UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS JURÍDICAS - CCJ
CURSO DE BACHARELADO EM DIREITO

EDSON GONÇALVES MARQUES DA SILVA

AS MULTIFACES DOS CRIMES CIBERNÉTICOS: DISPOSITIVOS TECNOLÓGICOS E CRIMINALIDADE

CAMPINA GRANDE – PB
2020

EDSON GONÇALVES MARQUES DA SILVA

AS MULTIFACES DOS CRIMES CIBERNÉTICOS: DISPOSITIVOS TECNOLÓGICOS E CRIMINALIDADE

Trabalho de Conclusão de Curso (Artigo) apresentado a Coordenação do Curso de Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de concentração: Ciências Criminais e Novas Tecnologias

Orientadora: Profª Drª Aureci Gonzaga Farias

CAMPINA GRANDE – PB
2020

S586m Silva, Edson Goncalves Marques da.
As multifaces dos crimes cibernéticos [manuscrito] : dispositivos tecnológicos e criminalidade / Edson Goncalves Marques da Silva. - 2020.
26 p.
Digitado.
Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2020.
"Orientação : Prof. Dr. Aureci Gonzaga Farias , Coordenação do Curso de Direito - CCJ."
1. Legislação Penal. 2. Crimes cibernéticos. 3. Crimes virtuais. I. Título
21. ed. CDD 345

Elaborada por Candice L. Brasileiro - CRB - 15/815 BSCCJ/UEPB

EDSON GONÇALVES MARQUES DA SILVA

AS MULTIFACES DOS CRIMES CIBERNÉTICOS: DISPOSITIVOS TECNOLÓGICOS E CRIMINALIDADE

Trabalho de Conclusão de Curso apresentado a Coordenação do Curso de Direito da Universidade Estadual da Paraíba, em cumprimento às exigências para obtenção do Título de Bacharel em Direito.

Aprovada em: 19/10/2020

BANCA EXAMINADORA

Profª Drª Aureci Gonzaga Farias
(Orientadora)
Universidade Estadual da Paraíba (UEPB)

Prof. Dr. Marcelo D'Angelo Lara
Universidade Estadual da Paraíba (UEPB)

Prof. Me. Renan Farias Pereira
Universidade Estadual da Paraíba (UEPB)

Dedico esta conquista primeiramente a Deus, que permitiu à minha família receber a multiplicação de seus dias sobre a Terra. Nos momentos mais dramáticos de nossa existência, nos mostrou os caminhos iluminados que precisávamos seguir e tem sido assim, pois até aqui Ele tem nos sustentado. Dedico também aos meus pais, Manassés e Inês, meus padrinhos Raimundo e Josefa, meus primos Sandra, Márcio e Thiago, pelo incentivo à leitura, à minha esposa Sayonara e filhas Adríny e Letícya; além de meus irmãos Rafael e Halley (*in memorian)*, pela estima e apoio.

Eis que estarei contigo e te guardarei por onde quer que fores, e te farei tornar a esta terra, pois não te deixarei até que haja cumprido tudo aquilo que tenho te falado.

A Bíblia (Gênesis 28:15)

SUMÁRIO

AS MULTIFACES DOS CRIMES CIBERNÉTICOS: DISPOSITIVOS TECNOLÓGICOS E CRIMINALIDADE

LAS MULTIFACES DE LOS DELITOS CIBERNÉTICPS: DISPOSITIVOS TECNOLÓGICOS Y EL CRIMEN

Edson Gonçalves Marques da Silva[1]

RESUMO

O presente Trabalho de Conclusão de Curso tem como objetivo central analisar os crimes digitais e as consequências jurídicas pertinentes, avaliando e demonstrando os impactos destes na vida das pessoas, dando ênfase aos avanços e entraves presentes na legislação penal brasileira. Utilizou-se a pesquisa exploratória, especificamente, a de ordem bibliográfica. Entendemos que há duas correntes acerca da temática dentro do Direito que divergem, são elas a que defende que a Internet é apenas mais uma mídia de expressão, logo os delitos nela cometidos devem estar alicerçados no mesmo grupo dos que ocorrem fora da rede, sendo assim não se faz necessário o uso de novas legislações; e a outra corrente defende que a própria Internet se caracteriza como prova da revolução digital e que o substancial número de casos reforça a necessidade de legislação específica. Consideramos que, uma maior atenção ao surgimento da criminalidade virtual e da regulamentação existente para estas condutas ilícitas e o estabelecimento de direitos e deveres cibernéticos, ainda que tardio, é de extrema importância para o combate dos crimes virtuais.

Palavras-chaves: Legislação Penal. Crimes Cibernéticos. Crimes virtuais.

RESUMEN

La investigación de conclusión del Curso tiene como objetivo central de analizar los delitos digitales y las consecuencias legales pertinentes, evaluar y demonstrar sus impactos en la vida de las personas, enfatizando los avances y obstáculos presentes en la legislación penal brasileña. Se utilizó la investigación exploratoria; en cuanto a los medios es bibliográfica. Entendemos que hay dos corrientes sobre el tema dentro de la ley que divergen, son las que defiende que Internet es solo un medio de expresión más, por lo que los crímenes cometidos en ella deben basarse en los mismo grupo de los que ocurren fuera de la red; y la otra corriente sostiene que la propia Internet se caracteriza como prueba de la revolución digital y que los numerosos casos refuerzan la necesidad de una legislación específica. Creemos que una mayor atención al surgimiento de los crímenes cibernéticos y la regulación existente para estas conductas ilegales y el establecimiento de derechos y deberes cibernéticos, aunque sea tarde, es muy importante para la lucha contra los crímenes cibernéticos.

Palabras-clave: Legislación Penal. Crímenes cibernéticos. Crímenes virtuales.

[1] Graduando em Direito pela Universidade Estadual da Paraíba – UEPB. edsonmarques9592@gmail.com

1 INTRODUÇÃO

Se o acesso à Internet em um mundo cada vez mais conectado é essencial ao exercício da cidadania, importante se faz executar medidas pedagógicas e sanções que possam ser incorporadas no intuito de combater possíveis violações de direitos. Hodiernamente, enfrentamos um aumento da disseminação do preconceito, do ódio e da discriminação nas redes sociais, assim, o presente Trabalho de Conclusão de Curso - intitulado "As Multifaces dos Crimes Cibernéticos: Dispositivos Tecnológicos e Criminalidade" - tem como objetivo geral analisar os crimes digitais e as consequências jurídicas pertinentes, avaliando e demonstrando os impactos destes na vida das pessoas, dando ênfase aos avanços e entraves presentes na legislação penal brasileira.

O acesso à tecnologia, em especial, o direcionado para a comunicação, torna-se cada dia mais presente e essencial no cotidiano das pessoas, considerando que, possibilita conexões mais fáceis, práticas e, em geral, acessíveis entre aqueles que a utilizam bem como interações que não se restringem às fronteiras físicas; além de serem importantes ferramentas para o trabalho, para a comunicação e para outras resolutividades de atividades simples e pertinentes à rotina humana. Sendo assim, destacamos que o acesso às numerosas possibilidades, ofertadas pelas tecnologias comunicacionais, se materializa pelo uso de suportes e/ou meios tecnológicos tais como os *smartphones*, computadores, *notebooks*, *tablets*, dentre outros, que são de fácil acesso à maioria da população, amparados pelo acesso à Internet.

Assim como no mundo real, o mundo virtual reproduz a prática de crimes tradicionais e permite a execução de novas condutas lesivas. Nos diversos países do mundo, inclusive no Brasil, multiplicam-se casos envolvendo crimes cometidos através da Internet.

As tecnologias oriundas e difundidas pela Internet têm um desenvolvimento extremamente veloz, surgindo novas relações que precisam de amparo jurídico, de forma igualmente dinâmica, sendo assim ainda que alguns tipos de crimes cibernéticos careçam de tipificação adequada, é imperioso saber como o Brasil lida com tais condutas e as alternativas atuais para a aplicação do Direito.

Para alcançar o objetivo proposto, quanto ao aspecto metodológico foram adotados o método exploratório, através de pesquisa bibliográfica. O motivo da escolha acerca da temática de pesquisa, por sua vez, ocorreu durante o período do curso ao atentar para o aumento da disseminação do preconceito, do ódio, da polarização política, da discriminação, da intolerância religiosa, do racismo, da xenofobia e das noticias falsas além dos golpes permeados pelos meios digitais e relacionados às redes sociais em contraste com a legislação ainda insuficiente para combater essas práticas.

Questiona-se então: Afinal, como oferecer segurança cibernética aos usuários - considerando quais decisões necessárias para proteção das informações e dados, já que até mesmo os *sites* oficiais dos governos, no mundo inteiro, parecem estar vulneráveis aos ataques de cibercriminosos – perante sua legislação que não atende às demandas da sociedade e seus problemas contemporâneos?

2 INTERNET E DIREITO DIGITAL NO MUNDO

A Internet surgiu em 1969, fruto de um projeto científico militar americano conhecido como a Agência de Pesquisa Avançada e Rede (ARPANET), a fim de que eles pudessem trocar informações, consideradas de extrema importância em casos de guerra. No

entanto, ficou conhecida como a Internet que conhecemos hoje bem mais tarde. Tornou-se pública a partir de 1990 com a desativação da ARPANET e a entrada no mercado do primeiro provedor comercial com acesso discado. No Brasil ela chegou, tão somente, em 1988 por meio da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e do Laboratório Nacional de Computação Cientifica (LNCC) localizado no Rio de Janeiro, entretanto foi só em 1991 que seu uso se estendeu ao público (TEIXEIRA, 2007, p.8-9).

Pouco antes, ainda em 1989, surgiu a *World Wide Web* (WWW) significando "grande teia mundial" que em uma definição simples para o português é "a principal responsável pela popularização da Internet, conciliada ao desenvolvimento dos navegadores". Segundo Correa (2020, p. 11), a WWW "ofereceu aos usuários aquilo que mais apreciavam: a utilização da imagem, som e movimento, em vez da melancolia do texto puro". Hodiernamente, a Internet é vista como meio de comunicação que interage dezenas de milhões de equipamentos eletrônicos, não só computadores. Quase todo o mundo pode ser conectado possibilitando acesso a uma grande quantidade de informações.

Obviamente, a Internet não tem um proprietário, mas sim um controle por parte de organizações mundiais, que acompanham o processo de evolução das novas tecnologias, promovendo o desenvolvimento e centralizando operações. Dentre elas, podemos citar a *Internet Architeture Board* (IAB), coordenando a pesquisa e desenvolvimento de seu funcionamento; a *Internet Engineering Task Force* (IETF) responsável por desenvolver padrões para funcionamento da Internet; a *Internet Network Informativo Center* (*INTER NIC*), que coordena a distribuição de endereços e registros de domínios mundialmente; o Comitê Gestor Internet (CGI) coordenador da implantação do acesso à Internet no Brasil; a Rede Nacional de Pesquisas (RNP) administradora do *BackBone* Internet no Brasil e a FAPESP em que se registram os domínios e endereços no Brasil.

Na concepção de Sydow (2009, p. 246) o novo bem jurídico oriundo da informática é a segurança telemática, e isso se dá pelo fato de que a tecnologia formada por *bits* se mostra melhor num ambiente em que as informações sejam armazenadas e processadas com extrema rapidez e transmitidas a qualquer parte do mundo nas mesmas velocidades que o som ou a luz se propagam, do que se mostraria num objeto individualizável. Portanto, assim como outro meio ambiente, exigem-se concepções novas de bem jurídico material, que apontam para valores como: a confidencialidade dos dados produzidos e armazenados pela informática, a integridade de dados e a disponibilidade de acesso como também a leitura e uso de tais dados.

A delinquência informática na rede mundial de computadores faz com que os esforços para proteger os cidadãos que convivem no meio virtual obtenham baixa proficuidade. Os recursos públicos são limitados, pouco sofisticados frente aos recursos dos agentes infratores e, além disso, a legislação é comumente atrasada bem como a política de enfrentamento. Sydow (2009, p. 247-248) ainda atribui à baixa comunicação acerca dos delitos, ao atraso no combate a essas novas formas de criminalidade, uma vez que, vários fatores contribuem para essa perspectiva como: não percepção dos crimes, medo de vitimização policial (secundária) ou mesmo embaraço de ter sofrido ataques criminosos pela Internet.

Há também, por parte do Estado, uma ampla debilidade no combate à nova tendência na criminalidade e seu reconhecimento leva à busca por alternativas de manutenção da delinquência num panorama que a autora intitula enquanto normal. Dessa maneira, a criminologia tem o intuito de entender como ocorrem os delitos de ordem informática, com o objetivo de criar propostas de política criminal com maior aplicabilidade e eficiência, tendo em vista que a perspectiva repressiva está em um nível inferior às expectativas. Por outro lado, é importante focar em esforços preventivos que se estabelecem na relação criminal. A autora complementa seu argumento defendendo que

“Para que a prevenção se mostre eficiente, é imprescindível que os axiomas de prevenção do mundo material sejam discutidos com vista às novas particularidades do meio”.

Na rede mundial de computadores mostra-se um cenário em que os usuários - potenciais vítimas - são, em diversos casos, os responsáveis por aquilo que a eles próprios acontece. Atenta para a necessidade de compreensão, por parte dos usuários, do meio em que navegam, com vista a se prevenir de possíveis riscos provenientes dos crimes virtuais. Para tanto, é necessário o conhecimento e entendimento sobre os perfis mais procurados pelos delinquentes bem como as fragilidades que eles exploram. Há, dessa forma, a necessidade de investimento em condutas pedagógicas que ajudem o usuário a, justamente, prevenir-se. Existe um perfil desses delinquentes que atuam em rede, são caracterizados como um grupo restrito, em geral, homens com acesso à tecnologia, além de status social e cultural razoável, cujas vítimas são escolhidas pelas fraquezas, cabendo ao autor dos crimes criatividade para escolhê-las.

Os usuários dos serviços disponibilizados pela Internet possuem os *firewalls*, antivírus e outras barreiras que objetivam protegê-los de ameaças cibernéticas. Contudo, para que essas soluções de fato funcionem, o usuário deve ter consciência de como usá-las de forma correta e eficiente. A crença de que essas ferramentas de fato proporcionam toda a proteção necessária, não é suficiente, para tanto ela pontua que “[...] apesar da sensação de segurança proporcionada pela tecnologia cada usuário deve entender-se como um administrador de seus próprios bens jurídicos virtuais” (SIDOW, 2009, p.248). Deve ainda compreender que os delinquentes que se beneficiam da prática de crimes no âmbito virtual, não se assemelham aos usuários comuns, daí a necessidade de atitudes por parte do Estado, que não se restrinjam aos serviços de proteção já disponibilizados pela Internet.

Viana (2001, p.62) sinaliza para seis tipologias de delinquentes que atuam na Internet. Os primeiros são os “*Crackers* de sistemas” aqueles que invadem computadores, que estão conectados a rede; os “*Crackers* de programas” que conseguem quebrar a proteção de *softwares* cedidos com o intuito de disfrutar deles; os “*Phreakers*” que são especialistas em telefonia tanto fixa quanto móvel; os que desenvolvem “vírus, *worms* e *trojans*” para causar danos ao usuário; os “piratas de programas” que os clonam e fraudam direitos autorais e os “distribuidores de Warez”, isto é, *webmasters* que disponibilizam em suas páginas da Internet *softwares*, sem ter a autorização daqueles que detêm os direitos autorais.

Diante das novas problemáticas trazidas da realidade virtual para a área penal, existe a necessidade de refletir valores tradicionais a partir de uma nova ótica, considerando que aspectos como “[...] a pessoalidade da relação criminosa, a teoria da atividade na consideração do local do crime, a limitação física do cometimento do delito, entre outros” (SYDOW, 2009, p. 246) adquirem outras maneiras de percepção, diante desse novo panorama. Desse modo, tais características trazidas pela tecnologia exigem que o Direito Penal deva adequar-se e interpretar seus valores.

A Internet desde o início sempre foi uma possibilidade de risco, considerando que é, em geral, revestida pelo aparente anonimato daqueles que a utilizam e, por sua vez, pelo expressivo número de êxitos daqueles que empreendem pela delinquência na rede, considerando as motivações como: seu conhecimento prévio nas nuances dos mecanismos da Internet, as fragilidades de suas vítimas, a pouca resolução dos casos, a ineficácia do Estado. Por isso, a importância de estabelecer a Internet como verdadeiro ambiente, considerando que frente aos casos não solucionados, se empilham crescentes denúncias de crimes virtuais.

2.1 Crimes virtuais próprios e impróprios e o sujeito ativo

De acordo com Correa (2000, p. 43), crimes digitais são "todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; e para tal prática é indispensável utilizar um meio eletrônico".

Destacamos que, apesar das diferenças entre as doutrinas, em relação à classificação e ao trato dos crimes cibernéticos, adotamos a divisão utilizada por Greco Filho (2001, p.1) que entende que os crimes digitais se dividem em próprios e impróprios, ou seja, os primeiros se caracterizam por condutas praticadas contra um sistema informático, independente das motivações daquele que age de maneira ilícita; já os outros são condutas cuja prática se realiza contra outros bens jurídicos, também graças a um sistema informático. O autor ainda explica que:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticada por meio da Internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crime de resultado conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico; sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conta livre, à lei importa apenas um evento modificador da natureza, como, por exemplo; o homicídio. O crime, no caso, é provocador do resultado morte, qualquer que tenha sido meio ou ação que o causou. (GRECO FILHO, 2000, p.1).

Os sistemas de informática, apesar de serem instrumentos como tantos outros utilizados por aqueles que cometem crimes, propiciam uma facilidade na prática de delitos, dessa forma é responsabilidade do Estado nivelar os modos de criminalidade (inclusive, os ainda não previstos no ordenamento jurídico de nosso país) que surgiram com o advento da Internet e das novas tecnologias de comunicação, uma vez que, seu alcance ainda não foi suficientemente avaliado.

Há, no entanto uma questão a ser tratada, a do sujeito ativo, tendo em vista que, sabemos que a comprovação acerca de autoria de crimes cibernéticos não é fácil, dada a ausência física desse sujeito ativo. Considerando essas dificuldades de identificação, percebe-se a necessidade de traçar perfis que pratiquem esses crimes como os abaixo descritos e os tratados no tópico anterior.

2.2 *Crackers, Hackers* e o sujeito passivo

Oliveira *et al* (2017, p. 123), em seus estudos, define cinco perfis de sujeitos ativos, sendo o primeiro deles o próprio usuário, tendo em vista que, às vezes, agem sem intenção criminal, como por exemplo, divulgando fotos de terceiros sem prévia autorização, criando os pefis "*fakes*" isto é, falsos nas redes sociais, etc.

O segundo perfil tratado pelas autoras é dos *hackers*. Bortot (2017, p. 343) afirma que, muitas vezes, por falta de entendimento ou critérios acaba por atribuir aos *hackers* à responsabilidade de crimes cibernéticos, contudo eles são os que, em geral, modificam *softwares*, atribuindo-lhes novas funcionalidades, detectando falhas, corrigindo-as, etc., utilizando seu conhecimento em consonância com os parâmetros da legalidade. Por outro

lado, os *crackers* – terceiro perfil tratado por Oliveira *et al* (2017, p.343) – são aqueles que de fato invadem os computadores e sistemas. São, portanto os que agem com o objetivo criminoso de violar e descobrir senhas, dados privados bem como invadir e roubar o patrimônio e/ou as informações acerca da vitima.

Os *carders* e os *Wannabes* são o quarto e quinto perfis de criminosos responsáveis, respectivamente, de descobrir senhas de cartões de créditos pela internet e desfrutar delas realizando compras e os que dispõem de pouco conhecimento da internet, mas que não os impede de realizar crimes (OLIVEIRA, *et al.*, 2017, p.123).

Por fim, o sujeito passivo dos delitos de ordem cibernética é aquele que "[...] assim como no crime comum, figura o polo passivo dos crimes cibernéticos aquele a quem recaiu a ação ou omissão, seja ele pessoa física ou jurídica, sendo assim a vítima". (BORTOT, 2017, p. 343).

2.3 Crimes cibernéticos e desinformação através de notícias falsas

O avanço da tecnologia e o crescimento de usuários conectados à Internet bem como o aumento de aplicativos e equipamentos fez multiplicar o acesso e a inclusão digital. Contudo, essas mudanças de comportamento coletivo acarretam o compartilhamento de informações pessoais e da vida íntima dos indivíduos, através do compartilhamento de fotos, vídeos e áudios que ultrapassam o controle da pessoa que publicou a informação, ocasionando consequências de natureza jurídica que envolve esta temática, fazendo-se necessário esclarecer os possíveis questionamentos éticos e sua relevância social e científica assim como elucidar dilemas sobre liberdade de expressão e comunicação bem como ao que vai contra ao âmbito privado dos usuários (SIMÃO FILHO; ZACARIAS, 2018, p. 3).

Segundo Nascimento (2019, p. 6) vários termos são, por vezes, utilizados para descrever os crimes cometidos utilizando computadores, no qual diferem entre si quanto ao seu significado, são eles: crime de computador, crime de Internet, *e-crime*, *cibercrime*, que podem assim ser entendidos: (I) Crime de computador é quando o objeto do delito ou ferramenta para sua comissão é o próprio computador. Exemplos podem ser as falsificações de informática - dados falsos que são apresentados como autênticos - e fraudes relacionadas ao computador. Interferência fraudulenta com a manipulação de dados para causar a perda da propriedade; (II) Crime de Internet refere-se ao uso da Internet como uma característica fundamental e inclui infrações relacionadas com o conteúdo, tais como posse de pornografia infantil, ou em alguns países, a disseminação do ódio e de matérias de conteúdo racistas; (III) *E-crime* é o rótulo geral para delitos usando um dispositivo de armazenamento de dados ou de comunicação eletrônica; **(**IV) *Cibercrime* é qualquer atividade ou prática ilícita na rede.

As *fake news* são exemplos de crimes cometidos pela Internet em que há criação e divulgação de notícias falsas com o intuito sensacionalista e, pautadas em exageros, apelos, distorções, etc.. Apesar de muito citadas e popularizadas atualmente, sua origem não é recente. Podemos afirmar que desde o acidente que vitimou a Princesa Dayana em 1996, a forma com que noticiam os escândalos e boatos juntamente com a perseguição de *paparazzi* aos famosos vem causando cada vez mais problemas e fofocas *online*. (NUNES, 2006, p. 1). Considerando que a interpretação dos fatos sempre pode ser eivada de ideologias e subjetividade jornalística, reportar notícias de forma fidedigna precisa ser o objetivo principal de qualquer veículo de comunicação. Mas, atualmente, não é isso que ocorre: manipulando-se editoriais e repassando informações de procedência duvidosa, fabricam-se informações e cria-se com isso a desinformação com a enganação direta e a

mentira absoluta, espalhando-se de maneira rápida; destruindo reputações de indivíduos e instituições, e isso vem sendo largamente utilizado até pela política partidária mundialmente. Piccolo (2019, p. 1) complementa ao afirmar que conteúdos falsos e desordem informacional, por meio da guerra virtual travada nos veículos comunicacionais - sobretudo pela Internet, principalmente por mensagens de aplicativos de mensagens, como o *WhatsApp* - influenciam comportamentos e com isso, muitas vidas acabam por perecer e memórias são profanadas.

A Tecnologia da Informação e da Comunicação (TIC) já há algum tempo é integrante de nossa vida cotidiana e na Austrália o termo *cibercrime* também é usado para descrever tanto os crimes dirigidos a computadores ou outras TIC's (como invasões de computador e ataques de negação de serviço) quanto os crimes em que computadores ou TIC's são parte integrante de um delito (como fraudes *online*). Os australianos têm o *ThinkUKnow* que é um programa de educação e prevenção *online* que usa uma rede de voluntários treinados para fazer apresentações de segurança *online* para pais, responsáveis e professores sobre como os jovens usam a tecnologia, os desafios que podem enfrentar e como obter ajuda e suporte se algo der errado *online*. As apresentações geralmente duram uma hora e são apoiadas por um site abrangente - thinkuknow.org.au - que fornece informações e recursos adicionais. O *ThinkUKnow* é uma parceria entre Polícia Federal Australiana, *Microsoft*, *Datacom*, *Commonwealth Bank* e é realizada em colaboração com as polícias estaduais e territoriais, além da *Neighbourhood Watch Australia* (AFP, 2020, s/p).

Essas agências lidam com crimes que dependem da utilização de toda sorte das TIC, ou que tenham como alvos equipamentos, dados e serviços. O foco está na capacidade de ligação em rede complexa de TIC, o que cria uma plataforma - anteriormente inimaginável - para cometer e investigar atividades criminosas. Até mesmo as populações que sofrem com a exclusão digital podem sofrer os efeitos de alguns crimes cometidos por tais meios, isso vem ocorrendo com o roubo de senhas e compras *online*. Embora saibamos que as dificuldades de acesso às TIC's estão relacionadas à boa parte da população que sempre encontrou as mesmas barreiras no acesso aos outros bens de consumo. "O mercado não irá incluir na era da informação os extratos pobres e desprovidos de dinheiro". (SILVEIRA, 2003, p. 29).

Neste cenário, possibilidades de condutas criminosas podem se proliferar, e ao longo dos anos, vários países têm tentado adaptar suas leis para combater os crimes cibernéticos, com destaque para os Estados Unidos, primeiro país a legislar sobre o assunto, e a Europa, pela elaboração da convenção sobre o *cibercrime*; conhecida como "Convenção de Budapeste". Enquanto isso, no Brasil, o legislativo carece de insumos no que se refere a esse combate; o que torna o território nacional um verdadeiro oásis para os criminosos. E, além do país não ser signatário da Convenção Europeia, não possui agentes suficientemente capacitados para investigar e periciar os crimes virtuais; o que torna a persecução penal quase impossível. (BORTOT, 2017, p. 339).

Outros grandes desafios são as complexidades contidas na Grande Rede. De acordo com Aguiar (2018, s/p), toda a sua "superfície" conhecida pelo termo *surface web*, é a parte da Internet indexada, que possibilita os canais de busca como *Google*, *Bing* etc. correspondendo a apenas 4% de toda a informação existente na Internet. Por outro lado, a *Deep Web* é a parte composta por *sites* não indexados, o que impossibilita encontrá-los nos canais de busca supracitados. No entanto, outra parte mais profunda da *Deep Web*, na maioria das vezes, utiliza redes criptografadas funcionando com os navegadores *Tor*, o *i2p* e o *FreeNet* ocultando ainda mais os dados dos usuários, embora a imensa maioria das pessoas que acessam a *Deep Web* de fato não se envolva com ilícitos, apenas não desejam ser rastreadas com facilidade. Há ainda a *Dark Web*, que é considerada a zona escura da

Internet, com criptografia mais complexa, dividida em cinco níveis: comum indexada, comum não-indexada, restrita com alteração de *proxy*, restrita com utilização de distribuição de acesso e secreta com alteração de *hardware* (AGUIAR, 2018). Nesse sentido, a *Dark Web* é então, uma pequena parte da *Deep Web* onde se proliferam crimes como negociações com *crackers* e assassinos, pornografia infantil, comercialização de drogas e contrabando, compartilhamento ilegal de informações e outros tantos delitos na maioria das vezes permeados através de pagamentos que utilizam *bitcoins* - as moedas mais comuns e de difícil rastreio, empregadas no meio virtual, dentre outras.

2.4 Liberdade de expressão ou criminalidade digital?

A Internet concomitantemente ao fato de ser, no mundo contemporâneo, a maior fonte e o maior veículo no tráfego de informações é também uma ferramenta perigosa no que consta a divulgação de notícias, informações, ameaças e outras questões falsas, violências, etc., cuja probabilidade de punição no cenário atual é praticamente escassa. Sendo assim, apesar da infinidade de benefícios por ela ofertados, há também que considerar praticamente a mesma proporção, só que inversa, de atos ilícitos que, por sua vez, aumentaram consideravelmente sendo, muitas vezes, usada como veículo para pessoas mal intencionadas e que agem de má fé para a prática de crimes, desse modo busca–se fazer um reconhecimento das normas vigentes para tais crimes. (SANTOS *et al*, 2017, p. 2).

Publicar ofensas em redes sociais não se confunde com o direito à liberdade de expressão. A falsa sensação de anonimato tem levado centenas de internautas a publicarem conteúdos ofensivos de todo tipo para milhares de pessoas, famosas ou não. Sem contar os casos de roubos de senhas, de sequestro de servidores, invasão de páginas e outros *cibercrimes*. Todas as pessoas que são atingidas podem recorrer à Justiça para garantir o seu direito de reparação. Apesar de ser um assunto relativamente novo, a legislação tem avançado com textos específicos para cada propósito.

Como aponta Santos *et al* (2017, p. 4), a falta de denúncias também é um meio de incentivo ao crescimento latente do número de golpes virtuais como também da violência digital como, por exemplo, o *ciberbullying*. Muito é discutido acerca da escassez de um conjunto de normas e sanções jurídicas direcionando penas para os crimes digitais. Contudo, com ou sem a existência de uma legislação específica que aborde essa problemática, quando o computador é usado como um meio que facilita ou proporciona a prática de delitos e violências estes crimes devem por obrigação ser adaptados ao Código Penal brasileiro e os agressores e golpistas punidos.

3 CRIMES DIGITAIS E A LEGISLAÇÃO BRASILEIRA

Toda essa revolução digital influencia e muito na esfera jurídica, entretanto as opiniões se dividem, tendo em vista que existem os defensores de que a toda interação humana na Internet deve-se aplicar os princípios gerais do Direito, com os institutos jurídicos já consolidados. Por outro lado, outra vertente avalia que se deve reinterpretar totalmente o Direito rompendo os paradigmas jurídicos tradicionais, propondo uma regulação específica. Diante disso, os que defendem que devem ser aplicados para a Internet os mesmos princípios penais já aplicados normalmente, negam o que chamamos de revolução e atribuem à Internet o caráter de apenas mais uma mídia de expressão, como é o

caso do pesquisador Greco Filho (2000) que afirma em seu artigo "Algumas observações sobre o Direito Penal e a Internet" que a tentativa de criar aportes jurídicos específicos para casos de crimes virtuais, nada mais é que "bajular os meios eletrônicos", cujo único intuito é uma exibição de vaidade. Nesse sentido, seriam apenas as mesmas interações humanas, tanto dentro quanto fora da Internet, e o que teria sido modificado foram os meios e a noção de tempo de resposta das interações. Ou seja, esse surgimento de tecnologias revolucionárias não necessariamente ensejaria uma regulação jurídica específica, já que perfeitamente poderiam ser aplicados os princípios gerais do Direito. A jurisprudência brasileira principalmente no Supremo Tribunal Federal (STF) segue essa linha. Essa mesma corrente sintetiza que os direitos humanos e sua antítese (os delitos) são os mesmos fora e dentro da rede, não tendo à Internet permeado novos bens jurídicos a serem tutelados de forma específica. No entanto, há uma problemática na perspectiva defendida por essa vertente que está justamente na facilitação da impunidade, tendo em vista que, nas defesas desses criminosos, por exemplo, em geral, conseguem penas brandas porque alegam a falta de tipicidade, em que na verdade estão no Código Penal e na Constituição como a inviolabilidade da honra etc.

A segunda corrente defende que a própria Internet é evidência de uma revolução digital trazendo impactos à nossa organização social similares aos que são trazidos pela Revolução Industrial. Esse fenômeno implica uma necessidade de reinterpretação do Direito, pois mais cedo ou mais tarde outros ramos do Direito passarão a lidar com questões decorrentes da Internet, tendo em vista que essas ocorrências, metaforizadas em denúncias ocorrem de maneira alarmante na Internet.

Observando o aumento considerável de denúncias de crimes cibernéticos[2], é importante observar que pensamentos relacionados à regulação de bens de informação, proteção de dados pessoais, regulação jurídica da Internet, propriedade intelectual, delitos informáticos, contratos digitais, aspectos trabalhistas da informática e valor probatório dos suportes de informação são algumas dessas áreas de interação *online* que irão demandar análises jurídicas específicas. Claro que a maioria dos juristas ainda não está suficientemente familiarizada com essa complexidade da Internet, sobretudo o próprio Poder Judiciário.

Compreendendo os fenômenos sociais, um dos principais papéis do Direito é a consecução da Justiça para a humanidade, o que é um fator importante para a harmonia do convívio social e para a realização do bem individual e comum.

Já tínhamos a Lei nº 9.296, de 24 de julho de 1996, disciplinando a interceptação de comunicação telemática ou informática; a Lei nº 9.609, de 19 de fevereiro de 1998, tratando da propriedade intelectual do programa de computador; a Lei nº 9.983, de 14 de julho de 2000, tipificado crimes relacionados ao acesso indevido à sistemas informatizados da Administração Pública; a Lei nº 11.829, de 25 de novembro de 2008, coibindo a

[2] Acerca da pesquisa divulgada pela SaferNet Brasil (2020, s/p) os três crimes mais denunciados em seu canal em 2020 – com o contexto da pandemia - foram o de pornografia infantil, seguidos à incitação e violência contra vida e, por último, o de violência contra as mulheres ou misoginia. Como podemos ver nas informações transcritas do "Mapa de Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos" disponíveis no site da SaferNet Brasil: (I) Pornografia Infantil com 60.002 denúncias relatadas e alta de 79,58% se comparada ao ano anterior; (II) Apologia e incitação a crimes contra a vida com 27.716 denúncias e um percentual de alta de 154,46%; (III) o crime de violência contra mulheres/misoginia contando com 16.717 denúncias e crescimento de 1.639,54%; (IV) Xenofobia, principalmente contra os nordestinos com 9.705 denúncias e crescimento de 567,93%; (V) Racismo com um número de 8.337 e aumento de 37,71% se comparado ao ano anterior. A lista de denúncia não cessa, no entanto na quinta tipologia de crimes virtuais cometidos, citando mais cinco que são, respectivamente, LGBTfobia, neonazismo, maus tratos contra animais, intolerância religiosa e tráfico de pessoas

pornografia infantil na Internet e a Lei nº 13.034, de 12 de setembro de 2009, delimitando os direitos e deveres dentro da Grande Rede, durante as campanhas eleitorais.

Em 30 de novembro de 2012, mais duas leis foram sancionadas tipificando os crimes na Internet, alterando o Código Penal brasileiro e instituindo penas para crimes como invasão de computadores, disseminação de vírus ou códigos para roubo de senhas, o uso de dados de cartões de crédito e de débito sem autorização do titular, a saber: as Leis nº 12.735 e a nº 12.737.

A Lei nº 12.737, de 30 de novembro de 2012, também conhecida como "Lei Carolina Dieckmann", em virtude do episódio com a atriz que em maio de 2012, teve seu computador invadido por criminosos que divulgaram 36 (trinta e seis) fotos íntimas da mesma, causando grande transtorno e constrangimento à vítima. Concomitantemente com essa lei, fora criado o tipo penal "invasão de dispositivo informático", com previsão legal no artigo 154-A, com a ação penal disposta no artigo 154-B, condicionada à representação e ambas dispostas no Código Penal brasileiro. Apesar de ganhar espaço na mídia com o caso da atriz, o texto já era reivindicado pelo sistema financeiro diante do grande volume de golpes e roubos de senhas pela Internet. A lei, portanto, identifica atos de invasão de computadores, violação de dados de usuários e/ou "derrubar" *sites*.

Os crimes menos graves, como "invasão de dispositivo informático", podem ser punidos com prisão de três meses a um ano e multa. Condutas mais danosas, como obter pela invasão conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas podem ter pena de seis meses a dois anos de prisão, além de multa. O mesmo acontece se este delito envolve também a divulgação, comercialização, ou transmissão a terceiros, por meio de venda ou repasse gratuito, deste material obtido com a invasão de privacidade. Se isso ocorre, a pena é aumentada de um a dois terços.

A Lei nº 12.735, de 30 de novembro de 2012, também conhecida como "Lei Azeredo", tipifica condutas realizadas mediante uso de sistema eletrônico, digitais ou similares, que sejam praticadas contra sistemas informatizados e similares, e dá outras providências.

No ano seguinte, foi promulgado o Decreto - lei nº 7.962, de 15 de março de 2013, objetivando sanar lacunas do Código de Defesa do Consumidor, quanto ao comércio eletrônico (ou comércio virtual). Na sequência, a ex-presidenta Dilma Vana Roussef sancionou a Lei nº 12.965, de 23 de abril de 2014, que ficou conhecida como o Marco Civil da Internet que estabelecem princípios, garantias, direitos e deveres aos usuários e também para o Estado, regulamentando o uso da Internet no Brasil.

Assim, aquele que praticava alguns dos crimes informáticos no Brasil, dada a ausência de legislação específica e a superlotação dos presídios, acabava sendo julgado de acordo com o Código Penal, por analogias e jurisprudências. Por exemplo, caso danifique dados que estavam mantidos armazenados em *pen drives* ou CD's de uma organização ou empresa, responde pelo artigo 163 que determina: pena de detenção, de um a seis meses ou multa.

Então até 2012 não existia sequer uma lei que punisse crimes virtuais próprios e as Leis nº 12.735 e 12.737, ambas no ano de 2012 e o Decreto - lei nº 7.962/2013 sanaram algumas lacunas importantes, ao serem sancionadas com maior urgência, dada a repercussão e a relevância dos crimes.

Entretanto, apesar do amparo legal que vem sendo criado e legitimado em nosso país o que parece faltar de fato é a eficiência na efetivação dessas leis, devido à morosidade de suas implementações. Zitrain (2008, p. 70), observa os processos de aperfeiçoamento que ocorrem, à medida que, as redes informatizadas recebem novas configurações, arquitetando os ideais de generatividade na Internet. Por esse motivo, considerando a

numerosa proliferação de crimes conhecidos como *revenge porn* e os reflexos do aumento do *bullying e cyberbullying*, foram necessárias duas atualizações.

Uma delas ocorreu com a Lei nº 13.718, de 24 de setembro de 2018, que acertadamente tipificou o *reveng porn* incluindo no Código Penal brasileiro o artigo 218-C, que prevê pena de reclusão de um a cinco anos para o agente que oferecer, disponibilizar, trocar, transmitir, vender ou expor à venda; publicar, distribuir, divulgar por qualquer meio, mídia (áudio, vídeo, fotografia etc.), que contenha cena de estupro de vulnerável ou não; ou de sexo, nudez, pornografia sem o consentimento da vítima. Há também o aumento de pena de um a dois terços, caso o agente manteve ou mantenha relações íntimas de afeto com a vítima e agiu com o intuito de vingar-se ou humilhar a mesma. Se a vítima for menor de 18 anos a divulgação sempre será considerada crime independentemente de consentimento, embora para os casos em que a divulgação for consentida acima dessa idade possa haver exclusão do crime bem como se a natureza da publicação for artística, jornalística, científica, cultural ou acadêmica com a adoção de recurso que impossibilite a identificação da vítima.

A outra atualização ocorreu no ano seguinte, quando a Lei nº 13.968, de 26 de dezembro 2019, entrou em vigor alterando o artigo 122 do Código Penal brasileiro. Totalmente reformulado, esse artigo agora conta, além de seu *caput*, com sete parágrafos, detalhando casos de indução ou instigação a alguém a suicidar-se ou praticar automutilação, ou ainda prestar-lhe auxílio material para que o faça. No sentido de reprimir tal crime, a inovação veio na inclusão de uma prática que se tornou comum em desafios de jovens, principalmente depressivos que é a de automutilação. Em virtude do alinhamento e sistematização das leis penais, essa alteração deu maior destaque à proteção aos menores de 14 anos e às pessoas que por enfermidade ou deficiência mental não possuem por óbvio, o discernimento adequado, ou se vejam sem condições de oferecer a devida resistência às práticas de induzimento e instigação.

Devemos atentar para as qualificações e causas de aumento de pena analisando primeiro o disposto no *caput* do artigo 122 do Código Penal brasileiro, buscando maior atenção no exame dos parágrafos inovadores, focou-se na inovação trazida na automutilação, já que a temática do suicídio já é tradicional quando se fala do tipo penal em tela. Aparentemente apagado, o artigo 122 foi então atualizado, abarcando condutas que levem à vítima ao ato de "prática de automutilação". Na forma simples de instigação e induzimento à prática de automutilação, ou sua prestação de auxílio material, tem pena relativamente pequena. Se resultar com essas condutas, lesões corporais graves e gravíssimas a pena passa a ser maior; exceto se atingir determinadas vítimas, como o menor de 14 anos, em que a pena será a mesma da lesão corporal gravíssima, de dois anos de reclusão e, se caso resulte morte, a conduta será apenada de maneira mais forte, exceto se atingir determinadas vítimas, como o menor de 14 anos, em que a pena será a mesma do homicídio.

Segundo Antônio Horácio Boa Sorte (2018), especialista do STJ, a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD), garantirá um maior controle dos cidadãos sobre suas informações pessoais e exige consentimento explícito para a coleta e o uso de dados, obrigando a oferta de opções para que o usuário visualize, corrija e exclua esses dados. Assim, as empresas que lidem com dados terão obrigações a serem cumpridas, como por exemplo, realizar a implantação da LGPD e agora ter um encarregado pelo tratamento de dados pessoais de seus clientes. Obviamente, os escritórios de advocacia também lidam com a segurança de dados dos seus clientes, e também estão sujeitos a tais obrigações legais. Essa Lei entrou em vigor, tão somente, no segundo semestre de 2020.

3.1 Jurisprudência

Segundo Floriano (2018, p. 2), no final do primeiro semestre de 2018, o Superior Tribunal de Justiça (STJ) divulgou jurisprudência sobre fraudes eletrônicas publicando levantamento sobre precedentes que julgaram crimes cibernéticos no Brasil. Na época, esse tipo de delito já afetava anualmente 62 (sessenta e dois) milhões de pessoas e causava prejuízo de 22 (vinte e dois) bilhões de dólares, de acordo com estudo, divulgado no início de 2018, por uma empresa de segurança virtual chamada *Symantec*. Isso porque o uso cada vez mais intenso e diversificado da Internet continua abrindo caminhos para a prática de novas fraudes, ou apenas para novas formas de cometimento de antigos crimes, que são casos nem sempre fáceis de enquadrar no ordenamento jurídico brasileiro.

Ramos (2018, s/p) defende que o STJ constantemente tem interpretado normas infraconstitucionais em relação aos ilícitos praticados pela rede. O STJ manteve preso: (I) um rapaz que, frequentemente, cobrava dinheiro para não divulgar vídeos íntimos de mulheres e definiu também como furto subtrair dinheiro de contas virtuais; (II) manteve preso preventivamente um homem que usou a Internet para obter fotos e vídeos com conteúdo erótico, extorquindo mulheres para não divulgar as imagens íntimas. Neste caso, segundo as investigações, por meio de mídias sociais, este homem de 19 anos compelia jovens - incluindo alguns menores de idade - a enviar fotos e vídeos íntimos e depois exigia que lhe entregassem dinheiro e outros bens para não divulgar o material na Internet e também estendia as ameaças às famílias das vítimas.

Para o ministro relator do caso (II), Rogerio Schietti, ficou nítido que o acusado se aproveitava da vulnerabilidade das vítimas no ambiente virtual exigindo valores, que eram cada vez mais altos, a cada ato de extorsão. Ao indeferir o *Habeas Corpus*, o ministro destacou que os crimes sexuais virtuais sempre são impulsionados pela oportunidade do anonimato e, independentemente, dos aspectos que permeiam a vida pessoal e socioeconômica do criminoso, estariam "diretamente relacionados ao comportamento sexista, comumente do gênero masculino". Este processo permanece em segredo de Justiça.

No que tange ao furto bancário, a 3ª Seção do STJ firmou compreensão de que a subtração de valores de conta corrente mediante transferência eletrônica fraudulenta se caracteriza como crime de furto que, por sua vez, está previsto no artigo 155, parágrafo 4º, inciso II, do Código Penal brasileiro. Há uma frequência de discussões que, segundo Ramos (2018), chegam à Corte sobre o juízo competente para análise dos casos de furto que ocorrem através da Internet. Para esses casos, o STJ afirma que a competência se define a depender do local em que o bem da vitima foi subtraído.

Não obstante, ao apreciar Conflito de Competência 145.576/2016 em um processo de furto mediante transferência eletrônica fraudulenta de contas-correntes que ocorreu em uma agência bancária, localizada em um município do Estado de São Paulo. Nesse caso, mesmo que os valores tenham sido enviados para o Estado do Maranhão, o colegiado ponderou que o juízo da cidade paulista tem sim a competência para julgar o caso, haja vista que os valores foram subtraídos das vítimas a partir da localidade paulista.

Quanto ao comércio *online*, definido em outro Conflito de Competência 133.534/2014, a Corte pacificou o entendimento que, criar *sites* na Internet para vender mercadorias com a intenção de nunca entregá-las, é conduta que se amolda perfeitamente ao crime contra a economia popular, previsto no artigo 2º, inciso IX, da Lei nº 1.521, de 26 de dezembro de 1951. Segundo esta decisão, ao se criar *sites* para vender produtos fictícios pela Internet, os criminosos não têm por objetivo selecionar e enganar determinadas pessoas, mas sim um número indeterminado de vítimas, comercializando com qualquer um que acesse tal *site*.

Em 2018, um empresário foi denunciado por induzir compras virtuais de produtos que não eram entregues, teve negado o pedido para que fosse revogada ordem de prisão emitida contra ele. Para negar o recurso em *habeas corpus* nº 65.056/2015, a 5ª Turma considerou não haver ilegalidade no decreto prisional, baseado entre outros elementos; na garantia de ordem pública e no provável risco de reiteração delitiva. Constava do processo que o denunciado registrava domínios de vários *sites* e oferecia produtos eletrônicos como *tablets, notebooks* e câmeras digitais por valores muito menores que aqueles normalmente praticados no mercado.

Sobre o crime de ameaças, nas hipóteses dessas serem feitas por redes sociais e seus respectivos aplicativos como *Facebook*, *Telegram*, *Viber* e *WhatsApp*, o STJ tem decidido que o juízo competente para julgamento de pedido de medidas protetivas será aquele de onde a vítima tomou conhecimento dessas intimidações, por ser este o local de consumação do crime previsto no artigo 147 do Código Penal brasileiro.

Neste sentido, e com base nesse entendimento, a 3ª Seção fixou a competência da comarca de um município do Mato Grosso do Sul para a análise de pedido de concessão de medidas protetivas em favor de uma mulher que teria recebido pelo *WhatsApp* e *Facebook* mensagens de texto com ameaças de uma pessoa residente no Paraná. O relator do caso, ministro Ribeiro Dantas, destacou que conforme o artigo 70 do Código de Processo Penal brasileiro, este já estabelece que a competência seja em regra, determinada pelo lugar onde se consuma a infração. Quanto às provas ilícitas, o STJ vem adotando a tese de que é ilícita a prova obtida diretamente dos dados armazenados no celular do acusado.

A jurisprudência do Tribunal entende que são inválidos Serviços de Mensagens Curtas (SMS) e conversas por meio de aplicativos como o *WhatsApp* obtidas diretamente pela polícia no momento da prisão em flagrante, sem a prévia autorização judicial. Neste caso de Recurso de *Habeas Corpus* nº 92.801 analisado, policiais civis acessaram as mensagens que apareciam no *WhatsApp* do celular do acusado no momento da prisão em flagrante, sem a devida ordem judicial. De acordo com esse *Habeas Corpus* analisado pela 5ª Turma, a prova obtida tornou-se ilícita e teve então de ser retirada dos autos, assim como todos os outros elementos probatórios derivados diretamente dela. Segundo o ministro relator Felix Fischer, esses conteúdos armazenados nos celulares decorrentes de envio ou recebimento de dados por SMS, programas ou aplicativos de troca de mensagens, ou mesmo por correios eletrônicos, dizem respeito à intimidade e à vida privada do indivíduo, sendo, portanto invioláveis, nos termos do artigo 5°, X, da Constituição da República Federativa do Brasil, de 1988.

Em outro recurso de *habeas corpus* nº 89.981/2017, segundo informações da Assessoria de Imprensa do STJ, este Tribunal também anulou provas obtidas por policiais que acessaram o conteúdo do celular de um suspeito: mensagens que indicavam o repasse de informações sobre imóveis onde uma quadrilha pretendia cometer furtos, por falta de autorização judicial devidamente motivada para este tipo de análise, o que nem sequer foi requerido, e concluiu assim, o relator ministro Reynaldo Soares da Fonseca, ao determinar o desentranhamento das provas.

3.2 Críticas, desafios e lacunas persistentes

Uma das críticas mais contundentes à "Lei Carolina Dieckmann" foi em razão do temor de supressão da liberdade virtual, e, principalmente, por prever a obrigatoriedade dos órgãos da polícia judiciária se estruturar com o objetivo de combater a criminalidade digital, quando veio a ser promulgada. Outra foi relacionada à violação de dispositivos de segurança, praticamente, deixando desprotegidos aqueles tantos milhões de usuários que

não instalam antivírus e outras barreiras. Ademais, alguns vícios foram apontados, como não considerar crime a indisponibilidade de sistemas de informação de instituições privadas, como, por exemplo, sites bancários. Até mesmo o termo "dispositivo informático" utilizado mereceu destaque numa crítica feita pelo Ministério Público Federal em 2015, devido à falta de definição. Podendo ser mais abrangente com o termo “equipamentos eletrônicos”, haja vista que atualmente possuem amplo acesso à Internet.

Já o Marco Civil da Internet continha muitos artigos, inclusive que responsabilizariam os provedores de Internet, e durante a tramitação quatro artigos foram reduzidos a dois por veto na sanção. Requerer a obtenção de ordens judiciais, que tem seu uso muito comum, porém com certa morosidade no ambiente físico; de forma análoga para o âmbito virtual parece incompatibilizar a velocidade contida nos dois ambientes.

No tocante ao julgamento dos crimes virtuais, entende-se que a maioria seja de competência federal, segundo entendimento do Supremo Tribunal Federal (STF), mas os crimes contra a honra, praticados virtualmente, são de competência estadual; exceto os que envolvam crianças e adolescentes que são regidos pelo artigo 241-A do Estatuto da Criança e do Adolescente (ECA). Então caberá sempre uma análise minuciosa dos casos, que poderia ser facilitada, caso se promulgasse uma lei processual que obrigasse mais rapidamente os provedores a informar os dados de endereço de Protocolo da Internet (IP), *login* e senha dos criminosos, demandando habilidade e destreza dos peritos que precisam estar à disposição das autoridades.

Segundo Dodge (2013, p. 22), em termos técnicos, um endereço IP é um número inteiro de 32 (trinta e dois) *bits*, que por sua vez é uma simplificação do termo "dígito binário" - *binary digit* em inglês. Diante disso, assinala Pasinato (2017 p. 13) que, "um delito, quando é praticado pela Internet, é possível através da identificação do IP da máquina utilizada atribuir a responsabilidade ao proprietário ou usuário do equipamento eletrônico".

Como a evolução da tecnologia é constante, Cerqueira e Rocha (2013, p. 155) apontam outro requisito imprescindível para a adequada coleta de provas: a disponibilidade de equipamentos com grande poder de processamento, de conectividade e franco acesso à rede mundial de computadores, pois é o que ocasiona cada vez mais a sofisticação dos delitos.

Percebemos que, a considerável maioria, dos bons peritos e interessados no tema de criminalidade digital está nos grandes centros do país e isso reforça a necessidade de descentralização de capacitações, o que evidencia o desafio que a instalação de delegacias virtuais em todo o território nacional se propõe, embora previsto pela Lei Carolina Dieckman.

4 CONSIDERAÇÕES FINAIS

Talvez seja impossível oferecer segurança aos usuários frente a uma legislação que não atenda às demandas de uma sociedade cada vez mais conectada. Mesmo os *sites* oficiais e governamentais do mundo inteiro parecem vulneráveis aos ataques por *cibercriminosos,* então é preciso tomar decisões efetivas no que tange à proteção das informações e dados dos usuários.

Constata-se que a inovação jurídica e a deficiência da persecução penal apresentadas nesse trabalho requerem muito mais que atualizações e regulamentações de novas leis no ordenamento jurídico brasileiro, pois o ritmo de evolução tecnológica será sempre mais veloz que o da atividade legislativa. É de suma importância que uma

legislação penal vigore, se adequando a essa realidade mundial quanto aos crimes cometidos pela Internet, protegendo os direitos dos internautas e atendendo a essas condutas criminosas que têm por objetivo afetar a vítima ou o seu computador. E em outros casos, tais delitos podem afetar uma rede maior de computadores, como o caso de empresas e departamentos públicos, acarretando uma maior insegurança e violação jurídica dos dados dos cidadãos, uma vez que, já é indispensável no dia a dia o uso constante dos serviços virtuais.

A resolução da questão problema da pesquisa foi alcançada, ao menos em níveis de discussão, uma vez que, ainda falta muito para colocar em prática todas essas mudanças. Sendo importante ressaltar a necessidade que providências possam ser tomadas, assim que os fatos criminosos sejam noticiados, ensinando como denunciar e qual a proteção que a população tem de segurança perante a legislação, pois aparentemente a popularização da Internet possivelmente fará com que o mundo fique constantemente refém dos *crackers*. A sociedade contemporânea poderá vivenciar um possível colapso de segurança dos sistemas de informação relacionada à Internet, caso não haja um maciço investimento dos governos em informação, segurança e diretrizes que analisem a atual legislação brasileira pertinente ao tema dos crimes virtuais que o direito penal precisa transpor.

Boa parte da evolução tecnológica comumente utilizada para a prática de crimes está diante da evolução jurídica no intuito de coibir tais práticas. Porém o ordenamento jurídico brasileiro não admite existência de crimes sem lei anterior que os defina, lançando um desafio descomunal aos legisladores. O esforço para que isso ocorra de forma clara e precisa tem de se dar com uma harmonização entre prevenção, investigação e combate aos crimes digitais em âmbito mundial, com ampliação da efetivação das legislações penais, no sentido de se resguardar a segurança telemática.

Embora alguns avanços tenham sido alcançados nos últimos anos, penalmente temos visto que a tutela dos bens como a intimidade, a privacidade, o sigilo de correspondência, de comunicações telegráficas e dados não são tão efetivos quando estes sofrem ataques virtuais, mesmo com a proteção conferida pela Constituição da República Federativa do Brasil, de 1988. Boa parte das condutas ofensivas e imorais contra esses bens tem sido repreendida com penas ínfimas, e também percebemos uma fragilidade imensa pela responsabilidade penal dos provedores de acesso não serem contemplados pela Constituição.

Tanto no Brasil quanto no resto do mundo, um esforço maior de cooperação entre as nações poderia ser benéfico para os cidadãos, que têm suas vidas cada vez mais interligadas à Internet, já que um mesmo cidadão pode cometer crimes virtualmente em qualquer parte, de diversas formas, afetando pessoas em qualquer lugar, ampliando seu número de vítimas substancialmente a cada investida, e por esta razão, o Mercosul já poderia ter dado um passo importante nesse sentido liderado pelo Brasil que é o maior país do bloco, para tratar sobre os desafios e as soluções de crimes cometidos em ambiente *online*. A aprovação de projetos de lei que possam criminalizar de forma mais contundente os crimes cibernéticos é uma necessidade mais que urgente em nosso País.

O Brasil pode buscar acompanhar o bom exemplo da Austrália, com temas voltados ao Direito na escola, mesclando inovações e conteúdos relacionados - de forma intertextualizada - ao comportamento nas mídias digitais, atuando como meio de prevenção de possíveis condutas ilícitas e seus reflexos. Assim, os alunos de diversas idades e no país inteiro, a partir das séries iniciais, já poderiam repassar aos seus amigos e familiares, os conhecimentos bem como as medidas úteis e simples para evitar a vitimização e delitos na seara digital.

Além da adesão aos tratados internacionais já existentes, o aperfeiçoamento das disposições presentes inclusive na Convenção de Budapeste já demonstram a necessidade

de celeridade no enfrentamento considerando o dinamismo presente nas tecnologias mundo afora, que o Brasil precisa acompanhar. Por fim, o Direito deve acompanhar a constante mudança da evolução da sociedade digital, aprimorar-se, renovar seus institutos e criar novas ferramentas para continuar garantindo a segurança jurídica das relações sociais, sob pena de ficar obsoleto.

REFERÊNCIAS

AUSTRALIAN FEDERAL POLICE. **Cyber crime**, 2020. Disponível em: https://www.afp.gov.au/what-we-do/crime-types/cyber-crime. Acesso em 30 set. 2020.

AGUIAR, A.J. **Qual é a diferença entre Dark Web e Deep Web?** (2018). Disponível em: https://m.tecmundo.com.br/internet/128029-diferenca-entre-dark-web-deep-web.htm. Acesso em: 22 ago. 2020.

BAHIA. Superior Tribunal de Justiça (STJ). **Recurso em Habeas Corpus nº 65.056** - BA (2015/271136-8) julgado em (20/03/2018). Ministro Relator Joel Ilan Paciornik.

BRASIL. Código Penal. Decreto - Lei nº 2.848, de 7 de dezembro de 1940. ***Vade Mecum***. 11. ed., São Paulo: Saraiva, 2017.

BRASIL. Decreto-Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. ***Vade Mecum***. 11. ed., São Paulo: Saraiva, 2017.

BRASIL. Decreto-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. ***Vade Mecum***. 11. ed., São Paulo: Saraiva, 2017.

BRASIL. Decreto-Lei nº 7.962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. ***Vade Mecum***. 11. ed., São Paulo: Saraiva, 2017.

BRASIL. Decreto - Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). ***Vade Mecum***. 11. ed., São Paulo: Saraiva, 2018.

BRASIL. Decreto-Lei nº 13.718, de 24 de setembro de 2018. Altera o decreto-lei nº 2.848, de 7 de dezembro de 1940 (código penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do decreto-lei nº 3.688, de 3 de outubro de 1941 (lei das contravenções penais). ***Vade Mecum***. 11. ed., São Paulo: Saraiva, 2018.

BRASIL. Decreto-Lei nº 13.968, de 26 de setembro de 2019. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para modificar o crime de incitação ao suicídio e incluir as condutas de induzir ou instigar a automutilação, bem como a de prestar auxílio a quem a pratique. ***Vade Mecum***. 11. ed., São Paulo: Saraiva, 2019.

CERQUEIRA, S.C.; ROCHA, C. Crimes cibernéticos: desafios da investigação. *In:* **Cadernos Aslegis**. Brasília, n. 49 (2013). Disponível em: https://bd.camara.leg.br/bd/handle/bdcamara/27420. Acesso em: 24 ago. 2020

BORTOT, J.F. **Crimes cibernéticos:** aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. (2017). Disponível em: http://periodicos.pucminas.br/index.php/virtuajus/article/view/15745/15745-56007-1.. Acesso em: 26 jun. 2020.

CORREA, G.T. **Aspectos jurídicos da Internet.** São Paulo: Saraiva, 2000.

DODGE, R.E.F. (Coord.). **Roteiro de atuação:** crimes cibernéticos. 2. ed., Brasília: Ministério Público Federal. (2013) – (Série Roteiro de atuação 5). Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Roteiro_crimes_cibernetics.pdf. Acesso em: 17 jul. 2020.

FLORIANO, F. Projeto de Lei nº 10.535, 04 de Julho 2018. **Câmara dos Deputados**. (2018). Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=B6BF31A5FE63298384B293703A3D3B86.proposicoesWebExterno2?codteor=1674494&filename=Tramitacao-PL+10535/2018. Acesso em: 24 jun. 2020.

GRECO FILHO, V. **Algumas observações sobre o direito penal e a internet**. (2000). Disponível em: https://arquivo.ibccrim.org.br/boletim_editorial/160-95-Outubro-Esp-2000. Acesso em: 12 jun. 2020.

MARANHÃO. Superior tribunal de justiça (STJ). **Conflito de Competência nº 145.576** - MA (2016/0055604-1) julgado em (13/04/2016). Ministro Relator Joel Ilan Paciornik.

MINAS GERAIS. Superior Tribunal de Justiça (STJ). **Recurso em Habeas Corpus nº 89.981**-MG (2017/02509663) julgado em (05/12/2017). Ministro Relator Reynaldo Soares da Fonseca.

NASCIMENTO, S.P. **Cibercrime**: Conceitos, modalidades e aspectos jurídicos-penais. (2019). Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/#:~:text=Esse%20crime%20consiste%20em%20fraudar,(ROSA%2C%202002%2C%20p. Acesso em: 23 jun. 2020.

NUNES, L. **Revista publica foto de Diana agonizando**. (2006). Disponível em: http://www.observatoriodaimprensa.com.br/monitor-da-imprensa/revista-publica-foto-de-diana-agonizando/. Acesso em: 17 jun. 2020.

OLIVEIRA, B.M. *et al*. **Crimes virtuais e a legislação brasileira**. (2017). Disponível em: https://core.ac.uk/download/pdf/229767447.pdf. Acesso em: 26 jun. 2020.

PASINATO, D.C. de A. **A tecnologia da informação na investigação policial**. (2017). Disponível em: http://www.arcos.org.br/artigos/a-tecnologia-da-informacao-na-investigacao-policial/. Acesso em: 17 jul. 2020.

PICCOLO, L. **O papel da computação na guerra contra "fake news"**. (2019). Disponível em: http://horizontes.sbc.org.br/index.php/2019/12/o-papel-da-computacao-na-guerra-contra-fake-news/. Acesso em: 24 jun. 2020.

RAMOS, C.E.C. **STJ divulga jurisprudência sobre conceitos de crimes pela Internet**. (2018). Disponível em: http://www.cavalcanteramos.adv.br/tag/direito-empresarial/. Acesso em: 26 jun. 2020.

SAFERNET BRASIL. **Mapa de Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos**. Disponível em: https://indicadores.safernet.org.br/. Acesso em: 01 de Out. de
2020.

SANTA CATARINA. Superior Tribunal de Justiça (STJ). **Agravo Regimental no Recurso Ordinário em Habeas Corpus nº 92.801** - SC (2017/0322640-7) julgado em (20/03/2018). Ministro Félix Fischer.

SANTOS, L.R.; MARTINS, L.B.; TYBUCSH, F.B.A. **Os crimes cibernéticos e o direito a segurança jurídica**: uma análise da legislação vigente no cenário brasileiro contemporâneo. (2017). Disponível em: http://coral.ufsm.br/congressodireito/anais/2017/7-7.pdf. Acesso em: 27 jun. 2020.

SILVEIRA, S.A. (Orgs.). **Inclusão digital, software livre e globalização contra-hegemônica**. Volume 7. (2003). Disponível em: http:// http://www.softwarelivre.gov.br/softwarelivre/artigos/artigo_02. Acesso em: 21 jan. 2020.

SIMÃO FILHO, A.; ZACARIAS, F. **Direito à privacidade na sociedade da informação**. (2018). Disponível em: http://www.periodicoseletronicos.ufma.br/index.php/revistahumus/article/download/8351/6475. Acesso em: 12 jun. 2020.

SORTE, A.H.B. (Esp.). **Crimes pela internet, novos desafios para a jurisprudência**. (2018). Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-06-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx. Acesso em: 25 set. 2020.

SYDOW, S.T. **Delitos informáticos próprios:** uma abordagem sob a perspectiva vitimodogmática. 2009. 282 p. Dissertação (Direito) - Faculdade de Direito do Largo São Francisco, Universidade de São Paulo, São Paulo (2009). Disponível em: https://www.passeidireto.com/arquivo/73891847/dissertacao-mestrado-versao-parcial-formatada-padroes. Acesso em: 26 jun. 2020.

TEIXEIRA, T. **Direito Eletrônico**. 4º Ed. São Paulo: Joarez de Oliveira, 2007.

VIANNA, T.L.. **Do Acesso Não Autorizado a Sistemas Computacionais**: Fundamentos de Direito Penal Informático. Disponível em http://www.bibliotecadigital.ufmg.br/dspace/bitstream/handle/1843/BUOS96MPWG/disserta o_t_lio_lima_vianna.pdf?sequence=1. Acesso em 01 de Out. de 2020.

ZITTRAIN, J. **The future of internet: and how to stop it**. New Haven; London: Yale University Press, 2008

AGRADECIMENTOS

A Jesus Cristo, filho de Deus, pois sem sua misericórdia em nos guiar, permitindo que em nossa longa viagem pela vida que ‘nenhum fio de cabelo de nossas cabeças’ fosse perdido, não estaríamos aqui há muito tempo.

Agradeço aos meus pais Manassés Marques da Silva (*in memorian*) e Inês Gonçalves dos Santos, que nunca mediram esforços para me sustentar, cuidar de minha saúde e permitir que eu pudesse estudar com muito sacrifício. Mãe, sei que negastes viver uma vida melhor para doar todo teu esforço toda a tua saúde e força para que eu sobrevivesse até hoje e pudesse um dia me formar, me tornando uma pessoa cada vez melhor.

Agradeço aos meus padrinhos, que sempre estiveram de prontidão nos momentos mais difíceis de minha vida e auxiliaram meus pais na minha formação, assim como todos os meus primos do Rio de Janeiro que me viram crescer.

Agradeço também a todos os tios e primos que me acolheram em minha jornada pelo estado da Paraíba, especialmente à minha avó Etelvina Gonçalves de Maria (*in memorian*).

À minha esposa Sayonara Fernanda Jácome de Moura Gonçalves e minha sogra Helena Melo de Moura que sempre me incentivaram à conclusão deste curso.

Às minhas amadas filhas Adríny Santos Marques e Letícya Helena Jácome Gonçalves que me fizeram compreender que também preciso viver por elas que são os melhores presentes que Deus poderia me dar: são heranças do Senhor para a minha vida inteira.

Aos meus irmãos Rafael Gonçalves e Halley Gonçalves Marques da Silva (*in memorian*) com os quais partilhei a aurora da minha vida e ajudaram na minha caminhada por essa existência.

A todos os colegas da turma 2014.1 do curso de Direito da UEPB, principalmente àqueles que me ajudaram muito com o suporte de seus conhecimentos. À Professora e orientadora Dra. Aureci Gonzaga Farias, com quem pude compartilhar maravilhosos sorrisos e muita troca de conhecimento. Nossa amizade estendeu-se para além dos limites da Universidade ainda que virtualmente. Afirmo que só tenho carinho e admiração pela dedicação e empenho com que trata sua missão.

Aos professores que aceitaram o convite para compor a banca examinadora e a todos que direta ou indiretamente contribuíram para que eu conseguisse concluir mais esta etapa de minha vida, deixo o meu muito obrigado!