UNIVERSIDADE ESTADUAL DA PARAÍBA
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
CURSO DE ESPECIALIZAÇÃO EM PRÁTICA JUDICANTE

ALANNA KÁSSIA DE ARAÚJO LEITE BUSTORFF

CIBERCRIMES: A DEEPWEB E OS PROCEDIMENTOS DE INVESTIGAÇÃO FRENTE A ESCASSEZ LEGISLATIVA

JOÃO PESSOA
2020

ALANNA KÁSSIA DE ARAUJO LEITE BUSTORFF

CIBERCRIMES: A DEEPWEB E OS PROCEDIMENTOS DE INVESTIGAÇÃO FRENTE A ESCASSEZ LEGISLATIVA

Trabalho de Conclusão de Curso de Pós-Graduação apresentado ao programa de Pós-Graduação em Prática Judicante da Universidade Estadual da Paraíba em parceria com a Escola Superior da Magistratura como requisito parcial para a obtenção do título de especialista.

Orientador: Prof.º Cláudio Simão de Lucena Neto, LLM

JOÃO PESSOA

2020

B982c Bustorff, Alanna Kássia de Araújo Leite.

Cibercrimes [manuscrito] : a deepweb e os procedimentos de investigação frente à escassez legislativa / Alanna Kássia de Araújo Leite Bustorff. - 2020.

40 p.

Digitado.

Monografia (Especialização em Prática Judicante) - Universidade Estadual da Paraíba, Pró-Reitoria de Pós-Graduação e Pesquisa , 2021.

"Orientação : Prof. Me. Cláudio Simão de Lucena Neto , Coordenação do Curso de Relações Internacionais - CCBSA."

1. Internet. 2. Cibercrimes. 3. Cibercultura. 4. Procedimentos de Investigação. 5. Legislações. I. Título

21. ed. CDD 341.757

Elaborada por Elesbao S. Neto - CRB - 15/347 BSC5/UEPB

ALANNA KÁSSIA DE ARAUJO LEITE BUSTORFF

CIBERCRIMES: A DEEPWEB E OS PROCEDIMENTOS DE INVESTIGAÇÃO FRENTE A ESCASSEZ LEGISLATIVA

Trabalho de Conclusão de Curso de Pós-Graduação apresentado ao programa de Pós-Graduação em Prática Judicante da Universidade Estadual da Paraíba em parceria com a Escola Superior da Magistratura como requisito parcial para a obtenção do título de especialista.

Aprovada em: 21 / 10 / 2020 .
Nota: 9,0

BANCA EXAMINADORA

Prof. Me. Cláudio Simão de Lucena Neto (Orientador)
Universidade Estadual da Paraíba (UEPB)

Assinado de forma digital por Rodrigo Monteiro Pessoa
Dados: 2021.01.07 10:14:48 -03'00'

Prof. Dr. Rodrigo Monteiro Pessoa
Universidad de la Frontera (TEMUCO/CHILE)

Profa. Cynara de Barros Costa
Universidade Estadual da Paraíba (UEPB)

RESUMO

O presente trabalho objetiva analisar os impactos dos cibercrimes na sociedade e os modos que os agentes delituosos vislumbram para se favorecem dos meios que a *deep web* dispõe para esconderem suas identificações e localizações. De forma específica, busca-se ressaltar a análise do psicanalista John Suler quanto ao computador ou a tela de um aparelho eletrônico acerca do efeito desinibitivo que provoca nos usuários modificando aspectos da personalidade dos indivíduos, ocasionando a manifestação de sentimentos, pensamentos e vontades, provavelmente reprimidos no ambiente físico. Ademais, apresentar algumas leis que foram criadas visando às ações no ambiente virtual, quais sejam: a Lei nº. 12.965/2014, também conhecida como Marco Civil da Internet e a Lei nº 12.737/2012 (Lei Carolina Dieckmann), levantando o questionamento sobre a insuficiência legislativa por não abranger todas as situações de fato que ocorrem no ciberespaço, principalmente as condutas delituosas que são praticadas com frequência na seara digital. Discorrer sobre os procedimentos de investigação utilizados nas averiguações de crimes virtuais e perícias de informática. Concluindo com a apresentação de uma forma de aperfeiçoar a prevenção e repressão dos cibercrimes garantindo a segurança dos usuários.

Palavras-chaves: Internet. Cibercrimes. Cibercultura. Procedimentos de Investigação. Legislações.

ABSTRACT

The present work aims to analyze the impacts of cybercrimes on society and the ways that criminal agents envision to favor the means that the deep web has to hide their identifications and locations. Specifically, it seeks to emphasize the analysis of the psychoanalyst John Suler regarding the computer or the screen of an electronic device about the disinhibitory effect it causes in users, modifying aspects of the individuals' personality, causing the manifestation of feelings, thoughts and wills, probably repressed in the physical environment. In addition, to present some laws that were created aiming at actions in the virtual environment, namely: Law no. 12,965 / 2014, also known as Marco Civil da Internet and Law nº 12,737 / 2012 (Law Carolina Dieckmann), raising the question about the legislative insufficiency because it does not cover all the factual situations that occur in cyberspace, mainly the criminal behaviors that are frequently practiced in the digital field. Discuss the investigation procedures used in the investigation of cyber crimes and computer skills. Concluding with the presentation of a way to improve the prevention and repression of cybercrimes, guaranteeing the safety of users.

Keywords: Internet. Cybercrimes. Cyberculture. Investigation Procedures. Legislation**.**

SUMÁRIO

1 INTRODUÇÃO

A Internet aumentou consideravelmente a troca de informações por permitir uma comunicação instantânea com qualquer lugar desde que tenha acesso a rede, quebrando as barreiras territoriais e geográficas, entretanto, pessoas mal-intencionadas podem corromper a finalidade da rede para praticar delitos e infrações penais, que são conhecidos como “Crimes Cibernéticos”.

Ademais, dentre inúmeros perigos que se pode encontrar no uso e navegação de aparelhos eletrônicos na internet, vale ressaltar os materiais impróprios e/ou ofensivos, as pessoas de má-fé, o furto de identidade e/ou perda de dados, a invasão da privacidade, a propagação de conteúdos falsos e os obstáculos para identificar a vontade subjetiva de outrem e assegurar a discrição.

Aliado aos riscos elencados, há a falsa sensação de segurança que a tela de um equipamento para acessar a internet passa para seus usuários, uma vez que pode ser acessada em lugares que aqueles que navegam na rede considerem seguros e livre de perigos.

Tendo em vista essa nova realidade e as tentativas de regulamentar sobre a matéria, foi promulgada a Lei nº 12.965/2014, também conhecida como o Marco Civil da Internet, que até a presente data ainda é considerada a legislação primordial sobre ciberdireito no Brasil, a qual foi elaborada para suprir as lacunas no ordenamento jurídico quanto aos crimes cibernéticos. Contudo, apenas uma legislação nacional não é suficiente para tratar sobre toda a matéria envolvendo delitos virtuais, é preciso observar também a legislação internacional, tendo em vista que a internet não possui limites geográficos e as condutas danosas podem atingir indivíduos em todos os lugares do mundo, não necessariamente nas fronteiras territoriais em que está o autor do fato criminoso.

Muitas cidades norte-americanas empregam a elevada capacidade de encadeamento de dados para prevenir crimes. Uma das ferramentas usadas como meio para prevenção é o *Big Data*, que atua como uma forma de evitar delitos por meio de padrões obtidos pela coleta de dados de todas as ocorrências policiais já registradas, juntamente com as características comuns aos criminosos, as formas e o *modos operandi* dos delitos.

Diante do exposto, o problema que ensejou essa pesquisa decorre dos efeitos causados pelas subculturas criminais na internet e das facilidades existentes na rede

da *deep web* para a prática de delitos. Nessa ótica, considerando os inúmeros casos de violação de direitos no ciberespaço e o efeito desinibitivo que a internet provoca nos usuários, as medidas protetivas estatais vigentes continuam sendo eficazes e suficientes para resguardar os bens jurídicos ou se faz necessário a elaboração de uma nova legislação mais específica?

Insta salientar que ainda está presente no meio social a sensação de impunidade para os criminosos virtuais, já que para ser possível uma proteção eficaz dos direitos no ciberespaço, imperioso se faz evidenciar a necessidade da elaboração de leis mais específicas que regulamentem o assunto, uma vez que o marco civil da internet e as demais leis criadas abordando o tema, não dispõem com objetividade e detalhes sobre a maioria dos crimes e das condutas ilícitas praticadas na internet, deixando lacunas que são supridas pelo uso do instituto da analogia para enquadrar os delitos ao Código Penal e aplicar as penas nele previstas.

Dessa forma, é imprescindível que seja sancionada uma nova lei regulamentando sobre o assunto, com foco na área tecnológica, estabelecendo regras para controlar os comportamentos e ações dos indivíduos no ciberespaço respeitando os princípios constitucionais basilares, principalmente na parte da *deep web*, onde se encontram formas de trocar informações sigilosas que proporcionam a prática constante de diversos crimes.

Ademais, por causa das inúmeras formas de manter o anonimato e se esconder na internet, os procedimentos de investigação dos crimes digitais encontram dificuldades de identificar os agentes delitivos e, por esse motivo, necessitam de técnicas e mecanismos mais eficazes no combate dessas práticas.

Diante do exposto, o objetivo geral deste trabalho é averiguar os reflexos causados pela internet dentro da sociedade brasileira quanto a proteção e a violação de direitos diante do efeito desibinitivo online relacionado a subcultura criminal, buscando ponderar se mediante a ausência de legislação específica que englobe todas as práticas delitivas cometidas na seara virtual, o poder judiciário possui meios de aplicar o direito adequado ou se essa ausência prejudica o direito do tutelado, gerando insegurança jurídica e o sentimento coletivo de impunidade.

Para a consecução desse objetivo geral, foram listados como finalidades específicas: discutir sobre os cibercrimes na *deep web* e as dificuldades jurídicas de determinação da autoria delitiva; discorrer sobre as legislações brasileiras vigente aplicáveis aos crimes virtuais e a analogia ao código penal utilizada como forma de

suprimento de lacunas legais; e apresentar noções sobre as ameaças e os procedimentos de investigação realizados no Brasil no tocante aos cibercrimes, ressaltando a utilização do *Big Data* como meio preventivo.

Este estudo tem natureza exploratória, sendo utilizado o método de pesquisa hipotético-dedutivo, uma vez que visa demonstrar os efeitos que a internet e suas inovações ocasionaram quanto a violação de direitos na esfera digital, confrontando com os métodos existentes para prevenir e reprimir essas condutas criminosas.

Para obtenção dos dados necessários, foi adotada a técnica bibliográfica-documental para obter maiores informações sobre os crimes cibernéticos praticados na atualidade, bem como, observar o marco civil da internet e as demais legislações que tratam sobre o tema, relatando sobre as possíveis consequências que a falta de uma legislação específica que regulamente e resguarde os bens jurídicos de forma eficaz na seara virtual da mesma forma que o é na “realidade”.

Inicialmente, será apontada uma breve explanação sobre o surgimento da internet e suas camadas. Depois de feitas as primeiras considerações, abordaremos a definição e as classificações dos crimes virtuais, bem como as características e as denominações dos sujeitos ativos. Mais adiante, serão expostas as leis que versam sobre os cibercrimes e, por fim, demonstrados os procedimentos de investigação dos delitos cibernéticos, ressaltando as dificuldades enfrentadas durante a resolução do inquérito e apresentando os benefícios do *Big Data* como forma de aperfeiçoar e provem maior efetividade aos métodos investigativos.

2 CONHECENDO A *WEB*

Com a multiplicação e aperfeiçoamento dos instrumentos tecnológicos utilizados como meios de comunicação, a interação humana passou a ocorrer de forma mais digital, por intermédio de uma máquina ligada à internet.

Historicamente, conforme Wendt e Jorge (2012, p. 5) o precedente mais distante do advento da informática ocorreu em 1946, quando foi desenvolvido o primeiro computador digital, que foi nomeado *Electronic Numerical Integrator and Computer* – ENIAC, em português, computador integrador numérico eletrônico.

Mais adiante, na busca por um aparelho eletrônico que possuísse comunicação em período partilhado, foi criada uma agência para realizar pesquisar e elaborar projetos para a rede – denominada de ARPANET – que se fixou com a ideia de desenvolver uma conexão capaz de se conectar aos outros computadores, mesmo que estejam a longa distância. (LIMA, 2014)

Entretanto, apenas com a criação do conhecido “WWW” ou World Wide Web que de fato passou a ser associada a internet que conhecemos hoje.

No Brasil, a internet chegou em 1981 para o setor acadêmico por meio da *Bitnet,* que interligava universidades locais aquelas instituições sediadas nos Estados Unidos. Posteriormente, em 1995 foi estabelecido o serviço de internet comercial destinada a usuários domésticos e empresas, a tornando tendência no país e a popularizando cada vez mais. (MACEDO, 2017)

Desse modo, Inellas (2004, p.3) conceitua a internet como sendo uma rede de computadores conectada a outra rede que se comunicam entre si através de um sistema lógico de códigos e endereços que proporcionam a troca de informações.

Atualmente, o consumo e acesso à internet ainda vem crescendo e conectando mais pessoas a rede. Uma pesquisa realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – CETIC (2018, p.105) constatou que cerca de 70% da população usam a internet, o que equivale a 126,9 milhões de pessoas, os dados se referem a pesquisa TIC Domicílios que afere sobre a conexão com à internet nas residências do país. Também constatou que entre os usuários de Internet, quase a totalidade utilizou a rede pelo telefone celular, com percentual de 97%.

Cumpre destacar que segundo um estudo realizado em uma parceria da We Are Social com a Hoopsuite (2019, p. 1), “o Brasil é o segundo país do mundo que

passa mais tempo conectado à internet e revela que o brasileiro fica conectado em média por nove horas e vinte nove minutos todos os dias, isso significa que, dos 365 dias do ano, 145 deles os brasileiros estão online na rede". Mas, em que consiste a internet?

Silva et al (2020, p. 229) aponta que "a internet compreende todos os servidores, computadores e outros dispositivos conectados juntos em uma rede de redes e pode ser dividida em dois elementos: o *Surface Web* e a *Deep Web*.".

O primeiro componente, chamado *surface web* (*web* superfície), representa uma rasa camada de todas as páginas e conteúdos que são disponibilizados online, pois sua navegação ocorre apenas pelos sites indexados, ou seja, que são localizados através dos mecanismos de busca comuns, sendo o Google um dos mais conhecidos.

Segundo Lins et al (2018, p. 4) ocorreram diversas formas de indexação no decorrer do tempo, através de escalas de palavras associadas a um contexto geral ou número de links que referenciam determinado site. Atualmente, a valorização de um site e sua posição na *surface web* é determinada por algoritmos recursivos que dão peso à referenciação, quanto mais referências maior a importância.

Por sua vez, o outro elemento da internet denominado *deep web* (w*eb* profunda), corresponde a todos os sites não listados e ordenados na rede, ou seja, que não podem ser acessados através dos mecanismos normais de pesquisa e dos quais precisam de algum método específico de acesso, pois seus endereços eletrônicos não são páginas da "www", exemplifica Lins et al (2018, p. 2):

> Por exemplo, os rastreadores dos mecanismos de busca (Web crawlers) podem nunca indexar uma página simplesmente porque nenhuma outra página rastreada anteriormente tinha um link para ela. Ou então, pode ser que a página exija algum tipo de autenticação, como um login e senha, a necessidade de preencher um formulário de pesquisa e clicar em enviar, ou até mesmo exigir um determinado certificado de segurança. Fora isso, se uma página contiver conteúdo ilegal, o Google não vai querer que o conteúdo apareça nos resultados da pesquisa, então não o indexa. E por fim, se o criador de uma página não quiser que ela seja indexada por mecanismos de busca populares, ele pode incluir um arquivo robots.txt adequado, que instrui os rastreadores a não indexarem a página (Protocolo de Exclusão de Robôs).

Dessa forma, a *deep web* é um ambiente virtual utilizado por usuários específicos que detêm as chaves de acesso e que, por possibilitar a troca de informações sigilosas, torna-se um lugar atrativo para os criminosos cibernéticos, mas não é um ambiente onde circula apenas matéria ilegal, ao contrário, grande parte do

material que é disseminado nesta rede é lícito e útil, na medida em que engloba sistemas bancários, empresariais, acadêmicos e de e-mails, entre outros conteúdos de acesso um pouco mais complexo em virtude de sua natureza ou porque não são localizados em uma procura normal.

Entretanto, a parte da *deep web* que é sim de conteúdo anônimo e, ocasionalmente, ilegal é denominada de *dark web* (*web* escura) e seu acesso exige programas próprios que fornecem aos usuários condições legais de garantir a privacidade na rede.

Sob essa ótica, Monteiro e Fidêncio (2013, p. 37) esclarecem que:

> Como nada é tão simples nos objetos contemporâneos, outra Web emerge, considerada Dark Web (the dark side of the cyberspace) ou a invisível de fato, posto que servidores e a navegação feita sob o anonimato fazem a dobra underground do ciberespaço.

Nesse contexto, pode-se conceituar a *dark web* como uma parcela da *deep web* composta por um conjunto de sites, fóruns e comunidades dos mais variados assuntos que não são acessados pela rede convencional, pois o ingresso está condicionado ao uso de ferramentas e mecanismos de segurança específicos para viabilizar o anonimato dos usuários.

Como mencionado acima, a web escura é aquela que requer a instalação de softwares específicos e o uso de "códigos secretos" para finalmente conseguir acessar os conteúdos, um dos mais utilizados é o *The Onion Routing* - TOR, pois através de ramificações virtuais dificulta e encobre a identificação dos usuários e seus equipamentos para acessarem determinado conteúdo, ou seja, funciona realizando o embaralhamento do sinal de origem e destino dos usuários dificultando o rastreamento dos internautas e permitindo o anonimato.

Cumpre esclarecer, que desde as primeiras conexões com a ARPANET durante o período da guerra fria que foram desenvolvidas redes secretas para envio de informações sigilosas. Em 1990, o Laboratório Central da Marinha para Segurança de Computadores através dos cientistas, Paul Syverson, Mike Reed e David Goldshlag desenvolveram o *The Onion Routing* - TOR que em português significa “Roteamento de cebola”. Esse software, como a própria denominação explica, é uma forma de comunicação onde “cada roteador pelo qual a mensagem ou conexão passa criptografa um pedaço ou uma camada”. Dessa forma, o usuário precisa passar por

cada parte, decodificando as etapas, para só então chegar a objetivo. (KLEINA, 2018, p. 2)

Além do TOR, há outros softwares que também são grandes redes e atuam com o mesmo objetivo de garantir o anonimato dos internautas, cada um com seus protocolos de acesso, mas com atuações semelhantes, já que estabelecem inúmeros internautas para servir de intermediários em cada conexão.

Insta salienta que “a maioria dos domínios da *dark web* são compostos por *strings* de letras e números sem o menor sentido, e apenas quem possui os domínios e credenciais completos é autorizado a entrar nesses sites”. (GOGONI, 2019, p. 2)

Por isso, que para navegar na *dark web* é necessário a utilização de instrumentos para criptografia e proteção de dados, tendo em vista, a *web* sombria ser um ambiente de difícil controle, onde seus usuários são constantemente atacados.

2.1 Ciberespaço e introdução aos crimes virtuais

A nova realidade social se apresenta pela revolução tecnológica, onde todos os cidadãos estão de alguma forma conectados através da internet e com esse novo cenário, as visões do que é real e do que é virtual estão cada vez mais interligadas, não sendo mais possível dissociar uma da outra.

O ambiente virtual é chamado de ciberespaço, que de acordo com Lévy (1999, p. 92) é definido “como o espaço da comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores”.

Esse lugar virtual não apresenta barreiras geográficas ou se limita por fronteiras, sua característica marcante é por ser um espaço sem dimensões, onde a comunicação se dá em tempo real, de forma instantânea. Conforme explica Lemos:

> O ciberespaço é concebido como um espaço transnacional onde o corpo é suspenso pela abolição do espaço e pelas personas que entram em jogo nos mais diversos meios de sociabilização [...] Assim sendo, o ciberespaço é um não-lugar, uma utopia onde devemos repensar a significação sensorial de nossa civilização baseada em informações digitais, coletivas e imediatas. Ele é um espaço imaginário, um enorme hipertexto planetário (LEMOS, 2008, p.128).

Entretanto, essa rapidez na troca de informações e conteúdos diversos, acarretou um aumento significativo na área criminal através dos chamados crimes virtuais, cibernéticos ou digitais. Para Augusto Rossini (2004, p. 110):

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

Nesse sentido, podemos compreender esses delitos como condutas típicas, antijurídicas e culpáveis que são praticadas com o uso das tecnologias ou contra o próprio sistema informático.

Pinheiro (2010, p. 46) conceitua os crimes virtuais como sendo toda e qualquer conduta de acesso não autorizado a sistemas informáticos, que viole direitos individuais ou coletivos, se propagando de diversas formas, dentre elas: “as ações destrutivas de sistemas, a interceptação de comunicações, modificações de dados, terrorismo, entre outras”.

Segundo Oliveira et al (2017, p. 122), basicamente o crime virtual se traduz na prática de uma “conduta ilícita através de um computador ligado a internet, que pode ser próprio ou impróprio”, mas que em razão da abrangência e da falta de fronteiras no ciberespaço, são de difícil resolução e identificação do infrator.

Os delitos de informática próprios ou puros são aqueles em que o meio e o fim pretendido pelo infrator encontram-se no próprio campo da informática, ou seja, ele utiliza-se da informática para danificar ou atingir elementos integrantes da própria informática, como os *softwares*, *hardwares* e os dados contidos em quaisquer chips.

Já os crimes virtuais impróprios são aqueles cometidos utilizando o computador, mas seu fim é atingir bens jurídicos diversos da seara tecnológica, ou seja, são condutas ilícitas já tipificadas no ordenamento jurídico que, depois da modernização na informática, estão sendo praticadas com o uso das novas tecnologias como mais uma forma para realização do crime.

Para Greco Filho (2000, p. 85), a classificação dos crimes virtuais seria decorrente da dissociação entre as condutas criminosas realizadas por meio da internet e contra ela enquanto bem jurídico. Sua justificação estaria baseada na concepção da conduta desses delitos, considerados de resultado de conduta livre e que, portanto, seria relevante apenas o evento fático que provocou a lesão.

Explica Vladimir Aras (2001, p.51), de uma forma diversa, que a divisão se daria em três categorias, uma onde o computador “constitui a necessária ferramenta de

realização pela qual o agente alcança o resultado legal", outra incluindo "todos aqueles comportamentos ilegítimos que contestam os computadores, ou mais precisamente, seus programas" e a última seria a união de todas as possíveis condutas delitivas envolvendo o computador em si.

Sobre essas subdivisões, Monteiro Neto (2008) afirma que são utilizadas para dissociar os delitos convencionais dos cibercrimes e, ressalta a importância dessa diferenciação ao mencionar que os crimes já tipificados no código penal, mesmo que sejam praticados pelos meios virtuais ou utilizando equipamentos eletrônicos, não são qualificados como crimes digitais, por se tratar apenas de uma modernização nos atos executórios, cabendo meramente o enquadramento nas qualificadoras ou como modalidade de aumento de pena, já que a essência da ação proibitiva do tipo permanece a mesma.

Além das especificações acimas, cumpre ressaltar a singularidade dos crimes virtuais quanto aos seus sujeitos ativos, já que são representados por pessoas que detêm conhecimentos específicos sobre sistemas tecnológicos. Tais criminosos empregam suas habilidades diversificadas para executar ataques a empresas, acessar dados pessoais e bancários, praticar fraudes, extorsões e assédios, entre outras práticas ilegais.

Conforme Vianna (2003, p. 9) esclarece, para se tornar um criminoso cibernético é preciso ter conhecimento sobre a atividade ilegal a ser desenvolvida, característica essa que faz tais delitos divergirem dos crimes clássicos – por exemplo, o homicídio – que não necessitam de saber técnico para sua prática, ao contrário dos cibercrimes que exigem compreensão dos aparelhos eletrônicos e domínio sobre a navegação na internet.

Mas, insta salientar, que apesar da maioria dos cibercrimes serem praticados por indivíduos especialistas sobre a internet, nos casos de crimes virtuais impróprios, há sim a possibilidade do agente delitivo ser uma pessoa sem conhecimento técnico sobre informática, pode ser uma pessoa comum sem grandes conhecimentos sobre informática, programação e internet.

Corroborando com o exposto, Inellas (2004) relata a mudança ocorrida entre os crimes virtuais primários e os atuais. No primeiro caso, esclarece que quase a totalidade dos delitos eram praticados por pessoas versadas em informática; já os delitos contemporâneos não há mais uma constância quanto os aspectos pessoais dos criminosos, na medida em que qualquer indivíduo com acesso a internet, mesmo

sem conhecimentos sobre informática pode cometer cibercrimes.

Exemplifica Lima (2018, p.75) em seus ensinamentos que:

> A tecnologia tem sido um fator bastante utilizado em ambos os lados do enredo criminal: na perpetração de crimes na internet e na reação estatal de combate. As redes sociais tem sido fortes aliadas para os crimes menos elaborados, tais como os que são cometidos através do intercâmbio de mensagens de texto, imagens e vídeos. Entretanto, para crimes mais sofisticados, como a derrubada de um site de comércio eletrônico ou de uma instituição financeira, pode ser necessários conhecimentos de ataque e camuflagem no meio virtual. Caluniar alguém por email ou por uma rede social não requer muita habilidade técnica quanto acessar o site do FBI ou da NASA e obter informações confidenciais por eles protegidas em suas respectivas bases de dados. Muitas vezes, o entendimento de criptografia, programação e técnicas de invasão e até de telefonia é exigido.

Desse modo, é preciso esclarecer que existem algumas nomenclaturas para caracterizar os sujeitos ativos dos crimes virtuais, as principais são *hacker* e *cracker*. O primeiro termo é utilizado erroneamente quando relacionado a todo e qualquer ato ilícito praticado na internet, pois, ao contrário do senso comum, os *hackers* são pessoas dotadas de conhecimento sobre informática, com domínio sobre as falhas de segurança dos sistemas digitais, mas sem a intensão de causar danos ou avarias.

Conforme Nogueira (2008) são indivíduos que costumam praticar invasões a sites e páginas virtuais com a finalidade apenas de testar suas habilidades e demonstrar seus conhecimentos na rede, sem a intenção de causar prejuízos, o que acarreta a admissão dessas pessoas em grandes empresas ou órgãos governamentais para descobrir fragilidades, prever e combater ataques em seus sistemas.

Já o termo *cracker* ou também conhecido como “chapéu negro”, é a correta denominação para os internautas que apresentam condutas e ações ofensivas na rede, representando aqueles que também possuem compreensão sobre tecnologia da informação e suas vulnerabilidades, mas, diferente dos *hackers*, esses usam seus conhecimentos técnicos para obter vantagens. (ASSUNÇÃO, 2008)

Kunrath (2017) aponta que além das denominações supracitadas, também é possível encontrar uma subcategoria dos *cracker*s com os chamados *phreaker* que são aqueles indivíduos especializados em coletar informações de telefonia e dados telefônicos sem autorização.

Por fim, outra classificação relevante e comumente utilizada por usuários da internet mal-intencionados, são os nomeados engenheiros sociais, que podem

“aproveitar-se das fraquezas das pessoas para obter as informações com ou sem o uso da tecnologia”. (PAIXÃO et. al., 2015, p. 5)

2.2 Riscos na internet e dados estatísticos

O amplo acesso da população à Internet, em paradoxo à falta de conscientização da necessidade de prevenção neste espaço, reflete a vulnerabilidade que a rede expõe os internautas, na medida em que muitas pessoas fazem o uso dela sem atentar para os perigos de invasões ao computador, sem utilizar softwares de segurança e sem verificar a credibilidade dos sites.

Os programas maliciosos usados para facilitar invasões são chamados de “*malware*”, a palavra deriva da junção dos termos *“malicious”* e *“software”*, são utilizados para diferentes finalidades, tais como: infiltrar um computador ou sistema, causar danos e apagar dados, roubar informações, divulgar serviços, entre outros”. (ARAUJO, 2018, p.94)

Atualmente, há uma grande variedade de códigos maliciosos para violar servidores eletrônicos, das mais variadas formas, cada um com sua função específica. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br (2012) apontou como os principais: o vírus, o *worm*, o *bot* e *botnet*, o s*pyware,* o *backdoor,* o t*rojan* e o *rootkit.*

Esclarecendo um pouco sobre cada um desses *malware* seguindo o CERT.br (2012)*,* temos que: o vírus é um programa que se multiplica sozinho depois que o arquivo infectado for executado, se espalhando para os demais aplicativos dentro do servidor; já o *Worm,* apesar de ser também um programa que se prolifera por si só e necessita ser executado, diferente do anterior por ele não se propagar apenas no mesmo servidor, ou seja, ele irá localizar outros aparelhos desprotegidos e se auto reproduz pela rede, tornando o computador contaminado em transmissor; sobre o *bot* e *botnet,* temos que o primeiro é similar ao *Worn*, mas com esse tipo de código malicisioso também é possível o controle à distância do dispositivo infectado sem conhecimento do usuário; já o *botnet* é quando ocorre a manipulação de um conjunto de aparelhos contaminados, formando uma rede.

Quanto aos demais apontados pelo CERT.br (2012), temos que o *spyware* é o denominado “programa espião”, ou seja, como o próprio nome sugere, é utilizado para vigiar o funcionamento de um sistema e obter informações; o *backdoor* é um malware

que garante o regresso ao dispositivo atacados além do procedimento normal de invasão; o t*rojan* também conhecido como “cavalo de troia”, é um programa duplo, na medida em que realiza as atividades para os quais foi desenvolvido e outras que tendem a prejudicar o desempenho do aparelho ou violar a privacidade e segurança dos dados; e por fim, o *rootkit* é a reunião dos mecanismos programados para assegurar a permanência do invasor no dispositivo, além de ocultar suas ações e seu malware dos demais usuários.

Insta salientar que o *“phishing”* é um dos golpes mais comuns na internet e se apresenta como uma das modalidades de obter dados pessoais e bancários dos indivíduos que acessam a internet, para cometer alguma forma de fraude. Se caracteriza pelo modo como obtém o conteúdo, qual seja: através do envio de mensagens eletrônicas sobre diferentes assuntos, no intuito de fisgar algum usuário que acessar as páginas falsas. (CERT.br, 2012)

A recente pesquisa realizada pela PSafe (2020, p. 1), explica que um em cada cinco brasileiros já sofreu golpe de *scammers*, o que representa 22,6 milhões de potenciais vítimas em todo o território nacional. Dentre elas, 5,9% foram chantageadas; 4,8% tiveram suas contas na internet hackeadas; 3,9% tiveram prejuízo financeiro; 2,4% tiveram fotos íntimas expostas; e 2,0% tiveram dados vazados.

Em outra pesquisa a PSafe (2019, p. 1) revela que 51,3% dos usuários entrevistados apontaram o número de telefone como sendo o dado mais utilizado de forma fraudulenta, seguido de credenciais de redes sociais (44,3%), credenciais de e-mail (37,1%), CPF (26,0%) e número de cartão de crédito (19,3%).

Segundo dados da DFNDR LAB (2019, p. 1) as previsões de cibersegurança com os principais golpes e ameaças que estarão em alta no Brasil em 2020 são: o aumento no número de clonagem de *Whatsapp*; o golpe de emprego falso; o uso de *Bots* em redes sociais para automação e divulgação de golpes; e o crescimento de *Trojans* bancários no google play.

Conforme CERT (2019) apontou que durante o ano de 2019 o *scan* foi o tipo de ataque mais reportado no período, correspondendo a 46,81% das denúncias, uma vez que por meio dessas notificações de varredura é possível a identificação das possíveis vulnerabilidades dos serviços habilitados nos computadores.

Além disso, também foram reportados DoS (34,42%) e *worm* (11,48%), que compreendem notificações de ataques de negação/serviço e atividades maliciosas

relacionadas com o processo automatizado de propagação de códigos maliciosos na rede, respectivamente.(CERT, 2019)

Nessa ótica, observa-se que os crimes cibernéticos estão presentes diariamente em nosso cotidiano e em todos os ramos sociais e profissionais, portanto, devem ser tipificados especificamente para que os danos produzidos como consequências desses delitos sejam evitados.

3 A CIBERCULTURA E OS INTERNAUTAS

A cibercultura é um termo utilizado para denominar as interações sociais que se desenvolvem no ciberespaço. Esse espaço virtual não criou novas relações sociais, o que ocorreu foi uma amplificação das formas de interação entre os indivíduos ante o advento das novas tecnologias e dos avanços nos meios de comunicação, ou seja, o que antes era realizado apenas no mundo físico passou a acontecer através de códigos e especificidades próprias que permitem simultâneos relacionamentos virtuais e diálogos sem a presença física do interlocutor.

A doutrina diz que a cibercultura pode ser compreendida como “a presença (virtual) da humanidade em si mesma” e, por isso, as interconexões são parte fundamental desse processo. “Para a cibercultura, a conexão é sempre preferível ao isolamento” (LÉVY, 1999, p.127).

Em decorrência da popularização da internet e pelo surgimento da cibercultura, com as interconexões no ciberespaço e o compartilhamento de informações ocorreu a formação das chamadas “comunidades virtuais” que Lévy (1999) define como sendo um conjunto de afinidades e interesses sobre determinados assuntos com o intuito de partilhar conhecimentos independentemente da localização geográfica dos internautas.

Entretanto, essa cultura virtual apesar de ter diversos benefícios, ocasionou o aumento da criminalidade através dos cibercrimes, por ser a internet um ambiente flexível, repleto de dados pessoais e financeiros, com locais de acessos restritos e meios de garantir o anonimato, onde aparentemente os usuários se demonstram mais propensos a atos e condutas desviante.

Existem diversas teorias que buscam explicar o criminoso e suas motivações, contudo, nesta pesquisa vamos analisar o cibercriminoso pela teoria da subcultura criminal juntamente com a pesquisa sobre os comportamentos dos indivíduos na

internet, denominado “efeito desinibição online” do psicanalista John Suler.

Em termos gerais, a subcultura se refere as atividades e os procedimentos de relacionamento interpessoais de uma específica parcela minoritária da sociedade associada, com princípios e valores próprios que regem seus membros de modos diversos dos padrões sociais pré-estabelecidos como “gerais e comum a todos”.

O vocábulo *subcultura* é um substantivo feminino e tem como definição um “grupo de pessoas com particularidades determinadas que desenvolve ou busca desenvolver uma divisão cultural menor”. Ademais, corroborando com os termos gerais, também pode ser definida como “grupo social menor com características, hábitos e identidades próprias que, de certa forma, se afasta de outro grupo dominante, mas mantém algumas de suas particularidades”. (DICIO, 2020, p.1)

Silva (2005, p. 5) esclarece que em tese cada indivíduo tem sua subcultura, sendo as “estruturas culturais (conjunto de representações, de valores, de hábitos, de regras sociais, de códigos simbólicos, de comportamentos) interiorizados pelo indivíduo podem ser elementos explicativos de comportamentos pessoais e sociais”.

A internet permite uma liberdade de expressão que não pode ser medida, dessa forma, alguns internautas interpretam essa condição como um meio de expressão para confessar sentimentos e/ou segredos, em outras palavras, o espaço virtual se revela como uma ampliação da consciência humana que se mostra como um ambiente para que “todo tipo de fantasias e reações de transferência sejam projetadas nesse espaço”. (SULER, 1999, p.1)

Entretanto, nem sempre as emoções e os conteúdos expostos são positivos, já que a maioria dos indivíduos usa o ambiente virtual para extravasar suas frustrações e raivas, publicar palavras agressivas, visitar sites de conteúdos impróprios ou ilegais, ou seja, fazem o que não têm coragem de fazer fora da internet.

Essa sensação de intimidade que a rede passa para os internautas é o que foi denominado de “desinibição online”. Mas o que causa esse efeito?

O pesquisador John Suler (2004) aponta seis fatores como causas: o anonimato dissociativo, a invisibilidade, assincronicidade, introjeção solipsista, imaginação dissociativa e a autoridade minimizadora.

A primeira causa, como o próprio nome explica, está no fato de a internet proporcionar aos usuários da rede a qualidade/condição de manter a identidade escondida e protegida de terceiros, dessa forma, algumas pessoas tendem a possuir uma identidade virtual independente da real, ocasionando uma sensação de

confiança. Suler (2004, p.1) revela que quando as “pessoas têm a oportunidade de separar suas ações do mundo real e da identidade, elas se sentem menos vulneráveis quanto à abertura (...) as pessoas podem até se convencer de que esses comportamentos "não são eu mesmo. Na psicologia, isso é chamado de "dissociação".”

Aliado ao anonimato, auxilia na desinibição o fato de não ter contato visual entre as pessoas, poder navegar na rede sem ser visto, sem revelar suas características físicas pessoais, nem expressões faciais no desenvolver de uma conversa, provocando mais conforto para aqueles que desejam expor conteúdos pessoais e coragem fazer o que no mundo real sensações como timidez, baixa autoestima ou outros fatores intrínsecos não permitiam que fossem realizadas.

Conforme Priberam (2020, p. 1) a assincronicidade é um substantivo feminino que significa “qualidade do que é assincrônico que, por sua vez, é aquilo que não se realiza ao mesmo tempo que outro”. Na internet, algumas formas de comunicação não são instantâneas, pois apesar da mensagem ser recebida quase no mesmo instante do seu envio, ela pode levar algum tempo para ser lida e respondida. Em resumo, Suler (2004, p. 2) explica que nas mensagens e e-mails “as pessoas não interagem entre si em tempo real. Outros podem levar minutos, horas, dias ou até meses para responder a algo que você diz. Não ter que lidar com a reação imediata de alguém pode ser desinibidor”.

O quarto fator apontado como causa para a desinibição online ocorre quando o internauta projeta a mensagem que leu na internet para sua mente, como uma voz interior ou como um narrador de uma história, ou seja, “como se a presença e a influência dessa pessoa tivessem sido assimiladas pela psique do leitor”. De forma consciente ou inconsciente o receptor da mensagem tende a imaginar um rosto para o remetente, criar um personagem “moldado em parte pela maneira como a pessoa realmente se apresenta por meio da comunicação de texto, mas também por nossas expectativas, desejos e necessidades”. (SULER, 2004, p. 2)

Sob essa ótica, a imaginação dissociativa está intimamente ligada a introjeção, pois, a partir do momento em que o internauta projeta um personagem em sua mente decorrente da comunicação com outrem, está consciente ou inconscientemente transformando indivíduos reais em “personagens imaginários” que, por essa razão, interagem em um espaço de fantasia/imaginário e o que acontece neste ambiente (que, no caso, é o ambiente virtual da internet) são ações e interações separadas das

exigências e responsabilidades do mundo real, ou seja, os usuários acreditam que não serão responsabilizados pelo que acontece na rede.

Por fim, o último fator da desinibição está no fato de todos os indivíduos se verem como iguais, terem as mesmas oportunidades, independentemente da aparência, poder aquisitivo ou qualquer outra condição pessoal de distinção que tenha no mundo real. Suler (2004, p.3) explica que “as pessoas relutam em dizer o que realmente pensam, diante de uma figura de autoridade (...) Mas on-line, no que parece um relacionamento entre colegas - com as aparências de "autoridade" minimizadas - as pessoas estão muito mais dispostas a falar ou se comportar mal”.

Lucena (2012, p. 2) aponta como desfecho sobre o estudo de John Suler que realmente há uma separação na maneira de se comportar dos indivíduos no mundo virtual e no mundo físico, o que provoca uma dupla personalidade, que por ventura, essa nova conduta surge com princípios e valores diversos dos constituídos pela sociedade.

Exemplificando a repercussão da nova conduta na vida dos internautas:

> O efeito de desinibição online afeta os usuários de internet de modo a dessensibilizar suas noções de empatia, respeito, convívio social e direitos humanos, tornando-os suscetíveis à prática de crimes cibernéticos – ou mesmo crimes comuns, só que praticados na web – sem que tenham a noção exata de que transgridam leis e de que estão sujeitos a suas devidas penas. (TASHINO, 2015, p. 18)

Nesse sentindo, todos esses fatores que levam a desinibição online proporcionam aos indivíduos que acessam a internet um ambiente para se expressarem abertamente e realizar as coisas que não fariam normalmente. Entretanto, nem todas as pessoas que navegam na rede têm boas intenções, grande parte dos acessos realizados são por aqueles que desejam expressar mensagens hostis e agressivas, que não querem assumir responsabilidades por seus atos ou palavras e que apresentam personalidades desviantes quando ingressam no ciberespaço, norteados pela falta de moralidade e boa-fé.

No âmbito da Psicologia Criminal, como bem assinalado por Debora Spagnol (2015, p. 1), “[...] que o perfil dos criminosos cibernéticos é composto por sujeitos que se acreditam imunes à punição e menos culpados e culpáveis, já que na maior parte dos crimes não possui contato com a vítima”.

Sob essa ótica, destaca-se a falta de percepção dos ciberdelinquentes sobre

as consequências que suas ações provocam, aparentemente, não têm ciência dos próprios atos, não tendo noção do impacto que suas opiniões ou atitudes possam causar às vítimas. Contudo, embora tais condutas sejam praticadas no ciberespaço, por trás das telas existem pessoas que sofrem diretamente com seus efeitos.

Além dos aspectos intrínsecos dos sujeitos ativos dos crimes virtuais acima mencionados, Florêncio Filho (2008) esclarece que o perfil da maioria dos agentes se apresenta como pessoas jovens, com aptidões e técnicas específicas de uso de dados e conteúdos da internet, pertencentes as camadas sociais consideradas como médias e altas.

Acrescenta Paesani (2010) ao mencionar Strano que esses indivíduos são, em sua maioria, reclusos, insociáveis, não violentos e cometem delitos que não cometeriam fora do espaço cibernético.

Insta salientar, que a maioria dos criminosos virtuais também não apresentam histórico de outros ilícitos além daqueles cometidos na internet, suas personalidades podem ser distintas de quando o agente infrator está atuando no ambiente físico e quando está agindo através de seu perfil na rede.

Sob essa ótica, é possível observar que em alguns casos o próprio meio se torna o instrumento propulsor para o cometimento da conduta desviante, pois está provocando nos indivíduos alguns efeitos que tendem a facilitar os desvios na personalidade.

4 POLÍTICA DE PREVENÇÃO AOS CIBERCRIMES NO BRASIL

A partir da Revolução Industrial que a globalização e o avanço tecnológico vêm crescendo e avançando consideravelmente e com rapidez. Entretanto, o Direito e seus ramos jurídicos que têm o dever de acompanhar a sociedade e suas mudanças, não conseguem se adequar a todo esse contexto virtual-real.

Mesmo com tantos avanços, o Direito tem como uma de suas funções essenciais, acompanhar a sociedade e suas mudanças, contudo, no atual cenário é possível observar que a sociedade avança mais rápido que o Direito e que após tantas mudanças tecnológicas, ocorreu um descompasso entre a legislação atual e as evoluções tecnológicas.

Um dos intrigantes pontos que se deve indagar está no fato de não ter sido criado um novo ramo jurídico, apenas ocorreu à evolução do direito para o que foi

chamado “Direito Digital”, o que até agora foi caracterizado apenas como uma versão atualizada do direito diante da era digital. Nesse sentido, urge a urgência de uma atuação ativa do Estado e do Legislativo para elaborar meios necessários e mais focados na área tecnológica a fim de evitar e cessar as brechas que possibilitam a impunidade na esfera digital.

A primeira legislação que tratava diretamente sobre crimes virtuais é a Lei nº 12.737, de 30 de novembro de 2012, chamada de Lei dos Crimes Cibernéticos ou comumente conhecida como Lei Carolina Dieckmann, que foi elaborada para alterar o Código Penal e acrescentar alguns dispositivos regulamentando sobre crimes virtuais, dentre eles se destaca o artigo 154-A que define como crime a invasão de dispositivo informático, expressamente o texto determina que:

> 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. (BRASIL, Lei 12.737, 2012)

A invasão de dispositivo informático pode ser agravada se os dados obtidos ilegalmente são informações sobre comunicação eletrônica particular, segredos empresariais ou industriais, conteúdo sigiloso ou o controle remoto não autorizado do dispositivo invadido. Bem como, pode ter a pena aumentada caso o conteúdo obtido por meio da invasão for divulgado ou repassado.

Além do delito acima, a Lei nº 12.737/12 tipifica como infração penal a produção e comercialização de programas, aplicativos ou vírus de computador criados para a invasão aos dispositivos informáticos ou roubo de dados.

Juntamente com a Lei Carolina Dieckmann também entrou em vigor a Lei nº 12.735/2012 que determina a instalação de delegacias especializadas para o combate de crimes digitais.

Posteriormente, sentindo a necessidade de um aprofundamento e regulamentação maior sobre a matéria, o Legislativo criou a Lei nº 12.965 de 23 de abril de 2014, denominada de Marco Civil da Internet tem como objetivo “estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria”. (BRASIL, Lei 12.965, 2014)

O Marco Civil é a principal legislação sobre o uso da internet e reafirma a garantia constitucional de inviolabilidade da intimidade e da vida privada, além de assegurar aos usuários direitos como o sigilo nas comunicações (salvo por ordem judicial), publicação e clareza nos termos para quaisquer serviços de internet, detalhamento explícito sobre o armazenamento e manuseio dos dados pessoais, proteção contra repasse de dados, entre outros.

O ponto inovador presente na legislação supracitada está na proteção aos registros, aos dados pessoais e às comunicações privadas, sendo expostos apenas mediante requisição judicial. Ademais, decorrente desse resguardo legal, em caso de violação e publicação de conteúdo privado e pessoal, é possível a retirada do material da rede, também apenas com autorização judicial, exceto nos casos de violação à intimidade nos delitos de “pornografia de vingança”, onde as vítimas da exposição podem solicitar a retirada de forma direta aos sites ou serviços que abrigam o material.

Outra novidade disciplinada no Marco Civil foi a obrigatoriedade de os provedores armazenarem os dados dos usuários da internet e o cronograma de registros de acessos a rede, pelo lapso de tempo de 6 (seis) meses para provedores de aplicação e 1 (um) ano para provedores de conexão, com imediata exclusão após o decurso do prazo.

Vale ressaltar que as supracitadas informações fornecidas pelos provedores são de relevante valor nas investigações dos crimes virtuais, uma vez que podem detectar um cibercriminoso. Entretanto, com a obrigação de excluir os dados após o lapso temporal mencionado, o próprio texto legal apresenta uma barreira para identificação dos possíveis delinquentes e compromete o regular procedimento investigatório dos cibercrimes.

Ademais, o Decreto nº 8.771, de 11 de maio de 2016, também traz uma escusa para aqueles que não querem seus dados coletados pelos provedores, ao dispor em seu art. 11 que “o provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados”, ou seja, aqueles provedores que geram redes abertas (que não são centralizadas em uma só empresa) não têm como fornecer os dados de acessos, tornando um ambiente atrativo para os usuários que não desejam ser identificados.

Além das citadas leis, também tivemos a lei nº 11.829/2008 que modificou o Estatuto da Criança e do Adolescente (ECA) para acolher condutas vinculadas ao crime de pedofilia no ciberespaço. Outro texto legal foi o Decreto nº 7.962/2013 que

disciplinou sobre a proteção aos consumidores no comércio virtual, garantindo a responsabilização dos fornecedores no caso de quebra da relação de consumo.

A legislação mais atual versando sobre a temática é a Lei nº 13.709, de 14 de agosto de 2018, intitulada de Lei Geral de Proteção de Dados Pessoais – LGPD, que entrou em vigor na data de 18 de setembro de 2020, que conforme o seu artigo primeiro, disciplina sobre:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, Lei 13.709, 2018)

Vale ressaltar que os artigos da LGPD que versam sobre as sanções administrativas para quem desrespeitar as regras de tratamento de dados pessoais ainda não estão vigentes, tendo em vista o disposto na Lei nº 14.010/20, a qual, fixou a vigência das sanções a partir de 1º de agosto de 2021.

Sobre o conteúdo da LGPD, destaca-se o artigo 18 da referida lei onde estão disciplinados diversos direitos para os titulares dos dados, dentre eles: confirmar o tratamento dos seus dados, corrigir dados incompletos ou desatualizados, anonimização, bloqueio ou eliminação de dadosdesnecessários, portabilidade de dados, entre outros.

Diante desse quadro, temos que é muito cedo para afirmar se a LGPD será eficaz em todos os aspectos para os quais foi elaborada, portanto, pode-se dizer que apesar da tentativa de se adequar as evoluções sociais, o Direito ainda não atingiu o patamar de eficiência necessário para garantir segurança no ambiente virtual e preservar o convívio social harmônico.

Corroborando com o entendimento, Oliveira et al (2017, p. 9) ressaltam que mesmo sendo “essas normas específicas, não abrangem todo o campo de atuação dos criminosos da internet, ficando ainda algumas lacunas”. Ou seja, apesar do Marco Civil ser um grande avanço para a sociedade brasileira ainda não atingiu a eficácia jurídica esperada.

Maues et al (2018, p. 7) reafirma a impunidade pelos crimes virtuais em razão de muitas condutas delituosas continuarem sem tipicidade, além de ressaltar que apenas sancionar leis específicas não se faz suficiente para combater e prevenir a criminalidade virtual, deve-se ter mais participação estatal para o desenvolvimento de

programas de conscientização.

Cumpre ressaltar que, não há como quantificar de forma específica quantos crimes ocorrem na *deep web*, nem quantos casos ainda se encontram sem soluções, em razão da dificuldade de se rastrear nesse ambiente e da incerteza quanto ao seu tamanho e alcance de usuários.

Diante do exposto, observa-se que a legislação brasileira encontra-se desvinculada da realidade social e a ausência de maior previsão de incriminações por condutas na internet só aumenta o sentimento de impunidade, na medida em que, se tem dificuldade na apuração da autoria das condutas e novas formas de praticar delitos através do ciberespaço estão surgindo (FERREIRA, 2000, p. 236- 237). Portanto, vemos que as novas mudanças necessitam de regulamentações específicas e completas, além de fiscalização do legislativo para sua atualização sempre que inovações se apresentarem na sociedade.

A Internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como às necessidades de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio (PINHEIRO, 2010, p. 296-297).

Neste contexto, ressalta Borges et al (2015) que além das dificuldades de persecução penal pelas omissões legais, há também aquelas decorrentes da limitação da liberdade.

Diante disso, apesar das legislações elencadas acima disciplinarem sobre cibercrimes e ainda não abarca a totalidade de condutas delitivas praticadas no ciberespaço, o que ocasiona um sentimento generalizado de imunidade na internet, de um ambiente sem regras.

4.1 Legislação Internacional – Convenção de Budapeste

Por não existir barreiras para o alcance da internet e das ações dos usuários, é preciso observar também a legislação internacional, nesse sentido, Santo (2015, p.34) aponta a Convenção de Budapeste ou também conhecida como “Convenção sobre o Cibercrime” no qual tem como principal objetivo uma cooperação internacional para

combate aos crimes virtuais, visando avanços na seara penal para responsabilização dessas condutas ilícitas.

Em meados de 2001, foi realizada a Convenção sobre o Cibercrime na cidade de Budapeste, com a finalidade de instituir normas gerais para proteger a sociedade dos crimes virtuais. Esta convenção buscou a cooperação internacional e “o auxílio mútuo para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma electrónica de uma infracção penal”, assegurando que as modalidades de assistências não afetariam a aplicação das legislações internas. (BUDAPESTE, Convenção sobre Cibercrimes, 2001)

Após o preâmbulo, a Convenção de Budapeste apresentou breves conceitos para definir os elementos essenciais do texto, em seguida, apresentou as medidas para serem tomadas em caso de violação a nível nacional, ressaltando a autonomia da legislação interna, conforme dispõe: “Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno (...)”. (BUDAPESTE, Convenção sobre Cibercrimes, 2001)

No corpo do texto da Convenção de Budapeste (2001) foi disciplinado como infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos: o acesso ilegítimo, a interceptação ilegítima, a interferência em dados, interferência em sistemas e o uso abusivo de dispositivos. Além desses delitos, foram dispostas as infrações relacionadas com computadores preceituando as condutas que tendem à “falsidade informática” e a “burla informática”, bem como, as infrações relacionadas com pornografia infantil e as infrações relacionadas com a violação do direito de autor e direitos conexos.

Por fim, cumpre ressaltar o artigo 25 do tratado, quando dispôs sobre os princípios gerais relativos ao auxílio mútuo e determinou que o auxílio mútuo será “sujeito às condições fixadas pelo direito interno da Parte requerida ou pelos tratados de auxílio mútuo aplicáveis, incluindo os fundamentos com base nos quais a Parte requerida pode recusar a cooperação”. (BUDAPESTE, Convenção sobre Cibercrimes, 2001)

Sob essa ótica, faz-se imperioso destacar que a legislação internacional, principalmente na seara criminal cria os chamados mandados de criminalização, a legislação em si não tipifica nenhum crime só cria a responsabilidade para que os Estados elaborem suas legislações internas para tipificar esses crimes, preveni-los e

reprimi-los, portanto, a criação de uma legislação internacional em si não implica dizer que haverá efetivamente uma prevenção ou repressão dos crimes virtuais seria apenas uma declarção de boa vontade entre os estados.

Por fim, insta salientar que atualmente o Brasil se prepara para formalizar sua adesão à Convenção de Budapeste sobre Crime Cibernético, tendo aprovação do Presidente em vigor - Jair Bolsonaro - concedida no final do mês de julho e sendo encaminhado o processo de ratificação legislativa ao Congresso Nacional, tendo em vista a necessidade de um aperfeiçoamento na legislação pátria no intuito de instituir normas mais específicas sobre crimes virtuais.

4.2 Procedimentos de Investigação

Quando um computador é conectado à internet um número é gerado para identificação do aparelho, esse código numérico é denominado Internet Protocol ou apenas IP, que pode ser interno ou externo. O interno é exatamente o endereço IP do dispositivo que é gerado ao contato do aparelho com uma rede interna. Já o externo, é o código gerado para realizar a navegação na rede mundial, em sites, redes sociais e outras páginas da web, sendo modificado a cada acesso a internet. Atualmente, o protocolo IPv4 foi substituído para o IPv6, pois, diante do aumento de dispositivos conectados à internet foi preciso aumentar a capacidade.

O endereço de IP tem várias funções, mas a que trataremos nesta pesquisa é sua capacidade de ser uma das formas para identificação de cibercriminosos, pois com o código é possível localizar e detectar a rede, o dispositivo e o endereço dos internautas.

Aliados a Internet Protocol temos os provedores, que são pessoas físicas ou jurídicas que realizam o trabalho de fornecer a acesso à internet ou trabalham por meio dela e que são utilizados nos procedimentos de investigação dos cibercrimes como registros de acessos que “permitem rastrear e identificar onde surgiu determinada conduta ilícita; são fornecidos somente mediante ordem judicial. Os registros de serviço podem apontar a divulgação ou compartilhamento de conteúdo criminoso”. (SHIMABUKURO, 2017, p. 22)

Entretanto, o grande primeiro desafio encontrado nos procedimentos de investigação dos cibercrimes são as ferramentas que permitem aos internautas esconder ou alterar o número de IP, conhecidas como *proxy*.

Shimabukuro (2017, p. 26) explica que “a criptografia de ponta a ponta permite que somente os próprios usuários (remetente e destinatário) possam decodificar a informação compartilhada”. Portanto, seus provedores ficam impedidos de dar informações, até mesmo para os casos de investigação policial, dificultando a persecução criminal.

Mas não há só dificuldades, a Polícia Federal usa um método bastante eficaz no rastreio de algumas informações ilícitas na rede mundial de computadores, conforme esclarece:

> Para auxiliar nesta busca, é possível criar uma identificação única para cada tipo de arquivo que é disponibilizado na rede, o *hash*. Trata-se basicamente de uma sequência única de letras e números que, gerados por algoritmos matemáticos, servem para verificar a integridade de um arquivo, armazenar senhas e, neste caso, buscar um determinado arquivo em uma grande base de dados. (SHIMABUKURO, 2017, p. 27)

Outra ferramenta é o Localizados de Evidências Digitais (LED) que apesar de ser muitos utilizado em crimes referentes a pornografia infantil, pode ser usado em outros tipos de delitos. Conforme esclarece Carneiro (2017, p. 40)

> Ainda que possa ser configurado para utilização em outros tipos de crime, a título de exemplo, para os locais de busca referentes à pornografia infantil, o LED executa:
> 4.2.1 Busca por arquivos conhecidos de uma base de dados da perícia, baseando-se no cálculo de uma função de *hash* dos arquivos.
> 4.2.2 Busca por palavras tipicamente encontradas em nomes de arquivos, relacionadas ao tipo de crime ou ao caso.
> 4.2.3 Busca por palavras em arquivos de textos e de configuração dos programas mais utilizados para compartilhamento de arquivos na Internet.
> 4.2.4 Processamento de vídeos para geração de imagens contendo alguns quadros do vídeo, para rápida visualização.
> 4.2.5 Processamento dos arquivos de registro do sistema operacional Microsoft Windows, para obtenção de informações que podem ser úteis à avaliação do material no local de busca.

Os crimes virtuais apresentam suas provas e evidências em quaisquer dispositivos eletrônicos, provedores de Internet e registros de rede, arquivos digitais, dados, históricos e imagens gravados na nuvem, entre outros. Contudo, por serem baseadas em algoritmos e códigos, esses vestígios podem ser rapidamente danificados e/ou alterados, sendo necessário proceder com eficiência para preservar as provas e garantir o andamento da investigação e identificação do criminoso.

Para toda e qualquer investigação a perícia é essencial e, nos crimes de

informática, da mesma forma como nos crimes comuns, seu exame e laudo auxiliarão no esclarecimento e convencimento do juiz.

Carneiro (2017, p. 38) explica detalhadamente que o roteiro da averiguação de cibercrimes após a identificação do IP e rastreio do endereço do local de onde ocorreu o acesso, executa-se a busca e apreensão para “coleta de vestígios digitais, além de quaisquer outros vestígios que possam esclarecer os fatos”.

Em suma, os procedimentos realizados na busca e apreensão são:

> a) Após convocação de testemunhas, ciência do morador ou responsável e entrada no imóvel, a equipe foca na busca por equipamentos que possam conter vestígios digitais. Esses itens são, não exaustivamente, computadores, *notebooks, smartphones, tablets*, dispositivos de armazenamento, tais como discos rígidos, discos de estado sólido ou *solid state drives* (SSDs), cartões de memória (normalmente utilizados em celulares e máquinas fotográficas digitais), memórias *flash* conhecidas como *pen drive* e mídias ópticas graváveis (CD-R, DVD-R, etc.). Desprezam-se assim mídias ópticas impressas, que normalmente contêm produtos comerciais.
> b) Faz-se avaliação do conteúdo do material encontrado *in loco,* somente quando houver condições técnicas e táticas, com a utilização do *software* Localizador de Evidências Digitais (LED), desenvolvido pelo PCF Wladimir Leite, no Núcleo de Criminalística (Nucrim) do Setor Técnico Científico (Setec) da Superintendência de Polícia Federal em São Paulo. Essa avaliação será explanada na seção 3.1.
> c) Faz-se a arrecadação ou apreensão do material que não foi excluído pela avaliação de conteúdo, com descrição detalhada dos materiais. Efetua-se uma explanação do procedimento executado para avaliação do conteúdo das mídias digitais, seja no auto circunstanciado da busca, seja em documento apartado. Em alguns crimes, como dispõe o art. 241-B da Lei n.º 8.069/90, que trata da posse de material contendo cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, esse documento formaliza os procedimentos realizados na busca que trouxeram convicção à equipe e às testemunhas para a prisão em flagrante, se identificado o proprietário daquele material. (CARNEIRO, 2017, p. 38-39)

Insta salientar que, o pessoal responsável pela busca e apreensão deveria ser instruído com o máximo de informações possíveis sobre o indiciado, para que ocorresse uma diligência com maior eficiência. Entretanto, na prática não é assim que acontece, eles só conhecem os dados constantes do mandado.

Após a busca, com o material coletado, são encaminhados para perícia que faz cópias para preservação dos vestígios antes de processar o conteúdo das mídias.

Para processamento das evidências, segundo Carneiro (2017, p. 45) usa-se o software denominado “IPED (Indexador e Processador de Evidências Digitais), que utiliza outros programas de código aberto, processando os principais sistemas de arquivos encontrados nos computadores. O Microsoft NTFS é o mais comum nos dias de hoje”.

Apesar de o IPED ser o programa padrão para processamento de evidências digitais, nada impede que seja complementada a perícia com outras ferramentas específicas. Sobre o IPED é importante destacar suas funcionalidades:

> a) **Cálculo de *hash* e consulta a bases de *hashes***: calcula os principais tipos de *hash* utilizados, tais como MD5, SHA-1, SHA256, e-Donkey, etc.; pode utilizar bases de *hashes* para alertar a presença de arquivos conhecidos ou ignorar arquivos comuns de sistema.
> b) **Categorização e indexação**: categorização dos arquivos baseada principalmente nos formatos comumente utilizados, bem como indexação dos textos extraídos de dezenas de tipos de arquivos.
> c) **Galeria de imagens e vídeos:** disponibilização de miniaturas das imagens e seleção de quadros dos vídeos para agilizar a visualização e análise.
> d) **Arquivos apagados e *data carving*:** recuperação de arquivos apagados do sistema, que pode ainda conter referências das remoções, assim como extração de arquivos em espaços não alocados no disco, arquivos de sistema como *pagefile*, entre outros de *cache* (armazenagem temporária), para diversos tipos de arquivos.
> e) **Detecção de imagens explícitas:** implementada pelo PCF Wladimir, em seu programa LED, é também utilizada no IPED para categorização de imagens possivelmente contendo pornografia, para auxílio dos exames de pornografia infantil.
> f) **Visualização integrada:** é possível visualizar dezenas de tipos de arquivos integradamente ao programa, para agilidade e independência do sistema. Também se pode visualizar o conteúdo hexadecimal, útil para análise de alguns tipos de arquivos, bem como texto puro extraído do arquivo, se presente.
> g) **Marcação de itens e geração de relatórios:** permite a marcação dos itens, a criação de categorias, a geração de relatórios com a exportação dos arquivos e a inclusão do próprio IPED para rápida visualização do conteúdo extraído, com busca por palavras-chave e galeria de imagens. (CARNEIRO, 2017, p. 45-46)

Portanto, apesar das dificuldades encontradas no decorrer das averiguações de crimes cibernéticos vemos que nossos procedimentos de investigações tem buscado avançar, só não que ainda estamos em descompasso com as mudanças da tecnologia, pois esta muda constante e rapidamente, além do mais, os criminosos tentam desenvolvem diariamente novas formas de burlas as técnicas e mecanismos de persecução criminal.

4.2 O *Big data*

Como já mencionado anteriormente, com o surgimento da Internet vieram os dados virtuais e, atualmente, a quantidade existente é incalculável tendo em vista as inúmeras tecnologias que são acessadas diariamente a todo tempo. Decorrente dessa conectividade entre as pessoas, sucedeu o aumento no número de cibercrimes e,

conforme o descompasso legislativo ante os avanços tecnológicos, advieram as dificuldades nos procedimentos de investigação desses delitos, surgindo a necessidade de encontrar meios mais eficazes de prevenção e repressão dessas atividades criminosas.

Para melhor compreender o *Big data* Gartner (2020, p. 1) esclarece como sendo “ativos de informações de alto volume, alta velocidade e/ou alta variedade que exigem formas inovadoras e econômicas de processamento de informações que permitem uma visão aprimorada, tomada de decisões e automação de processos”.

Saisse (2017, p. 1) aponta quatro tipos de análises em Big data, quais sejam: prescritiva, diagnóstica, descritiva e preditiva. A primeira faz o “estudo dos casos e fatos tecendo as possíveis consequências sobre as ações tomadas”. O segundo tipo, como o próprio nome remete, faz um apanhado do histórico dos acontecimentos que propiciaram a “tomada de decisão baseada em fatos”. Na descritiva, “é a análise de dados em tempo real”. E, por fim, a preditiva, é o estudo de dados para tecer possibilidades futuras.

No Brasil atualmente teremos a lei 13.709/2018 que entrará em vigor no dia 29 de dezembro de 2020 que disciplina indiretamente sobre o uso do *Big data*.

O *Big data* é um repositório que armazena informações e dados de redes que pode ser usado para prevenir e antecipar possíveis ameaças e ataques, seu funcionamento acontece através de padrões obtidos pela coleta de dados de todas as ocorrências policiais já registradas, juntamente com as características comuns aos criminosos, as formas e o *modos operandi* dos delitos.

A lei geral de proteção de dados aponta que “a partir de tais capacidades de armazenamento, tratamento e análise de dados pessoais coletados a partir de nossos hábitos, torna-se plausível inferir tendências e traços de personalidade, predizer possíveis comportamentos e estabelecer perfis bastante detalhados de todos nós”. (BRASIL, Lei 13.709, 2018)

A compreensão sobre as atividades habituais e corriqueiras da rede permite dissociar aquelas que são consideradas típicas das atípicas e, com isso, possibilitar a mudança de conduta da empresa, instituição ou órgão, para uma reação ativa frente a segurança.

Em outras palavras, o *Big data* seria utilizado para prever e prevenir os crimes cibernéticos, por exemplo, no setor bancário e financeiro, analisando os dados passados de seus usuários e os dados de ataques de força bruta anteriores, os bancos

podem prever futuras falhas nos servidores e tentativas fraudes de cartão, arquivamento de trilhas de auditoria, entre outras.

5 CONSIDERAÇÕES FINAIS

Durante um processo investigatório acerca de crime de natureza cibernética é possível encontrar inúmeros obstáculos para o deslinde da causa, em razão da maleabilidade dos conteúdos presentes na internet e das brechas existentes na rede para o anonimato, bem como, pela falta de legislação própria e específica dos crimes virtuais. Desse modo, a adoção de métodos e técnicas interdisciplinares se revela uma possível solução para as dificuldades enfrentadas pelas autoridades policiais e judiciais.

Os crimes virtuais trazem certa complexidade pois seus agentes podem ser pessoas comuns do dia a dia que ficam desinibidas diante da tela de um computador ou aparelho eletrônico ou são dotadas de conhecimentos técnicos bem específicos, em razão disso, os casos de violação de direitos no ciberespaço devem ser analisados individualmente a partir de uma interação com a realidade, conectando os fatos com os textos legais e atuando em um planejamento interdisciplinar de modo a atingir a resolução dos casos concretos de forma eficaz e célere.

Insta salientar que as polícias e os membros do poder judiciário deveriam ser constantemente capacitados e atualizados sobre as mudanças e avanços cibernéticos, para que sejam dotados de conhecimento técnico adequado para lidar com as investigações dos crimes.

Apesar dos instrumentos de investigação utilizados atualmente nos casos de violação de direitos no ciberespaço serem eficazes na persecução dos elementos probatórios, a tecnologia está em constante mudança e, tais instrumentos têm a necessidade de se modificar também.

Sob essa ótica, para o cenário ideal da política de prevenção ao cibercrime não basta a descoberta da evidência do delito, mais sim, de um novo mecanismo de averiguação capaz de armazenar padrões com perfis de criminosos e seus *modus operandi,* para que assim possa ser possível prever eventuais ataques, antes que aconteçam, identificar os infratores mais facilmente naqueles delitos já praticados e proporcionar mais segurança as vítimas.

Ademais, tendo em vista que o ciberespaço não tem fronteiras, não se limita a

nenhuma das existentes no mundo físico e seus internautas podem estar em qualquer parte do planeta, se faz necessário uma comunicação e cooperação internacional entre os países para prevenir e reprimir os crimes virtuais.

Com a assistência mútua entre os países seria possível facilitar a resolução dos casos de violação de direitos no ciberespaço, prever ataques cibernéticos, compartilhar informações sobre possíveis ameaças e perfis de criminosos, entre tantas outras vantagens que só auxiliariam no aumento da segurança contra crimes virtuais.

Além disso, deve-se evidenciar constantemente por divulgação em meios de comunicação as possíveis situações virtuais que colocam o indivíduo em estado de vulnerabilidade e exposição, como forma de alerta para todos os que utilizam a Internet.

Sob essa ótica, também cabe ressaltar que o ciberespaço se apresenta como um cenário complexo para aplicação do direito, na medida em que o ambiente virtual é algo instável e com diversas situações imprevisíveis, tornando assim um local de difícil regulamentação e controle.

Diante disso, é imperioso que o Estado encontre o equilíbrio e estabeleça limites de atuação a fim de não violar direitos fundamentais já tutelados quando da criação de proteções para essa nova sociedade virtual.

REFERÊNCIAS

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. Jus Navigandi, Teresina, ano 5, p. 51, out. 2001. Disponível em: <https://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em: 10 mai. 2019.

ARAUJO, Fábio Lucena de. Aspectos jurídicos no combate e prevenção ao ransomware. In: BRASIL. Ministério Público Federal da 2ª Câmara de Coordenação e Revisão. Crimes cibernéticos – coletânea de artigos. vol. 3. Brasília: MPF, 2018, p. 92-115.

ASSINCRONICIDADE. In.: PRIBERAM, Dicionário Priberam de Língua Portuguesa. Priberam Informática S.A. 2020. Disponível em: <https://dicionario.priberam.org/assincronicidade>. Acesso em: 20 jun. 2020.

ASSÍNCRONO. In.: PRIBERAM, Dicionário Priberam de Língua Portuguesa. Priberam Informática S.A. 2020. Disponível em: <https://dicionario.priberam.org/assincrono>. Acesso em: 20 jun. 2020.

ASSUNÇÃO, Marcos Flávio Araújo. Segredos do hacker ético. 3ª edição. Florianópolis: Visual, 2008.

BORGES, Daniela Cristina; SARTORI, Liane Pioner; BARROS, Maurício Sebastião de. A Deep Web e a relação com a criminalidade na internet. Direito&TI. 2015. Disponível em: < http://direitoeti.com.br/artigos/a-deep-web-e-a-relacao-com-a-criminalidade-na-internet/#_edn2>. Acesso em: 24 ago. 2020.

BRASIL. Decreto nº 8.771 de 11 de maio de 2016. Brasília, 2016. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm#:~:text=Regulamenta%20a%20Lei%20n%C2%BA%2012.965,transpar%C3%AAncia%20na%20requisi%C3%A7%C3%A3o%20de%20dados>. Acesso em: 19 jul. 2020.

BRASIL. Lei 12.735 de 30 de novembro de 2012. Altera o Código Penal. Brasília, 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm#:~:text=Altera%20o%20Decreto%2DLei%20n%C2%BA,que%20sejam%20praticadas%20contra%20sistemas>. Acesso em: 19 jul. 2020.

BRASIL. Lei 12.737 de 30 de novembro de 2012. Lei dos Crimes Cibernéticos. Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 19 jul. 2020.

BRASIL. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 19 jul. 2020.

BRASIL. Marco Civil da Internet. lei nº 12.936, de 23 de abril de 2014. Vade mecum. São Paulo: Saraiva, 2016.

BUDAPESTE, Convenção sobre Cibercrime. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em: 27 ago. 2020.

CARNEIRO, Márcio Rodrigo de Freitas. Perícia de informática nos crimes cibernéticos. In: BRASIL. Tribunal Regional Federal da 3ª Região. Investigação e prova nos crimes cibernéticos. São Paulo: EMAG, 2017, p. 17-53.

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC). Pesquisa sobre o uso das tecnologias de Informação e Comunicação nos domicílios brasileiros – TIC Domicílios. 2018. Disponível em: <https://www.cetic.br/media/docs/publicacoes/2/12225320191028-tic_dom_2018_livro_eletronico.pdf>. Acesso em: 30 mar. 2020.

CERT.br. Cartilha de Segurança para a Internet. Versão 4.0. Comitê Gestor da Internet no Brasil. São Paulo. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf/>. Acesso em: 24 jul. 2020.

CERT.br. Estatísticas de Incidentes Reportados ao CERT.br - Janeiro a Dezembro de 2019. Disponível em: <https://www.cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.html>. Acesso em: 20 mai. 2020.

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

FERREIRA, Ivette Senise. A criminalidade informática in Direito & Internet: Aspectos jurídicos relevantes, Bauru, SP: Edipro, 2000, p. 236-237

FLORÊNCIO FILHO, Marco Aurélio Pinto. Crimes informáticos: uma abordagem à luz dos objetos da criminologia. In: SÁ, Alvino Augusto de & SHECAIRA, Sérgio Salomão. Criminologia e os problemas da atualidade. São Paulo: Atlas, 2008. p. 244

GARTNER. Glossário de tecnologia da informação. In: Big Data. 2020. Disponível em: < https://www.gartner.com/en/information-technology/glossary/big-data>. Acesso em: 30 ago. 2020.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000

INELLAS, Gabriel Cesar Zaccaria. Crimes na internet. São Paulo: Editora Juarez de Oliveira, 2004.

GOGONI, Ronaldo, Deep Web e Dark Web: qual a diferença?. Tecnoblog. Mar. 2019. Disponível em: < https://tecnoblog.net/282436/deep-web-e-dark-web-qual-a-diferenca/>. Acesso em 30 de outubro de 2020.

KLEINA, Nilton. A história da Deep Web, o submundo da internet. TecMundo. Jul. 2018. Disponível em: <https://www.tecmundo.com.br/internet/131843-historia-deep-web-submundo-da-internet-video.htm>. Acesso em: 31 mar. 2020.

KUNRATH, Josefa Cristina Tomaz Martins. A expansão da criminalidade no cyberespaço. Feira de Santana. Universidade Estadual de Feira de Santana, 2017. 167p. Disponível em: < http://www.uefs.br/modules/documentos/get_file.php?curent_file=3330&curent_dir=1772>. Acesso em: 05 de mai. 2020.

LEMOS, André. Cibercultura: tecnologia e vida social na cultura contemporânea. 4.ed. Porto Alegre: Sulina, 2008

LEVY, Pierre. Cibercultura. São Paulo: Editora 34, 1999.

LIMA, Geilson Carlos Silva de. Crimes informáticos: Análise dos processos de criminalização. 2018. UFRN. Biblioteca Setorial do CCSA.

LIMA, Simão Prado. Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. Âmbito Jurídico. Set. 2014. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-penal/crimes-virtuais-uma-analise-da-eficacia-da-legislacao-brasileira-e-o-desafio-do-direito-penal-na-atualidade/>. Acesso em: 30 mar. 2020.

LINS, Luis Fernando; VILELLA, Felipe; AZEVEDO, Vitor de. DEEP WEB. Trabalhos sobre a Deep Web. URFJ. 2018. Disponível em: <https://www.gta.ufrj.br/ensino/eel878/redes1-2018-1/trabalhos-vf/deepweb/index.html>. Acesso em: 30 mar. 2020.

LUCENA, Mariana Barrêto Nóbrega de. O desvio social na rede mundial de computadores. Aspectos sociológicos e psicológicos dos indivíduos pertencentes às subculturas criminais da internet. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 17, n. 3128, 24 jan. 2012. Disponível em: < https://jus.com.br/artigos/20921/o-desvio-social-na-rede-mundial-de-computadores>. Acesso em: 17 jun.2020.

MACEDO, Herivelto Raimundo L. Surgimento e evolução da internet no Brasil. Eletronet. Jun. 2017. Disponível em: <https://eletronet.com/surgimento-e-evolucao-da-internet-no-brasil/>. Acesso em: 30 mar. 2020.

MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladirson Ronny da Silva. Crimes Virtuais: Uma análise sobre a adequação da legislação penal brasileira. Revista científica da FASETE. 2018. Disponível em: <https://www.fasete.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf>. Acesso em: 21

abr. 2019.

MONTEIRO NETO, João Araújo. Aspectos constitucionais e legais do crime eletrônico. Fortaleza: Universidade de Fortaleza, 2008. 191p. Dissertação (mestrado).

MONTEIRO, Silvana Drumond; FIDÊNCIO, M. V. As dobras semióticas do ciberespaço: da web visível à invisível. TransInformação, Campinas-SP, v. 1, n. 25, p. 35-46, jan./abr.2013. Disponível em: <https://www.puc-campinas.edu.br/periodicocientifico>. Acesso em: 28 fev. 2020.

NOGUEIRA, Sandro D'Amato. Crimes de Informática. São Paulo: BH Editora, 2008. p.61.

OLIVEIRA, Bruna Machado de; MATTOS, Karoline Reis; SIQUEIRA, Marcela Scheuer; OLIVEIRA, Nathalia; WERLE, Vera Maria. Crimes Virtuais e a Legislação Brasileira. Revista Repensando Direito. Santo Ângelo. 2017. Disponível em: <https://core.ac.uk/download/pdf/229767447.pdf>. Acesso em: 21 abr. 2019.

OLIVEIRA, Priscila Chagas; NUNES, João Fernando Igansi. Cultura Digital e as Tecnologias da Memória no Ciberespaço. Alcar2015. Disponível em: <file:///C:/Users/Alanna%20Kassia/Downloads/GTMIDDIG_OLIVEIRA-%20Priscila_%20NUNES-%20Joao.pdf>. Acesso em 16 jun. 2020.

PAESANI, Liliana Minardi. O papel do direito contra o crime cibernético. Âmbito Jurídico, 2010. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-79/o-papel-do-direito-contra-o-crime-cibernetico/>. Acesso em: 28 ago. 2020.

PAIXÃO, Luís Antonio da; CAETANO, Marliza Núbia; ALVARENGA, Fabiana Cristina da Silveira. Crimes Cibernéticos: Evolução do direito penal eletrônico frente às novas demandas da vida atual. Revista Jurídica da Libertas Faculdades Integradas. 2015. Numero 1. Ano 5. Disponível em: <http://www.libertas.edu.br/revistajuridica/mostrar revista.php?idsum=81227>. Acesso em: 23 ago. 2020.

PINHEIRO, Patrícia Peck. Direito digital. 4ª ed. São Paulo: Saraiva, 2010. PSafe. Pesquisa sobre Roubo de Identidade. 2019. Disponível em:<https://cdn.blog.psafe.com/blog/wp-content/uploads/2019/05/Pesquisa-PSafe-sobre-Roubo-de-Identidade.pdf>. Acesso em: 22 mai. 2020.

PSafe. Pesquisa sobre Scammers. 2020. Disponível em:<https://cdn.blog.psafe.com/blog/wp-content/uploads/2020/02/Pesquisa-sobre- scammers.pdf>. Acesso em: 22 mai. 2020.

PSafe. Relatório da Segurança Digital. 2019. Disponível em: <https://www.psafe.com/dfndr-lab/relatorio-da-seguranca-digital-2018/>. Acesso em:

22 mai. 2020.

ROSSINI, Augusto Eduardo de Souza. Informática, Telemática e Direito Penal. São Paulo: Memória Jurídica, 2004.

SAISSE, Renan. Big Data contra o crime: efeito Minority Report. Direito&TI, 2017. Disponível em: < http://direitoeti.com.br/artigos/big-data-contra-o-crime-efeito-minority-report/#_edn1>. Acesso em: 30 ago. 2020.

SANTO, Kleber Assunção do Espírito. Crimes Cibernéticos. Universidade Tuiuti do Paraná. Curitiba. 2015. Disponível em: <https://tcconline.utp.br/media/tcc/2015/09/CRIMESCIBERNETICOS.pdf>. Acesso em: 21 abr. 2019.

SHIMABUKURO, Adriana. Cibercrime: quando a tecnologia é aliada da lei. In: BRASIL. Tribunal Regional Federal da 3ª Região. Investigação e prova nos crimes cibernéticos. São Paulo: EMAG, 2017, p. 33-31.

SILVA, Adelina Maria Pereira da. Mundos Reais, Mundos Virtuais. Os jovens nas salas de chat. Universidade Aberta. 2005. Disponível em: <http://bocc.ufp.pt/pag/silva-adelina-mundos-reais-mundos-virtuais.pdf>. Acesso em: 19 jun. 2020.

SILVA, Fernanda Viero da; FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. Deep Web e Dark Web: implicações sociais e repercussões jurídicas. Revista eletrônica Direito e Sociedade – REDES. Canoas, v.8, n. 2, 2020. Disponível em: < https://revistas.unilasalle.edu.br/index.php/redes/article/view/6756>. Acesso em: 19 abr. 2020.

SPAGNOL, Débora C. Implicações Criminais no Espaço Virtual. Empório do Direito. 2015. Artigo disponível em: <http://emporiododireito.com.br/implicacoes-criminaisno-espaco-virtual-por-deboracspagnol/>. Acesso em: 25 jun. 2019.

SUBCULTURA. In.: DICIO, Dicionário Online de Português. Porto: 7Graus, 2020. Disponível em: <https://www.dicio.com.br/subcultura/>. Acesso em: 17 jun. 2020.

SULER, John. Cyberspace as Psychological Space. 1999. Disponível em:<http://www-usr.rider.edu/~suler/psycyber/psychspace.html>. Acesso em: 19 jun. 2020.

SULER, John. The online desinhibition effect. Mary Ann Liebert, Inc.Vol. 7, No 3, 2004.

TASHINO, William Hideki. Direito ao anonimato na Internet. Universidade de Brasília. 2015. Disponível em: <https://bdm.unb.br/bitstream/10483/11158/1/2015_WilliamHidekiTashiro.pdf>. Acesso em: 01 jul. 2020.

VIANNA, Túlio Lima. Hackers: um estudo criminológico da subcultura cyberpunk. Academia. 2003. Disponível em <https://www.academia.edu/1911168/Hackers _um_estu-do_criminológico_da_subcultura_cyberpunk>. Acesso em: 10 abr. 2020.

WE ARE SOCIAL; HOOTSUITE. Digital in 2019. Disponível em: <https://wearesocial. com/global-digital-report-2019 >. Acesso em: 30 mar. 2020.

WENDT, E.; JORGE, H. V. N. Crimes Cibernéticos. São Paulo: BRASPORT, 2012.