve-se contatar o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério de Justiça (WEDNT; JORGE, 2013).

Referente à cooperação internacional, destaca-se o acordo de Assistência Judiciária na matéria Penal entre o Governo Brasileiro e o Governo dos Estados Unidos da América (MLAT) e Decreto nº 3.810, de 02 de maio de 2001, e também a Convenção de Budapeste que o Brasil não é signatário (BARRETO; BRASIL, 2016).

> No ano de 2001, na Hungria, foi criada a Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime, pelo Conselho da Europa. Dentre suas principais finalidades cabe destacar: o incremento para a cooperação internacional entre os órgãos responsáveis pela investigação criminal; a previsão de novas condutas criminais que, pela internet, causem prejuízo ou transtorno para a vítima; a pressão para aprovação de legislação específica sobre o tema etc (WEDNT; JORGE, 2013, p. 169).

A ideia de preservação das evidencias dos crimes cibernéticos surgiu em um encontro de integrantes dos países que compõem o G8, no ano de 1997, foi criado um subgrupo High-Tech Crime, visando garantir persecução do criminoso cibernético em qualquer lugar do mundo, nesse tocante foi criado uma rede de cooperação internacional não era um meio rápido e eficaz, logo a nova rede visa a preservação rápida e pontual das evidências buscando com êxito a localização e a prisão desses cibercriminosos. A rede é composta por pontos estratégicos de contatos entre os países disponível 24 horas por dia e sete dias por semana, esse modelo de cooperação está previsto na convenção de Budapeste sobre Cibercrime, caso haja a necessidade de preservação de evidência, deve-se procurar a Superintendência da Polícia Federal oficializado a guarda desse conteúdo (BARRETO; BRASIL, 2016).

Classificação da Convenção de Budapeste (2001), embora o Brasil não seja signatário da Convenção sobre o Cibercrime, é de suma importância conhecer sua classificação, de acordo com Barreto e Brasil (2016, p. 28):

> Título 1 — Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos: acesso ilegítimo; intercepção ilegítima; interferência em dados; interferência em sistemas; uso abusivo de dispositivos.
> Título 2 — Infrações relacionadas com computadores: falsidade informática; burla informática.
> Título 3 — Infrações relacionadas com o conteúdo: infrações relacionadas com pornografia infantil.

Título 4 — Infrações relacionadas com a violação do direito de autor e direitos conexos.

A Interpol, serviço de cooperação internacional e a maior organização policial do mundo com 190 países membros, fornecendo serviços essenciais e necessários possibilitando o desenvolvimento policial de forma eficaz e efetiva, através de uma capacitação e suporte investigativo, banco de dados e canais que comunicam-se de forma segura e rápida, ressaltado que a Interpol auxilia as polícias nacionais identificado e localizando foragidos, com vista na prisão e posteriormente na extradição ou ato congênere, a Polícia Federal tem esse papel de realizar a cooperação internacional, tarefa essa executada pelo Coordenação Geral de Cooperação Internacional, no qual está vinculada ao Gabinete do Diretor Geral da Polícia Federal, caso seja necessário um delegado da polícia civil obter informações de um investigado em outro país, deverá solicitar apoio juntamente com a Coordenação da Polícia Federal, através do serviço de Cooperação Policial, centralizando informações para entrar em contato com a Interpol. Brasil e Uruguai assinaram em 2004 um acordo onde buscam o aperfeiçoamento das investigações e controle dos fatos delituosos e relacionado a cooperação policial, sendo também pelo Mercosul celebrados acordos visando este aperfeiçoamento da atuação policial no âmbito investigativo e combate à criminalidade (BARRETO; BRASIL, 2016).

Devemos de fato, conscientizar a população e todos os usuários que não conhecem todas as dimensões e características da internet, isso é de fato problemático, muitos utilizam os recursos tecnológicos sem realmente saber das consequências que podem ter se utilizarem de maneira equivocada e errada, sendo os riscos de receber um e-mail e acabar clicando nele sem saber dos riscos, instalação de um programa com conteúdo suspeito que pode roubar seus dados, a utilização das redes sociais também representando um grande perigo, pois muitos postam seus dados pessoais e aonde tem muitos criminosos estão de prontidão para agir, sendo indispensável a educação ou reeducação da população pois muitos não sabem da imensidão da internet e dos seus recursos, e as redes sociais são frágeis para explanar arquivos maliciosos para as vítimas, podendo contaminar a todos seus contatos, que inclusive poderão acreditar no seu conteúdo colocado ou compartilhado e acabam clicando por consequência disso serão contaminados, esse alerta é para todos, sendo em especial para crianças e adolescentes, pois são

grande parte da população que utilizam estes recursos tecnológicos e são suscetíveis a caírem nesses golpes, sendo necessário no dia a dia usar boas práticas tornando a internet mais segura no processo de conscientização, pode ser um processo demorado, mas que certamente deve ser inserido na educação digital, não apenas pelos órgãos de prevenção mas também de repressão, assim os policiais informam os usuários dos perigos que ocorrem na internet, estas pessoas podem precaver-se e conscientizar-se sobre os crimes cibernéticos, consequentemente reduzindo esses delitos praticados por criminosos em todo o Brasil, sendo que muitas vítimas não tiveram essa oportunidade de precaver-se, sendo fundamental para não cair em golpes do mundo virtual (WEDNT; JORGE, 2013).

5 CONCLUSÃO

O crescimento da internet é incontestável, sendo utilizado no mundo todo desde sua criação e também com o passar dos anos houve avanços significativos, inclusive no Brasil, chegando a marca de 60% da população conectada. Diante desses dados, os avanços já eram previstos, possuído um índice maior de criminosos que ainda estão migrando para este âmbito virtual, tanto na Deep Web e na Dark Web, vírus espalhados para infectarem pessoas desprevenidas e despreparadas, inclusive por falta da educação digital na sociedade, é comum vivenciamos Cracker e Hackers navegando livremente por este meio e buscando novas vítimas para seus crimes, e muitas vezes acabando impunes.

Nesse sentido, devemos concluir essa monografia, que apesar da evolução da internet, os crimes virtuais vêm acentuando-se desde a criação da internet, e, contudo, o Brasil, demorou para transpor essas leis para o papel. Com a inovação da legislação pertinente aos crimes cibernéticos, realmente houve uma mudança no cenário atual dos crimes cibernéticos. A criminalidade evolui, mas nosso Código Penal de 1940, não teve essa evolução. Os crimes são sempre recorrentes em nossa sociedade, pois são de fato muito lucrativos, tornando-se extremamente críticas com a tecnologia à disposição de uma grande parcela da população, hoje muitos que acabam imigrando para esse tipo de criminalidade, pois acreditam que o anonimato não será punido, consequentemente não temos uma eficácia da nossa legislação pertinentes a estes crimes, estamos realmente vulneráveis aos delitos cibernéticos, e devemos agir para combater e prevenir a criminalidade cibernética no Brasil, que hoje infelizmente está muito à frente da justiça brasileira.

Os crimes se tornam rotineiros e cada vez mais avassaladores no Brasil, deve-se o legislador dar a devida importância a essa temática, pois os infratores continuem a cometer crimes, em escala cada vez maior. Os cibercriminosos migraram para as redes da Deep Web e Dark Web, onde estão buscando anonimato e uma suposta “privacidade” para aplicar golpes e crimes, e não temos ferramentas adequadas para lidar com essa progressão dos crimes cibernéticos, hoje temos uma legislação específica, mas com pena realmente ínfima e por isso muitos criminosos sabem disso e acabam por continuar a cometer os crimes visto a impunidade que temos em nossa legislação atual brasileira.

Diante do exposto, e análise da legislação, Lei 12.737/12, conhecida como Lei Carolina Dieckmann, houve significativas mudanças, no qual tipifica os crimes informáticos, no qual anteriormente não estava tipificado em nossa legislação vigente, sendo um fato marcante e um passo importante para progressão do combate aos crimes cibernéticos e também temos a Lei do Marco Civil da Internet, Lei 12.965/14, que trata dos princípios, garantias direitos e deveres do uso da internet, também a importância do registro de logs e da neutralidade da rede, mas não elencam um rol de crimes e tipificações próprias penais para todos os delitos de âmbito virtual, sendo as legislações devidamente brandas e insuficientes para o colapso atual da sociedade em virtude do aumento exponencial dos crimes cibernéticos no Brasil.

Também temos a nova Lei de Proteção de Dados Pessoais, 13.709/2018, no qual complementa o Marco Civil da Internet, sendo importante sua aplicação, no momento atual em que vivenciamos, onde muitos dados são vazados e expostos de maneira indevida, tratando a LGPD, a proteção desses dados pessoais inovando com Autoridade Nacional de Proteção de Dados ANPD, que tem o dever de fiscalizar e regulamentar o cumprimento da Lei em todo o território nacional, além das sanções e maior proteção dos direitos fundamentais de liberdade e garantias da privacidade e intimidade.

Outro fato importante é o agente infiltrado prevista na Lei 13.441/17, onde foi instituído no Estatuto da Criança e do Adolescente, a figura do policial que atua não no ambiente físico, mas sim no virtual com objetivo de investigar e obter provas para inibir os criminosos que utilizam esses recursos virtuais nos crimes de dignidade sexual, onde o avanço realmente foi significativo, pois sabemos que estes crimes ocorrem muito na Dark Web, e em relação a estes crimes de dignidade sexual trouxemos avanços nos últimos anos, assim combatendo esse forte mercado de pornografia infantil e a pedofilia na internet.

A investigação e os meios de provas também são de suma importância para identificação dos criminosos e práticas delituosas ocorridas na internet, um dos problemas dessas investigações é que tem servidores que são de outros países fazendo com esses fatos demorem mais tempo para obtenção das informações, devendo ter uma Cooperação Internacional eficiente, lembrando que o Brasil não é

signatário da Convenção de Budapeste, no qual teria maior celeridade no combate e repressão e provas dos crimes cibernéticos no âmbito internacional.

Fato comum, porém, deverá ser analisado uma legislação especifica para tipificação dos crimes cibernéticos, tal como dar todo suporte e autonomia necessária no tocante aos investigadores e peritos para combate da criminalidade no ciberespaço, pois quem acaba sofrendo os prejuízos é toda a sociedade brasileira, onde deverá focalizar em delegacias especializadas para combate e prevenção dos crimes cibernéticos.

Fundamentalmente, além dos tipos penais, devemos primar sempre pela educação digital, conscientização das pessoas, dos riscos de condutas incriminadoras que podem ocorrer na internet, para que efetivamente reduza o número de pessoas infectadas por vírus e vítimas de estelionatários, sexting, e crimes digitais em geral, sendo estas pessoa informadas dos perigos do mundo cibernético, certamente não haverá a mesma eficácia dos criminosos, sendo todas pessoas informadas dos riscos, consequentemente reduziria a escala desses crimes virtuais, e muitas vítimas desprotegidas poderiam prevenir-se, pois ainda carecem e estão despreparadas para o uso correto do meio virtual.

REFERÊNCIAS

ANDREUCCI, Ricardo Antonio. *Legislação penal especial*. São Paulo: Editora Saraiva, 2018.

BARRETO, Alesandro; SANTOS, Hericson. *Deep Web:* Investigação no submundo da internet. Rio de Janeiro: Brasport, 2019.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. *Manual de Investigação Cibernética à Luz do Marco Civil da Internet*. Rio de Janeiro: Ed. Brasport, 2016.

BARRETO, Alesandro Gonçalves; WENDT, Emerson; CASELLI, Guilherme. *Investigação Digital em fontes abertas*. Rio de Janeiro: Brasport, 2017.

BARRETO, Alesandro Gonçalves; WENDT, Emerson. *Inteligência e Investigação criminal em fontes abertas*. Rio de Janeiro: Brasport, 2020.

BOMFATI, Cláudio Adriano; JUNIOR, Armando Kolbe. *Crimes Cibernéticos*. Cutiriba: Intersabares, 2020.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil*. Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 abr. 2020.

BRASIL. *Decreto-lei n° 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília, DF: Presidente da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 16 abr. 2020.

BRASIL. *Decreto-lei nº 3.914, de 09 de dezembro de 1941*. Lei de introdução do Código Penal. Brasília, DF, Presidente da República, [1941]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm. Acesso 25 abr. 2020.

BRASIL. Lei 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Brasília*,* DF, 13 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 16 abr. 2020.

BRASIL. Lei nº 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 10 mar. 2020.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm**.** Acesso em: 10. Abr. 2020.

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

CASTELLS, Manuel. *A Galáxia Internet:* reflexões sobre a Internet, negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CHIMENEZ, Mariana. Crimes Contra a Honra na Era Digital. *Jus Brasil [s.l.],* 2017. Disponível em: https://marianachimenez.jusbrasil.com.br/artigos/498225563/crimes-contra-a-honra-na-era-digital. Acesso 10 de maio de 2020.

CLARKE, Richard A.; KNAKE, Robert K. *Guerra cibernética:* a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015.

CRESPO, Marcelo. Crimes Digitais: do que estamos falando? *Canal Ciências Criminais, [s.l.],* 17 jun. 2015. Disponível em: https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando. Acesso em: 23 mar. 2020.

CONVENÇÃO DO CIBERCRIME, 1., 2001, Budapeste. *Conferência do Cibercrime.* Budapeste: Conselho da Europa, 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci-en/rules-and legislation/legislacao/legislacoes-pertinentes-do brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 12 de mar. 2020.

COUTO, Cleber. Pedofilia no Estatuto da Criança e Adolescente: art. 241-E e sua interpretação constitucional. *Revista Jus Navigandi***,** ISSN 1518-4862, Teresina, a. 20, n. 4421, 9 ago. 2015. Disponível em: https://jus.com.br/artigos/41178. Acesso em: 13 maio. 2020.

D'URSO, Luiz Flávio Borges. Racismo é diferente de injúria racial. *Migalhas*, *[s.l],* 8 set. 2016. Disponível em: https://migalhas.uol.com.br/depeso/245234/racismo-e-diferente-de-injuria-racial. Acesso em: 15 de maio de 2020.

FIORIM, Franzvitor. *Criptografia para iniciantes*: o que é, como funciona e por que precisamos dela? *CanalTech*, *[s.l.],* 17 ago. 2015. Disponível em: https://canaltech.com.br/seguranca/criptografia-para-iniciantes-o-que-e-como-funciona-e-por-que-precisamos-dela-46753. Acesso em: 28 abr. 2020.

FREITAS, Felipe. O que é LGPD e o que muda com essa lei. *CanalTech*, *[s.l],* 03 set. 2020. Disponível em: https://canaltech.com.br/governo/lgpd-o-que-e-e-como-funciona. Acesso em: 20 set. 2020.

GARCIA, Lara Rocha *et al. Lei Geral de Proteção de Dados (LGPD):* Guia de implantação. São Paulo: Editora Blucher, 2020.

GOGONI, Ronaldo. Deep Web e Dark Web*:* Qual a diferença? *TecnoBlog*, *[s.l.],* 18 mar. 2019. Disponível em: https://tecnoblog.net/282436/deep-web-e-dark-web-qual-a-diferenca. Acesso 05 de mar. 2020.

LATIF, Omar Aref Abdul. Dos crimes contra a honra. *Âmbito Juridico. [s.l.],* 31 de maio. 2007*. Disponível em:* https://ambitojuridico.com.br/cadernos/direito-penal/dos-crimes-contra-a-honra. Acesso 12 maio. 2020

JESUS, Damásio de; MILAGRE, José Antonio. *Manual de crimes informáticos.* São Paulo: Saraiva, 2016.

JORGE, Higor Vinicius Nogueira*. Investigação Criminal Tecnológica.* Rio de Janeiro: Brasport, 2018. v.1.

MARTINS, Elaine. O que é backbone*? Techmundo, [s.l.], 10 mar. 2009. Disponível em:* https://www.tecmundo.com.br/conexao/1713-o-que-e-backbone-.htm. Acesso 30 abr. 2020.

NAÇÕES UNIDAS BRASIL. No Brasil quase 60% das pessoas estão conectadas à internet, afirma novo relatório da ONU. *Nações Unidas Brasil, [s.l.]*, 21 set. 2015. Disponível em: https://nacoesunidas.org/no-brasil-quase-60-das-pessoas-estao-conectadas-ainternet-afirma-novo-relatorio-da-onu. Acesso em 22 mar. 2020.

PEREIRA, Ana Paula, O que é um Trojan*? Tecmundo*, *[s.l.],* 26 ago. 2008. Disponível em: https://www.tecmundo.com.br/seguranca/196-o-que-e-um-trojan-.htm. Acesso em: 10 maio. 2020.

PEREIRA, Dimitri. Saiba o que é a Tor e como essa rede garante o seu anonimato na Web. *Canaltech, [s.l.], [2020?]. Disponível em:* https://canaltech.com.br/internet/saiba-o-que-e-tor-e-como-essa-rede-garante-o-seu-anonimato-na-web. Acesso 15 abr. 2020.

RIBEIRO, Thiago de Lima. *O direito aplicado ao cyberbullying*: honra e imagem nas redes sociais. Curitiba**:** Intersaberes, 2013.

STIVANI, Mirella. O que é um worm? Entenda o malware que se multiplica sozinho. *Techtudo*, *[s.l.],* 08 nov. 2018. Disponível em: *https://www.techtudo.com.br/noticias/2018/11/o-que-e-um-worm-entenda-o-malware-que-se-multiplica-sozinho.ghtm*l. Acesso em 15 mar. 2020.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes Cibernéticos (2a. ed):* Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2013.

WENDT, Emerson; LOPES, Fábio Motta. *Investigação Criminal:* ensaios sobre a arte de investigar crimes. Rio de Janeiro: Brasport, 2014.