UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS JURÍDICAS – CCJ
DEPARTAMENTO DE CIÊNCIAS JURÍDICAS – DCJ
CURSO DE DIREITO (UNIDADE SANTA RITA)
TRABALHO DE CONCLUSÃO DE CURSO

DOUGLAS MAGNO FERNANDES DO NASCIMENTO LIMA

OS DESAFIOS DA INVESTIGAÇÃO NOS CRIMES CIBERNÉTICOS

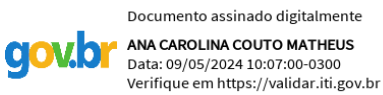
SANTA RITA – PB
2024

DOUGLAS MAGNO FERNANDES DO NASCIMENTO LIMA

OS DESAFIOS DA INVESTIGAÇÃO NOS CRIMES CIBERNÉTICOS

Trabalho de Conclusão de Curso apresentado ao Departamento de Ciências Jurídicas (DCJ) do Centro de Ciências Jurídicas (CCJ) da Universidade Federal da Paraíba (UFPB), como requisito obrigatório para a obtenção do título de Bacharel em Direito.

Orientadora: Profa. Dra. Ana Carolina Couto Matheus.



SANTA RITA – PB
2024

Catalogação na publicação Seção de Catalogação e Classificação

L732d Lima, Douglas Magno Fernandes do Nascimento.
Os desafios da investigação nos crimes cibernéticos
/ Douglas Magno Fernandes do Nascimento Lima. - Santa Rita, 2024.
74 f. : il.

Orientação: Ana Carolina Couto Matheus. TCC
(Graduação) - UFPB/CCJ/DCJ.

1. Direito penal. 2. Crime cibernético. 3. Persecução penal. I. Matheus, Ana Carolina Couto. II. Título.

UFPB/DCJ/CCJ-SANTARITA CDU 34

Elaborado por ANA BEATRIZ DE OLIVEIRA ABRANTES SILVA - CRB- 15/596

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS JURÍDICAS
DIREÇÃO DO CENTRO
COORDENAÇÃO DE MONOGRAFIAS
DEPARTAMENTO DE CIÊNCIAS JURÍDICAS
DISCIPLINA: TRABALHO DE CONCLUSÃO DE CURSO

CCJ Centro de Ciências Jurídicas

DISCIPLINA: TRABALHO DE CONCLUSÃO DE CURSO – TCC

ATA DA BANCA EXAMINADORA DA DEFESA PÚBLICA DO TRABALHO DE CONCLUSÃO DE CURSO

Ao vigésimo quinto dia do mês de Abril do ano de dois mil e vinte quatro, realizou-se a sessão de Defesa Pública do Trabalho de Conclusão do Curso de Direito intitulado "Os desafios da investigação nos crimes cibernéticos", sob orientação do(a) professor(a) Ana Carolina Couto Matheus que, após apresentação oral, foi arguido pelos integrantes da Banca Examinadora que se reuniram, reservadamente, e decidiram emitir parecer favorável à APROVAÇÃO, de acordo com o art. 33, da Resolução CCGD/02/2013, do(a) aluno(a) Douglas Magno Fernandes do Nascimento Lima com base na média final de 9,5 (nove pontos e meio). Após aprovada por todos os presentes, esta ata segue assinada pelos membros da Banca Examinadora.

Ana Carolina Couto Matheus

Alex Taveira dos Santos

Wyrna Karenina Marques de Sousa

AGRADECIMENTOS

Agradeço a Deus pelas promessas cumpridas, pelo conforto em noites turbulentas e pela fidelidade. Aos meus pais por acreditarem na educação e em todo investimento feito ao longo da minha vida estudantil. Ao meu irmão por sempre me apoiar para que eu conquiste meus objetivos. Nada disso seria possível sem tê-los ao meu lado.

A todo corpo docente do Departamento de Ciências Jurídicas, aqui eu aprendi o que é um Direito humano, para além das normas jurídicas.

Em especial agradeço a professora orientadora, Ana Carolina Couto Matheus, que não olvidou esforços em apoiar e esclarecer detalhadamente o norte necessário para a produção do presente estudo, sendo a pessoa que reservou parte de seu tempo para realizar as correções, apontamentos salutares e indispensáveis ao desenvolvimento da monografia. Agradeço por todo trato e carinho ao longo dessa caminhada, a qual fez ser menos árdua.

Agradeço aos Professores Examinadores por aceitarem o convite para compor a minha banca, pela disponibilidade e generosidade em contribuir com o meu trabalho de pesquisa e com a conclusão deste ciclo.

Aos meus colegas de turma, por termos passado juntos por essa experiência, que é algo que guardarei dentro de mim para toda a minha vida. Por dividirem comigo as angústias da vida acadêmica, assim como as vitórias. Não tenho dúvidas que serão todos profissionais incríveis.

Quereis prevenir delitos? Fazei com que as leis sejam claras e simples.

Cesare Beccaria

RESUMO

O presente trabalho tem como escopo mostrar os desafios da investigação nos crimes cibernéticos, abordando as principais legislações concernentes a esse tipo de delito, dando enfoque ao crime de invasão de dispositivo informático, único crime exclusivamente cibernético disposto no art. 154-A do Código Penal pela Lei nº 12.737/12. Utilizando o método de pesquisa dedutivo foi possível vislumbrar o atual cenário legislativo responsável por regular esse âmbito, tendo em vista que a lei é o principal norte para a realização da *persecutio criminis*. Deste modo, as reflexões acerca no tema se iniciam com uma breve análise histórica da *Internet*, com o intuito de mostrar como o ciberespaço se tornou o principal ambiente para práticas ilícitas, tornando os usuários diariamente vulneráveis àqueles que intentam obter vantagens através da lesão aos bens jurídicos, sobretudo relativos à intimidade e privacidade, dispostos no art. 5º da Constituição Federal. Ademais, após o desmembramento dos principais pontos estruturais do conceito de *cibercrime*, foi apresentada uma evolução histórico-legislativa das normas que visam prevenir os delitos virtuais, explanando sua respectiva ineficácia.

Palavras-chave: Direito Penal; Crime Cibernético; Persecução Penal.

ABSTRACT

The purpose of this work is to show the challenges of investigating cybercrimes, addressing the main legislation concerning this type of crime, focusing on the crime of invading a computer device, the only exclusively cybercrime provided for in art. 154-A of the Penal Code by Law number 12.737/12. Using the deductive research method, it was possible to glimpse the current legislative scenario responsible for regulating this area, considering that the law is the main guide for carrying out persecutio criminis. Therefore, reflections on the topic begin with a brief historical analysis of the Internet, with the aim of showing how cyberspace has become the main environment for illicit practices, making users daily vulnerable to those who try to obtain advantages through damaging property. Legal provisions, especially those relating to intimacy and privacy, set out in art. 5th of the Federal Constitution. Furthermore, after breaking down the main structural points of the concept of cybercrime, a historical-legislative evolution of the norms that aim to prevent virtual crimes was presented, explaining their respective ineffectiveness.

Keywords: Criminal Law; Cybercrime; Criminal Persecution.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
ARPA	Advanced Research Projects Agency Network
ARPAnet	Advanced Research Projects Agency Network
ART	Artigo
BITNET	Because It's Time Network
CUNY	City University of New York
ECA	Estatuto da Criança e do Adolescente
EUA	Estados Unidos da América
FAPESP	Fundação de Amparo à Pesquisa do Estado de São Paulo
IP	Internet Protocol
LGPD	Lei Geral de Proteção de Dados
LNCC	Laboratório Nacional de Computação Científica
MCT	Ministério da Ciência e Tecnologia
Nº	Número
RNP	Rede Nacional de Pesquisa
TCP/IP	Transmission Control Protocol/Internet Protocol
UFRJ	Universidade Federal do Rio de Janeiro
URSS	União das Repúblicas Socialistas Soviéticas
WWW	World Wild Web

SUMÁRIO

1 INTRODUÇÃO

Após a revolução tecnológica e digital advinda, sobretudo, da eclosão da Internet, o modo de comunicação se transformou demasiadamente, gerando interações cada vez mais instantâneas e globais, onde o meio cibernético se tornou o principal ambiente responsável por manter as relações sociais, e onde os indivíduos passam a maior parte do tempo, compartilhando dados e informações de qualquer natureza.

Todavia, essas mudanças não promoveram apenas benefícios às atividades diárias, mas concomitantemente, inúmeras ameaças aos bens jurídicos, visto que se trata de um espaço em que não é possível manter um controle e fiscalização em decorrência de sua alta volatilidade, abrindo deste modo, diversas oportunidades para a prática de crimes cibernéticos.

Ademais, um dos procedimentos mais relevantes do sistema jurídico é a Persecução Penal, por meio desta, a Polícia Judiciaria será encarregada para investigar o fato delituoso, devendo, portanto, respeitar os ditames legais.

Sendo assim, a falta de normas exclusivas e próprias de determinada matéria, tornará a conduta criminosa atípica, por isso se exige que o ordenamento jurídico esteja em consonância com as modificações e atualizações presentes na sociedade, visando assim, tipificá-las e evitar possíveis lacunas, caso contrário, o Estado tornar-se-á inabilitado para punir os modernos comportamentos ilícitos.

A produção de normas específicas consoante aos crimes virtuais já é uma realidade no ordenamento jurídico brasileiro, no entanto, esse desenvolvimento ainda é lento e gradual, resultante inclusive da celeridade do legislador em sanar vacuidade normativa decorrente do clamor popular, elaborando tipos penais inoperantes na prática, criando um extenso leque de dispositivos legais meramente simbólicos.

Em vista disso, o primeiro capítulo do presente trabalho abordará de modo amplo e contextualizado o surgimento e deslanche da Internet, principal ferramenta responsável por propulsionar a evolução tecnológica, além de uma breve explanação sobre o modo como essas mudanças impactaram de forma negativa na sociedade, incluindo a eclosão de delitos virtuais em demasia.

O segundo capítulo consistirá no desmembramento do conceito e aspectos

do crime cibernético propriamente dito, apresentando suas respectivas nuances, incluindo os princípios essenciais que norteiam a produção dos tipos penais responsáveis por regular a contenção desses ilícitos praticados no ciberespaço.

Sendo assim, o terceiro capítulo abordará de modo cronológico algumas normas responsáveis por prevenir os crimes cibernéticos. Mas será que esse singelo acervo detém o condão para de fato gerar intimidação àqueles que visam lesionar os bens jurídicos através da esfera virtual? Tais normas possuem uma aplicabilidade impecável que servirá como forte apoio ao sistema judicial na resolução de conflitos?

As respostas para essas hipóteses serão apresentadas nos capítulos quarto e quinto, os quais irão abordar as principais dificuldades encontradas durante o processo de investigação criminal dos crimes virtuais.

Além disso, desmembrará o art. 154-A do Código Penal advindo da Lei nº 12.737/12, referente ao crime de “invasão de dispositivo informático”, por se tratar do único delito exclusivamente cibernético. Desta forma, por meio de um exemplo concreto será possível avaliar de maneira prática a (in) eficácia existente nos tipos penais concernentes aos delitos virtuais.

Em vista disso, este trabalho terá natureza qualitativa, pois não abordará nenhum tipo de elemento estatístico, mas sim a análise de dados para a compreensão do fenômeno que influi tanto no desenvolvimento da contenção dos cibercrimes, quanto os seus respectivos empecilhos presentes no processo investigativo. Posto isto, a pesquisa possui como principal objetivo expor a fragilidade do ordenamento jurídico frente aos modernos meios digitais.

Além disso, foi utilizado o método dedutivo, partindo do geral para o particular, assim, os argumentos devem se apresentar como verdadeiros, visto que já possuem validação pela ciência. A questão fundamental da dedução está na relação lógica que deve ser estabelecida entre as proposições apresentadas, a fim de não comprometer a validade da conclusão.

Utiliza, ainda, os métodos de procedimento documental e bibliográfico, visto que traz elementos advindos de legislação, jurisprudência, coleta de dados em artigos científicos, teses, dissertações e livros.

2 O SURGIMENTO E A EXPANSÃO DA INTERNET

O ser humano moderno está inserto em um contexto onde o desenvolvimento dos meios digitais cresce de modo exponencial. Além disso, as atividades diárias são demasiadamente pragmáticas, basta apenas um clique ou o acionamento de um dispositivo eletrônico para que seja possível obter: comidas, roupas, pagar faturas ou conhecer uma pessoa, por exemplo, assim, quase tudo se tornou instantâneo.

Todavia, essas transformações trouxeram mudanças consideráveis em todo o mundo, não apenas no que tange ao aparato tecnológico e seu alto consumo, mas também na forma de pensar dos indivíduos, e por consequência, no seu comportamento e modo de agir, pois passam a realizar condutas repetitivas e automáticas em um ciclo altamente vicioso resultante da era virtual.

> Toda revolução tem a sua consequência. A era digital trouxe inúmeras para a humanidade. A principal delas é o dinamismo e a agilidade na propagação da informação. Enviar e receber conteúdos atualizados 24 horas por dia, podendo ser acessados a qualquer instante, seja dia ou noite, de qualquer ponto que tenha uma conexão de dados, é uma das características da Internet (Carvalho, 2014, p. 1).

Ademais, essa praticidade apresenta concomitantemente muitos riscos, pois os usuários passaram a expor de maneira exacerbada seus dados e informações na rede mundial de computadores, o que acarreta o interesse de terceiros e agentes criminosos em busca de benefícios ilicitamente. Consoante à Borges:

> É certo que a criminalidade, obviamente, não deixaria de aproveitar as oportunidades trazidas pelas novas tecnologias, e a prática de ilícitos na Internet é uma realidade perversa, com um sem número de fraudes bancárias, extorsões decorrentes de invasões de computadores, vírus e programas espalhados pela rede para obtenção de dados que permitam a prática criminosa, pornografia infantil e muitas outras condutas ilícitas ou reprováveis (Borges, 2015, p. 1).

Posto isto, nota-se que, o mau uso das ferramentas digitais, gera grande impacto não apenas nas relações sociais, mas também no ordenamento jurídico. Além disso, a tendência contemporânea e futura está na substituição das ações do meio físico para o eletrônico, logo, é necessário analisar as normas legais referentes aos crimes virtuais por outra perspectiva, promovendo assim, mais segurança aos

usuários, para que possam usufruir com mais tranquilidade do vasto e infinito espaço cibernético.

Deste modo, percebe-se que essa acelerada mudança de hábitos dirimiu inclusive as relações físicas e dificuldades decorrentes do distanciamento geográfico, basta o interesse comum entre os usuários para que associações e negócios possam existir, por isso, as plataformas digitais possibilitam uma infinidade de atividades no ciberespaço, gerando uma sociedade multifacetária em constante conexão.

Destarte, a grande revolução do século XXI trouxe entre suas inúmeras mudanças uma nova maneira de comunicação, afinal, o mundo se reformulou após a eclosão da Internet, portanto, é imprescindível apresentar uma breve análise histórica dessa ferramenta, bem como sua expansão no território nacional, pois somente a partir de então, surgiram os crimes cibernéticos, objeto de estudo do presente trabalho.

2.1 O SURGIMENTO DA INTERNET

Para compreender o surgimento dos cibercrimes, é importante ressaltar a eclosão da principal ferramenta que serve como suporte para a prática de tais delitos: a Internet. Desde a era mais remota, o ser humano necessita utilizar códigos para realizar sua própria comunicação, isso se torna evidente quando se analisa, por exemplo, as artes rupestres e primeiras invenções tecnológicas, como o telégrafo, inventado pelo americano Samuel Morse em 1835, o qual visava proporcionar uma forma de comunicação instantânea entre pessoas que estavam distantes.

A necessidade de lograr uma comunicabilidade mais ágil e precisa ainda perdura, devido, sobretudo, ao dinamismo da “modernidade líquida”, conceito denominado pelo sociólogo polonês Zygmunt Bauman, que se dedica ao trabalho de fazer sociologia, analisando a sociedade contemporânea na pós-modernidade em uma época em que as relações se encontram no estado similar ao estado liquefeito da matéria, flexíveis e voláteis, podendo dispensar na maioria das vezes a “liga” necessária para manter as partes do sólido unidas.

Através do aforismo 354, Nietzsche em sua obra “A Gaia Ciência” menciona

que a consciência humana se desenvolveu sob a pressão da necessidade de comunicação. Consciência, portanto, seria uma rede de ligação entre homens. Deste modo, a partir do momento que o indivíduo produz ferramentas para evoluir a própria interação, expande inclusive, sua própria consciência. Segundo o autor:

> A consciência desenvolveu-se apenas sob a pressão da necessidade de comunicação – de que, desde o início foi necessária e útil apenas entre uma pessoa e outra (entre a que comanda e a que obedece, em especial), e também se desenvolveu apenas em proporção ao grau dessa utilidade. Consciência é, na realidade, apenas uma rede de ligação entre as pessoas – apenas como tal ela teve que se desenvolver: um ser solitário e predatório não necessitaria dela (Nietzsche, 2001, p. 36).

Por meio da expansão da Internet, os indivíduos deslancharam não apenas a comunicação, mas se tornaram pessoas mais conscientes, em decorrência, sobretudo, da enxurrada de elementos informacionais resultantes desse revolucionário instrumento, mas afinal, quando surgiram as primeiras conexões que promoveram toda essa evolução?

Somente após o lançamento do primeiro satélite artificial denominado Sputnik em 1957 pela União Soviética, o então presidente dos Estados Unidos, Dwight Eisenhower, autorizou a criação da ARPA (Advanced Research Projects Agency), agência sob sua supervisão que tinha como intuito o desenvolvimento de equipamentos tecnológicos os quais pudessem proteger a nação de possíveis ataques, bem como proporcionar preponderância dos EUA diante de outros países, ora, se a URSS possuía poderio suficiente para realizar esse tipo de ação, detinha potência para atacar o território americano.

Destarte, constatou-se a necessidade da criação de uma rede mais ampla que funcionasse como uma válvula de comunicação a longo alcance e que se mantivesse estável entre militares e cientistas mesmo após um possível bombardeio. Assim, em 1969, nasceu a ARPANET (Advanced Research Projects Agency Network), considerada o “embrião da Internet”, proporcionando interação comunicativa e fomento à pesquisa científica dos meios computacionais.

Na concepção de Manuel Castells (2003, p. 214): “Como parte desse esforço, a montagem da ARPAnet foi justificada como uma maneira de permitir aos vários centros de computadores e grupos de pesquisa que trabalhavam para a agência, compartilhar on-line tempo de computação”.

No início da década de 1980, foi criado um protocolo capaz de trocar as informações da ARPAnet, denominado TCP/IP (Transmission Control Protocol/Internet Protocol), o qual tornou-se essencial para criar a ferramenta em voga. Esse dispositivo forneceu uma linguagem única utilizada pelos computadores, pois não seria produtivo manter uma conexão estável se não existisse um código definido para que o maquinário e seus comandantes interagissem de fato.

Em vista disso, no ano de 1996, eclodiu a World Wide Web, por Tim Berners-Lee, um sistema criado exclusivamente para acessar a Internet baseado em hipertextos, onde o usuário tinha acesso a: textos, imagens, sons, vídeos, etc., todos de modo interativo. De acordo com Paesani:

> O WWW nasceu no ano de 1989 no Laboratório Europeu de Física de altas energias, com sede em Genebra, sob o comando de T. Berners – Lee e R. Calliau. É composto por hipertextos, ou seja, documentos cujo texto, imagem e sons são evidenciados de forma particular e podem ser relacionados com outros documentos. Com um clique no mouse o usuário pode ter acesso aos mais variados serviços, sem necessidade de conhecer os inúmeros protocolos de acesso (Paesani, 2006, p. 11).

Em vista disso, o número de pessoas conectadas à rede aumentava desenfreadamente, e a Internet ganhou milhares de adeptos ao redor do mundo, sendo o principal instrumento destinado às práticas comuns e complexas do dia a dia. Assim, após adentrar no mundo virtual, o ser humano se manteve constantemente imerso no ciberespaço.

2.2 A EXPANSÃO DA INTERNET NO BRASIL

Diferentemente dos EUA que desenvolveu a principal ferramenta virtual com intuitos militares, a Internet no Brasil teve como o seu estopim a educação. Em 1988 a comunidade acadêmica da FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo), UFRJ (Universidade Federal do Rio de Janeiro) e o LNCC (Laboratório Nacional de Computação Científica) conectaram-se às universidades americanas, incluindo a Universidade de Maryland e o Laboratório Fermilab (Fermi National Accelerator Laboratory). Na época, utilizaram um fio de cobre dentro de um cabo submarino, gerando então uma conexão de ponta a ponta, através da rede Bitnet - (Because It's Time Network) estabelecida em 5 de maio de 1981, como rede

cooperativa entre a City University of New York (CUNY) e a Yale University.

Progressivamente, os países começaram a aderir essa ferramenta, pois se tornava cada vez mais notório que os seus benefícios eram vastíssimos. No ano de 1989, por iniciativa do Ministério da Ciência e Tecnologia (MCT), eclodiu a RNP (Rede Nacional de Pesquisa), objetivando proporcionar a ligação entre as universidades federais de pesquisa, contando com um laboratório específico para promover melhorias e aplicações relacionadas à rede, ou seja, a ampliação da Internet no Brasil já era uma realidade nessa época.

No início dos anos 90 a Internet continuou restrita à comunidade acadêmica e ao governo, no entanto, havia a necessidade de distribuí-la à população, deste modo, em 1994, a ferramenta finalmente apresentou-se acessível comercialmente, adentrando oficialmente na residência dos brasileiros.

No entanto, ainda não existia a facilidade e acessibilidade hodierna, pois a priori, utilizavam-se linhas discadas, ou seja, a conexão era realizada através da rede de telefonia, e por consequência, as faturas eram muito onerosas, logo, nem todo cidadão possuía condições de pagar para usufruir dos benefícios dessa ferramenta.

Além disso, para que não houvesse um monopólio pela Embratel - estatal na época -, foi aprovada em 1995 a Portaria nº 148, pelo Ministério das Comunicações Sérgio Motta, autorizando a privatização dos serviços de Internet. A partir de então, os brasileiros obtiveram mais liberdade e oportunidades para inserir-se no espaço cibernético e desfrutar de suas intensas e diversas vantagens.

> Não será criada tarifa especial alguma. O que o governo tem que fazer com os usuários da Internet é deixá-los em paz. Tem que oferecer serviços melhores e sair do campo, deixando o negócio para a iniciativa privada. É isso que será feito. Não vai subir tarifa nenhuma e a partir do ano que vem o serviço que a Embratel está prestando será assumido por outras empresas, em regime de concorrência (Motta, 1996, p. 1).

A chegada das redes sociais se tornou o marco na expansão do uso exacerbado da Internet no país. Fotolog, LinkedIn e MySpace, exibiam compartilhamento de imagens, busca por vagas de emprego, arquivos de áudio, entre outras atividades. No entanto, a rede social que ganhou maior notoriedade no Brasil foi sem dúvida o Orkut, criado em 2004 pelo turco Orkut Buyukkokten.

A partir de então, os brasileiros começaram a expor descontroladamente:

intimidade, privacidade, dados e informações pessoais. A problemática surge quando a maioria dos usuários não se preocupam com os riscos de inserir sua rotina e informações relevantes em um espaço virtual onde o mundo inteiro pode ter acesso instantâneo e salvá-los perpetuamente.

A cultura marcada principalmente pelas tecnologias digitais, denomina-se "*cibercultura*", abrangendo a ampliação de dados, e gerando uma fusão entre tecnologia e vida social.

> A cibercultura nada mais é do que a cultura contemporânea em sua interface com as novas tecnologias de comunicação e informação, ela está ligada às diversas influencias que estas tecnologias exercem sobre as formas de sociabilidade contemporâneas, influenciando o trabalho, a educação, o lazer, o comércio, etc. Todas as áreas da cultura contemporânea estão sendo reconfiguradas com a emergência da cibercultura (Lemos, 2003, p. 1).

Portanto, esse comportamento novo e sui generis, traz uma nova modalidade de cultura que permeia as relações sociais, promovida por diversos recursos e aplicativos característicos da cultura cibernética.

2.3 INTERNET COMO FERRAMENTA PARA PRÁTICAS ILÍCITAS

A Internet passou a ser utilizada não apenas como uma ferramenta propulsora de benefícios, mas também se tornou um instrumento de dependência na vida dos usuários. É fácil perceber o quão o homem está indissociável à tecnologia, basta observar sua rotina, onde boa parte se passa nos meios eletrônicos.

> Com o aparecimento da Internet como um novo instrumento de comunicação e o seu acesso cada vez mais presente em todas as classes sociais, profissionais e faixas etárias, relatos de comportamentos patológicos de dependência da Internet constituem temas frequentes da literatura médica atual e também, com grande destaque, na mídia popular (Razzouk, 1998, p. 1).

Assim, por não ser um ambiente limitado, sua dimensão torna o local propenso a inúmeras práticas criminosas, por isso, a dependência humana no uso dos meios tecnológico fornecem ainda mais oportunidades para os agentes criminosos. Apesar disso, não estamos diante de uma terra sem lei, mas um

verdadeiro desafio para o direito brasileiro, sobretudo no que tange à materialidade do delito. O crime online está fora de controle e a maioria dos usuários não estão preparados para lidar com as possíveis ameaças, navegando na Internet sem qualquer prevenção.

O agente criminoso pode se inserir de diversas maneiras quando se trata do meio digital, diferentemente das práticas ocorridas no mundo físico. Invadir sistemas através de vírus, captar e roubar dados pessoais, apresentar falsidade ideológica e ter acesso a informações confidenciais, são apenas alguns dos inúmeros delitos desenvolvidos no espaço cibernético.

Além disso, está cada vez mais difícil traçar o perfil de um criminoso na Internet, pois não se sabe precisamente como o delito foi arquitetado em virtude das diversas possibilidades que o agente possui de se ocultar através do anonimato, e por consequência, lograr impunidade.

Destarte, a facilidade para o cometimento de delitos é tão expansiva que mesmo se o indivíduo não for um agente criminoso na vida real e perceber a inclinação de se camuflar no mundo virtual, acaba por se sentir mais seguro para praticar o fato transgressor.

> A Internet pode ser usada para diversos benefícios, no entanto também pode ser usada como um território atraente para criminosos, isto porque atribui uma espécie de conhecimento minucioso sobre seu funcionamento, “a internet é vista, por muitos, como um caos organizado ou um caos que funciona. Tudo pode se ligar a tudo, com um clicar do mouse” (COSTA, 1998, p. 17).

A Internet fez com que qualquer pessoa pudesse ser um criminoso digital em potencial. Além disso, é importante ressaltar que tais delitos não recaem apenas ao cidadão comum, mas também ao Estado, podendo ocasionar grandes prejuízos para toda nação.

2.4 O LADO OBSCURO SOBRE O AVANÇO DAS REDES SOCIAIS

Nas redes sociais, os usuários estão propensos à exposição constante de sua vida diária, exibindo dados inteiramente pessoais, como: fotos de família, bens particulares ou até mesmo bancários. Assim, a probabilidade de o agente criminoso monitorar suas possíveis vítimas se tornou mais simples e acessível, visto que a

privacidade do sujeito passivo se transmutou em domínio público. Conforme assevera o livro Geração Interativa sobre a rede social Orkut:

> Essa febre trouxe consigo uma série de problemas. Como é amplamente sabido que a rede é muito usada por crianças e adolescentes, o Okurt, como outras redes sociais, converteu-se em um território altamente visado pelos pedófilos. De acordo com a ONG Safernet, 90% das denúncias de pedofilia no Brasil tinham relação com o Orkut (Chalezquer; Sala, 2009, p. 253).

Destarte, entende-se que produção de aplicativos e ferramentas virtuais sem uma evidente fiscalização ou normatização, torna o ambiente virtual cada vez mais independente e irregular, pois as problemáticas existem, mas as medidas para sanar esses impactos ainda são morosas e tardias, o que não deveria ocorrer em um mundo digital e globalizado.

As redes sociais transformaram-se não apenas em um ambiente de entretenimento diário, mas também em um território de vários ataques delituosos conforme supracitado, em decorrência de inúmeros fatores, dentre eles a facilidade do agente em se ocultar no ciberespaço através do anonimato.

> Tais crimes aumentaram muito, devido à facilidade encontrada para praticá-lo, onde muitas informações pessoais estão disponíveis na rede. Assim, os criminosos coletam dados e informações privilegiadas para extorquir ou simplesmente prejudicar o outro, causando prejuízos moral e financeiro. (Deslandes; Arantes, 2017, p. 175).

Na sociedade moderna, o indivíduo é incentivado pelas mídias sociais a passar boa parte do seu tempo exibindo-se de modo incessante na web, desde o momento que acorda até a hora de dormir, possuindo a ideia de que quanto maior o número de seguidores, melhor será sua visibilidade e importância na sociedade, no entanto, não se trata apenas do mero compartilhamento de sua rotina, o ser humano está perdendo inclusive sua própria essência em busca de aceitação.

Quanto maior for a frequência de uso, maior será a probabilidade de vício. Os utilizadores com uma frequência alta de utilização da internet têm um perfil que inclui as seguintes variáveis psicossociais: a tendência à introversão; sentimentos de incapacidade para se relacionarem com os outros; relações sociais incômodas; a procura de reforços sociais sem necessidade de contato real.

Em vista disso, termos como: “stalking”, “sexting”, “cyberbullying”, “oversharing”, são apenas alguns exemplos de práticas realizadas pelos próprios internautas as quais envolvem perseguição e exposição excessiva não apenas de seus dados pessoais, mas inclusive conteúdos íntimos.

Deste modo, os cibercriminosos obtém facilmente o conhecimento das vulnerabilidades oferecidas pelos próprios usuários, pois no espaço cibernético é muito comum a presença de perfis falsos para realização desse tipo de conduta.

> Como as redes sociais na Internet ampliaram as possibilidades de conexões, ampliaram também a capacidade de difusão de informações que esses grupos tinham. No espaço off-line, uma notícia ou informação só se propaga na rede através das conversas entre as pessoas. Nas redes sociais online, essas informações são muito mais amplificadas, reverberadas, discutidas e repassadas (Recuero, 2009, p. 25).

Sendo assim, a facilidade do fornecimento de informações por parte da própria vítima, corrobora para uma eficiente abordagem do agente delituoso nas relações cibernéticas, bem como a introdução do *iter criminis*, visto que, ao ter conhecimento dos gostos e peculiaridades da vítima, é possível traçar um perfil próprio em comum, a saber:

> As redes sociais ultrapassaram o âmbito acadêmico/científico, conquistando e ganhando espaço em outras esferas. E podemos observar esse movimento chegando à Internet e conquistando cada vez mais adeptos, aglutinando pessoas com objetivos específicos, ou apenas pelo prazer de trazer à tona ou desenvolver uma rede de relacionamentos (...). Enfim, são ambientes que possibilitam a formação de grupos de interesses que interagem por meio de relacionamentos comuns (Tomaél; Alcara; Di Chiara, 2005, p. 96-97).

Contudo, por mais que as redes sociais possam aparentar ser um grande ambiente lúdico e de grandes distrações, tornam-se um entorno gerador de delitos em grande escala, decorrentes principalmente do mau uso da Internet e das redes sociais, portanto, navegar no espaço virtual passou a ser um ambiente inseguro e arriscado àqueles que não tomam quaisquer medidas preventivas para conter tais ataques.

3 OS CRIMES CIBERNÉTICOS

Os proveitos oriundos da era digital são notórios, a sociedade continua transformando o seu modo de viver, pensar e agir, impactando assim, no desenvolvimento mundial e em diversas esferas, seja: sociais, culturais, políticas ou econômicas. Todavia, a geração de dados em demasia ocasiona um descontrole no ciberespaço, acarretando assim, vulnerabilidades excedentes conforme exposto no capítulo anterior.

> A habilidade ou inabilidade de uma sociedade dominar a tecnologia ou incorporar-se às transformações das sociedades, fazer uso e decidir seu potencial tecnológico, remodela a sociedade em ritmo acelerado e traça a história e o destino social dessas sociedades; remetendo que essas modificações não ocorrem de forma igual e total em todos os lugares, ao mesmo tempo e instantânea a toda realidade, mas sim é um processo temporal e para alguns, demorado (Castells, 1999. p. 76).

Percebe-se que, a sociedade unida à tecnologia produz uma união poderosa, principalmente no que diz respeito às influências, criando uma cultura própria. Contudo, a tecnologia em si não é determinante, mas condicionante das transformações sociais. Uma das maiores consequências geradas após a eclosão do espaço cibernético, foi a modificação do estilo de vida dos indivíduos, tornando a sociedade cada vez mais célere, promovendo impactos em todas as esferas, assim, o sistema jurídico percebeu a necessidade de atualizar a legislação vigente para de fato assegurar a tutela dos bens de acordo com a nova realidade.

3.1 O CONCEITO DE CRIME CIBERNÉTICO

Antes de adentrar no conceito de crime cibernético, é importante analisar o crime por três aspectos: material, formal e analítico. O conceito material está ligado ao Código Penal e norteia o legislador a um critério político-criminal, sobre o que deve ou não punir.

“É a concepção da sociedade sobre o que pode e deve ser proibido, mediante a aplicação de sanção penal. É, pois, a conduta que ofende um bem juridicamente tutelado, merecedora de pena” (Nucci, 2009, p. 166).

Destarte, o crime formal, segundo Nucci: “É a concepção do direito acerca do delito, constituindo a conduta proibida por lei, sob ameaça de aplicação de pena, numa visão legislativa do fenômeno” (Nucci, 2009, p. 167). Por fim, segundo as palavras do referente autor sobre o conceito de crime analítico:

> Trata-se de uma conduta típica, antijurídica e culpável, vale dizer, uma ação ou omissão ajustada a um modelo legal de conduta proibida (tipicidade), contrária ao direito (antijuridicidade) e sujeita a um juízo de reprovação social incidente sobre o fato e seu autor, desde que existam imputabilidade, consciência potencial de ilicitude e exigibilidade e possibilidade de agir conforme o direito. Justamente quanto ao conceito analítico é que se podem encontrar as maiores divergências doutrinárias (Nucci, 2007, p. 160).

Percebe-se que este último conceito se assemelha ao segundo, mas de uma forma fragmentada em elementos que promovam uma concepção mais inteligível, logo, não se diferem em sua essência, a partir de então, analisar-se-á de modo breve os conceitos gerais referentes aos crimes virtuais.

O crime cibernético possui múltiplas denominações, entre suas variantes: crimes eletrônicos, cibercrimes, crimes virtuais, delitos informáticos, entre outros. Trata-se de condutas ilícitas onde o agente, através dos meios computacionais, digitais, dispositivos informáticos, etc., utilizando-se dos meios tecnológicos para atingir diretamente ou indiretamente os bens jurídicos. É possível compreender melhor este conceito através de Augusto Rossini:

> 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 (Rossini, 2004, p. 110).

Os delitos virtuais abrangem também os demais crimes e contravenções penais, logo, não se restringem às práticas ilícitas do ciberespaço, mas toda e qualquer ação relacionada aos sistemas informáticos, onde os meios digitais, neste caso, são simples ferramentas, as quais não necessitam obrigatoriedade de conexão com a Internet.

A evolução cibernética se tornou tão expansiva e incontrolável que hoje não se fala somente em desigualdade social ou privilégios de possuir um dispositivo

informático, mas sim do surgimento de novos tipos penais, além disso, o agente criminoso também se vale desse meio para fomentar delitos pré-existentes.

> É inegável o prejuízo que pode ser provocado por esse tipo de ferramenta, sendo possível, de uma determinada localidade, acessar um sistema de computadores situado do outro lado do mundo e manipular seus dados, tornando-se crimes “limpos”, que não deixam quaisquer rastros (Rosa, 2005, p. 23).

Ademais, o conceito de crime cibernético também é abordado por Castro:

> Aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador. Inclui-se neste conceito os delitos praticados através da internet, pois pressuposto para acessar a rede é a utilização de um computador (Castro, 2001, p. 9).

As condutas delituosas eclodidas a partir dos crimes cibernéticos revelam também uma nova intimidação, visto que conceitos mais tradicionais relacionados às jurisprudências, competências e soberanias, necessitam de interpretações sob a ótica atual, decorrentes dessas novas relações de criminalidade.

3.2 AS CARACTERÍSTICAS DOS CRIMES CIBERNÉTICOS

Existem aspectos e características comuns em relação aos cibercrimes, deste modo, faz-se necessário conhecer alguns atributos para compreender não apenas o fato jurídico propriamente dito, mas se resguardar de possíveis ameaças. Um dos pontos que mais chamam a atenção nesse ambiente é a possibilidade de obter e manter o anonimato, o agente criminoso possui interação livre e ilimitada com a comunidade virtual, padrão que muitas vezes não seria aceitável no mundo físico, principalmente partindo de indivíduos desconhecidos.

> Os crimes virtuais mais recorrentes do mundo digital são velhos conhecidos dos ordenamentos jurídicos, tais como crimes contra a honra, discriminação, ameaça, fraude, falsidade ideológica entre outros, sendo que, agora, existem mais ocorrências dos mesmos. No caso da internet a possibilidade do anonimato estimula o descumprimento de regras, pois gera maior certeza de impunidade (Pinheiro, 2014, p. 33-44).

Em vista disso, existe uma grande dificuldade em identificar o agente criminoso para determinar a autoria do delito, bem como encontrar sua respectiva materialidade, visto que os dados e informações dispostos nesse ambiente são demasiadamente voláteis, perdendo-se em apenas um comando. Além disso, possuem inúmeros formatos advindos das diárias inovações tecnológicas, o que demanda uma análise mais cautelosa de profissionais qualificados que promovam a excelência na persecução penal.

Outra característica marcante desse tipo de delito, é a transnacionalidade, não importa a cidade, estado ou país, o agente criminoso poderá praticar o ilícito contra qualquer pessoa conectada ou não à rede mundial de computadores, assim, quanto maior a habilidade técnica de quem pratica a conduta, mais fácil será burlar os meios digitais e legais. Cruz desenvolve o conceito de como:

> Emergência de novos espaços públicos plurais, solidários, cooperativamente democráticos, livres das amarras ideológicas da modernidade, decorrentes da intensificação da complexidade das relações globais, com capacidade jurídica de governança, regulação, intervenção – e coerção – com o objetivo de projetar a construção de um novo pacto de civilização (Cruz, 2009, p. 6).

Neste mesmo sentido, é o entendimento de Fiorillo, a saber:

> A criminalidade informática traz como uma de suas principais características a informatização global, sendo a mais relevante delas a transnacionalidade uma vez que praticamente todos os países, hoje, tem acesso ou fazem uso da informática, de maneira que possível praticar um ilícito penal a partir de qualquer lugar da denominada sociedade global (Fiorillo; Conte, 2016, p. 5).

Além disso, o anonimato é uma das principais barreiras encontradas pelos legisladores para detectar o sujeito ativo, conforme supracitado, desta forma, o mesmo torna-se apto a destilar ódio, ofensas e ferir, inclusive, a dignidade da pessoa humana através de perfis falsos na esfera cibernética.

> Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da Internet são denominados de crimes virtuais, devido à ausência de seus autores e seus asseclas (Terceiro, 2009, p. 2).

Considerando tais características, podemos perceber que a inserção de um cibercriminoso dar-se-á por diversas vias, sejam detectáveis tecnologicamente ou não.

> A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução (Ferreira, 2011, p. 25).

Logo, o acesso às variadas informações as quais perpetuam na imensidão do campo cibernético, desperta o interesse dos agentes criminosos que vislumbram nesse tipo de ambiente um alcance de benefícios de modo demasiadamente instantâneo, decorrente das mais variadas novidades tecnológicas que se tornam aliadas ao agente delituoso.

3.3 A CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Greco Filho traz uma excelente observação acerca da classificação dos cibercrimes, a saber:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados 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 crimes de resultado de 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 conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou (Greco, 2000, p. 3).

Sendo assim, a classificação mais adequada a atual realidade é a que os crimes cibernéticos podem ser próprios ou impróprios.

3.3.1. Crimes cibernéticos próprios ou puros

O crime cibernético próprio é aquele que necessita do meio computacional para que haja a execução do delito. São condutas voltadas contra os sistemas informáticos e por consequência seus dados e informações, sem o qual resta o crime impossível.

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado (Damásio, 2003, p. 24).

Malaquias fortifica o conceito da seguinte maneira:

> Crime cibernético próprio: é aquele que necessita do espaço virtual para ser praticado, ou seja, está diretamente relacionado com a utilização da tecnologia da informação e comunicação. Para facilitar a compreensão, têm-se como exemplos enquadrados neste grupo, a criação e disseminação de vírus e outros códigos maliciosos, a negação de serviços, a invasão e a destruição de bancos de dados (público ou privado) e tantos outros atos ilícitos (Malaquias, 2015, p. 55).

Representam exemplos de crime cibernético próprio o crime de “invasão de dispositivo informático”, disposto no art. 154-A do Código Penal, exclusivamente cibernético, onde o agente se vale do aparato eletrônico para exercer o ilícito, deste modo, conforme o artigo supracitado é crime:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (Brasil, 2012, art. 154-A).

Outro exemplo é a disseminação de vírus, ocasionando inúmeras vulnerabilidades de acordo com o interesse do infrator, conforme observado no § 1º, do referido artigo. “Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput” (Brasil, 2012).

Desta maneira, o crime cibernético próprio se caracteriza, principalmente, quando o sujeito ativo invade o sistema de outrem para consumar o delito, seja por meio de software, hardware ou armazenamento de dados e informações, ademais,

esse tipo de delito consumar-se-á na esfera virtual, não produzindo efeitos fora desse âmbito.

3.3.2 Crimes cibernéticos impróprios ou mistos

Os crimes cibernéticos impróprios são mais amplos, pois não se limitam exclusivamente a utilizar o aparato computacional ou apenas dispositivos específicos, estes, tornam-se instrumentos para a prática delituosa, ou seja, tais delitos se voltam contra os bens jurídicos em geral, de modo que sua tipificação já se encontra ordenada no Código Penal Brasileiro. Conforme expõe Damásio de Jesus:

> Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática. (Damásio, 2003, p. 25).

É necessário ressaltarmos que essa classificação serve para abordamos de modo mais didático a temática, pois não há um padrão fixo em decorrência do dinamismo e volatilidade desse tipo de delito, é impossível acompanhar e/ou categorizar detalhadamente os cibercrimes, visto que são passíveis de inúmeras modalidades e mudanças.

Um exemplo de crime cibernético impróprio é o crime de pornografia infantojuvenil com utilização da Internet, disposto no art. 241 da Lei Nº 8.069/90, do Estatuto da Criança e do Adolescente (ECA). Conforme o texto legal:

> Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (Brasil, 1990).

Nesse caso, segundo o entendimento do Supremo Tribunal de Justiça, existem duas situações possíveis: a divulgação de fotos, vídeos ou arquivos nas redes sociais, mesmo que apenas pessoas próximas tenham acesso, assim, a competência será da Justiça Federal, pois em decorrência da transnacionalidade proporcionada pelo meio digital, tais arquivos estarão disponíveis para o mundo

inteiro. A segunda hipótese é a troca de e-mails entre pessoas no Brasil com esse tipo de conteúdo, restará, portanto, a competência da Justiça Estadual. Além disso, em relação ao local da infração, prevalecerá o local da publicação.

> Pode-se dividir os crimes virtuais como próprios ou impróprios. Os primeiros, são aquelas condutas antijurídicas e culpáveis que visam atingir um sistema informático ou seus dados violando sua confiabilidade, sua integridade e/ou sua disponibilidade. Já os segundos, são condutas comuns – típicas, antijurídicas e culpáveis – que são perpetradas utilizando-se de mecanismos informáticos como ferramenta, mas que poderiam ter sido praticadas por outros meios (Sydow, 2014, p. 75).

Apesar dos diversos benefícios gerados pelo meio virtual, estamos diante de sistemas capazes de coagir e coibir do mesmo modo que um explosivo ou arma de fogo, ou seja, ferramentas que agilizam o comedimento da prática ilícita. Portanto, é dever do Estado regulamentar essas novas modalidades, para que promova verdadeiramente a tutela jurisdicional.

3.4 OS SUJEITOS DO CRIME CIBERNÉTICO

Conforme abordado anteriormente, não é fácil identificarmos os sujeitos do delito na esfera virtual, principalmente devido à ausência física do ciberespaço, onde o agente criminoso desenvolve uma confiança muito maior em suas práticas delituosas, executando-as através do anonimato.

Porém, é possível traçar um molde ou padronizar certos indivíduos que possuem determinadas condutas assíduas. Além disso, existem diversas denominações destinadas àqueles que praticam delitos nesse âmbito, por isso, realizar-se-á uma abordagem mais básica para compreender as características dos respectivos sujeitos dos crimes cibernéticos.

O agente criminoso responsável por praticar o crime propriamente dito é o chamado sujeito ativo, no caso dos crimes virtuais, eles são chamados também de “*crackers*”, do verbo em inglês “to crack”, que significa “quebrar códigos de segurança”. Assim, com um alto grau de conhecimento e nenhuma ética, os crackers invadem sistemas e podem apenas deixar a sua marca ou destruí-los completamente.

> Sujeito ativo do crime é aquele que pratica a conduta descrita na lei, ou seja, o fato típico. Só o homem, isoladamente ou associado a outros (co-autoria ou participação), pode ser sujeito ativo do crime, embora na Antiguidade e na Idade Média ocorressem muitos processos contra animais. A capacidade geral para praticar crime existe em todos os homens, é toda pessoa natural independente da sua idade ou de seu estado psíquico, portanto também os doentes mentais (Mirabete, 2008, p. 110).

Além disso, Almeida ratifica que os crimes virtuais: “são aqueles em que o sujeito ativo utiliza o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime” (Almeida, 2015, p. 224). Por se tratar de um crime comum, o sujeito ativo pode ser qualquer pessoa que realize os elementos do tipo.

Desafia a legislação atual as dificuldades que têm os órgãos judiciais e investigativos em identificar os sujeitos ativos dos crimes virtuais, o que se deve às nuances tecnológicas que facilitam a fuga e ocultação da autoria, ademais, isso ocorre em razão do “grande número de usuários dessa nova tecnologia e a possibilidade de colocar informações inverídicas sobre seu endereço de IP”. (Siqueira, 2017, p. 122).

Sendo assim, nota-se que a possibilidade de realizar condutas de modo desconhecido, faz com que o agente ativo se transmute em uma incógnita para o investigador, gerando empecilhos na fase pré-processual da persecução penal.

“Seria possível a identificação do criminoso obtendo o seu endereço de IP, login e senha do aparelho utilizado para a prática do crime, porém, os criminosos utilizam endereços falsos, dificultando o trabalho investigativo dos policiais” (Siqueira, 2017, p. 122).

Em vista disso, ordenamento jurídico brasileiro já busca conter os excedentes advindos do anonimato virtual, conforme a seguinte jurisprudência:

> AGRAVO DE INSTRUMENTO. LIBERDADE DE MANIFESTAÇÃO DE PENSAMENTO. LIMITES. VEDAÇÃO AO ANONIMATO. I – A liberdade de manifestação do pensamento constitui um dos fundamentos essenciais de uma sociedade democrática, mas o seu exercício deve ocorrer de forma responsável, não se admitindo o anonimato e a violação de direitos fundamentais da pessoa humana. II – Os provedores devem manter os dados mínimos à identificação eficaz de seus usuários, coibindo o anonimato. III – Deu-se provimento ao recurso. (TJ-DF - AGI: 20150020058545, Relator: JOSÉ DIVINO DE OLIVEIRA, Data de Julgamento: 29/04/2015, 6ª Turma Cível, Data de Publicação: Publicado no DJE: 12/05/2015. p. 368).

Depreende-se, portanto, que os ditames referentes ao espaço cibernético, devem se pautar na congruência dos direitos e garantias fundamentais, visando deste modo, assegurar os bens jurídicos dos cidadãos, tal como: liberdade de expressão, intimidade e privacidade.

O sujeito passivo é aquele sobre o qual recaiu a ação ou omissão do agente, sendo pessoa física ou até mesmo jurídica, ou seja, o titular do bem lesado. Mirabete (2008, p. 114) destaca que o sujeito passivo pode ser uma ou mais vítimas. Segundo estabelecido no artigo 147 do Código Penal: “ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave”, conduta comum realizada no meio virtual.

Contudo, ocorre que, atualmente muitos delitos que foram praticados no ciberespaço não são divulgados ou denunciados, o que acaba por ocasionar ainda mais a propagação dessas transgressões.

Ademais, o sujeito passivo do crime cibernético pode ser a pessoa física ou jurídica que tem a propriedade do dispositivo informático lesionada. Segundo Cabette, o sujeito passivo é “qualquer pessoa que tenha sua privacidade violada pelo invasor é sujeito passivo da infração” (Cabette, 2013, p. 1). Assim, o sujeito passivo é também aquele que sofre a instalação indevida de várias vulnerabilidades em seu disposto para que o sujeito ativo obtenha vantagens ilícitas.

3.5 JURISDIÇÃO E COMPETÊNCIA

Visto que os crimes cibernéticos se caracterizam por sua transnacionalidade, torna-se relevante destacar quais são as respectivas competências responsáveis para processar e julgar os crimes virtuais.

A competência diz respeito à parcela da jurisdição indicadora do âmbito geográfico o qual o juiz irá atuar, bem como da matéria e das pessoas, portanto, não se restringe ao território, mas abrange também a função. Conforme preceitua Aury Lopes Júnior: “A competência é um conjunto de regras que asseguram a eficácia da garantia da jurisdição e, especialmente, do juiz natural. Delimitando a jurisdição, condiciona seu exercício.” (Lopes Jr., 2011, p. 423).

O Direito Penal Brasileiro, através de seu art. 6º, adota a Teoria da Ubiquidade, segundo a qual: “Considera-se praticado o crime no lugar em que

ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado" (BRASIL, 1940, art. 6º). Sendo assim, o legislador amplia a percepção de lugar do crime para inserir tanto aquele que se verifica a conduta delituosa, como o resultado naturalístico – nos crimes os quais são exigidos -, inclusive o bem jurídico violado.

Ademais, essa teoria também é adotada pelo Direito Penal Militar, conforme disposto no seguinte julgado:

> ESTELIONATO - COMPETÊNCIA - LUGAR DO CRIME - TEORIA DA UBIQUIDADE – CONCORRENDO DOIS OU MAIS JUÍZES IGUALMENTE COMPETENTES - REGRA DA PREVENÇÃO. Atividade delituosa iniciou-se em Brasília (11ª CJM), com a emissão e apresentação da declaração tida como falsa. Resultado ocorreu no Rio de Janeiro (1ª CJM), quando do recebimento do valor pecuniário. IPM instaurado em Manaus (12ª CJM), por ter o indiciado declarado ir residir em Tabatinga-AM. Art. 6° do CPM. Lugar do crime. Teoria da ubiquidade, considerando tanto o crime praticado no lugar onde se desenvolveu a atividade criminosa, como também onde se produziu ou deveria produzir o resultado. Art. 88, do CPPM, competência determinada pelo lugar da infração. Diferença ante o art. 70 do CPP - Competência pelo lugar em que se consumar a infração - Teoria do resultado. Regra para dirimir aparente impasse: Prevenção. Auditoria da 11ª CJM praticou atos que previnem o referido Juízo. Provimento negado ao Recurso - Competente para conhecer o presente processo - Juízo da 11ª CJM, em Brasília. Decisão por maioria. (STM, 1999).

Os crimes virtuais configuram-se também como crime à distância, em decorrência das dificuldades apresentadas na aplicação da lei penal no espaço e delimitações de competência para o julgamento da ação penal, pois ocorrerá fatos os quais envolverão territórios diversos onde os provedores são instalados. O ilustre professor Flúvio Cardinelle, classifica os crimes à distância como aqueles em que os atos executórios e a consumação ocorrem em territórios distintos, cada qual sujeito à jurisdição de um Estado soberano diferente. (GARCIA, 2007, p.176). Deste modo, a consumação do delito pode ocorrer em mais de um país, de forma que o *iter criminis* ultrapassa o espaço geográfico nacional.

Conforme o Acórdão do Recurso Extraordinário nº 628.624 do Estado de Minas Gerais, mesmo que a conduta tenha origem no estrangeiro, a competência de instrução e julgamento será da Justiça Federal caso possua os seguintes requisitos:

> À luz do preconizado no art. 109, V, da CF, a competência para processamento e julgamento de crime será da Justiça Federal quando preenchidos 03 (três) requisitos essenciais e cumulativos, quais sejam, que:

> a) o fato esteja previsto como crime no Brasil e no estrangeiro; b) o Brasil seja signatário de convenção ou tratado internacional por meio do qual assume o compromisso de reprimir criminalmente aquela espécie delitiva; e c) a conduta tenha ao menos se iniciado no Brasil e o resultado tenha ocorrido, ou devesse ter ocorrido no exterior, ou reciprocamente (STF, 2016).

Um exemplo comum ocorre quando alguma publicação de fotos ou vídeos em determinadas plataformas como Facebook ou Instagram, por exemplo, mesmo que seja restringido a pessoas próximas, será de competência da Justiça Federal visto que foi atendido o requisito da transnacionalidade, conforme o art. 109, inciso IX da Constituição Federal c/c o art. 88 do Código de Processo Penal.

Nos casos em que há trocas no âmbito nacional, a competência será da Justiça Estadual, e no que tange ao local da infração, será considerado o local da publicação.

Em relação aos crimes tentados e consumados, os tribunais superiores entendem que em regra, a competência está disposta no art. 70 do Código de Processo Penal, sendo o foro competente o local da consumação, no caso dos delitos virtuais, o local onde se encontra o provedor, quando o crime ocorrer dentro do Estado e não atingir bens da União.

3.5.1 Aplicação da Lei Penal e Processual no Espaço

A lei penal no espaço se encarrega de analisar o lugar onde o crime é praticado, sobretudo nos casos em que a execução se inicial em um determinado local e a consumação se perfaz em outro. O território que abrange a esfera cibernética excede as limitações da vida real, apresentando uma nova ideia, a qual emerge em forma de rede.

> O ciberespaço não dispõe de fronteiras territoriais, mas de normas ou técnicas, que regulam sistemas de acesso e que não pertencem ao mundo jurídico. Assim, não vigora o conceito de soberania e nem de competência territorial (Moles, 2000, p. 25-26).

Pode ocorrer do agente criminoso invadir um sistema informático localizado no Brasil com provedor americano, promovendo prejuízos na França, por exemplo. Assim, qual seria a competência responsável por julgar esse delito? Gabriel Cesar

Zaccaria Inellas, disserta sobre a referida problemática da seguinte maneira: “Como a Rede da Internet é mundial e sem fronteiras e sem donos, torna-se quase impossível para qualquer país, aplicar e executar leis, para regular o denominado ciberespaço” (Inellas, 2004, p. 79).

Apesar de existirem fontes contemporâneas que visam promover soberania nacional em favor de uma conjuntura internacional que produza documentos os quais fomentem a globalização, essas iniciativas na prática não são eficazes quando se trata de aplicabilidade do Direito Penal e Processo Penal no âmbito da cibercriminalidade, sobretudo em decorrência de seu cunho subsidiário. Portanto, se trata de um tema complexo o qual requer uma análise mais cautelosa por parte dos profissionais e operadores do Direito.

Conforme supracitado, o Código Penal trata do lugar do crime através da Teoria da Ubiquidade. Não há consenso entre os doutrinadores sobre a real efetividade e suficiência da aplicação dos arts. 5º e 6º do Código Penal para esse tipo de transtorno. Em vista disso, compreende que a localidade do agente seria a melhor opção para determinar a jurisdição mais adequada, mas não se trata de um entendimento pacífico, aliás, não existe quiçá aceitação internacional.

Assim, em contrapartida Gabriel César Zaccaria de Inellas (2004, p. 79), aborda que o art. 6º do Código Penal deve ser aplicado, sem prejuízos as regras ou tratados internacionais, logo, os crimes cometidos fora do território nacional, poderiam receber sanções neste âmbito, contanto que esteja previsto nos Acordos Internacionais os quais o país faz parte.

É importante destacar que, se os atos preparatórios ocorrerem no Brasil intentando uma execução em nação estrangeira, o agente não será atingido pela lei pátria, a qual aplica penalidades aos atos executórios, por isso existe uma grande dificuldade sobre a fragmentação do *iter criminis* no meio virtual, pois em decorrência dessas nuances, surgem obstáculos na punição do sujeito ativo do crime.

Por isso os tratados e convenções internacionais exclusivos e destinados a nortear os crimes cibernéticos se tornam tão relevantes, pois apontam parâmetros os quais visam evitar as problemáticas e divergências entre os países em relação à jurisdição do delito, gerando uma regulamentação mais evidente e prevenindo para

que crimes com consequências devastadoras se tornem impunes devido à falta de consenso entre governos e nações.

3.6 PRINCÍPIOS RELATIVOS AOS CRIMES CIBERNÉTICOS

Tendo em vista que a sociedade da informação está constantemente ligada aos meios digitais, os crimes cibernéticos surgem diariamente e consequentemente, novos delitos, bem como a necessidade de proteção aos bens jurídicos. Logo, há um impacto da sociedade da informação na ordem constitucional, o que gera consequências na esfera penal (Monteiro Neto, 2008, p. 6; Oliveira, 2013, p. 11).

De acordo com o art. 5º da Carta Magna, o direito à informação está intrinsicamente ligado à liberdade, conforme os seguintes incisos (Brasil, 1988):

> Art. 5 – Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> IV – é livre a manifestação de pensamento, sendo vedado o anonimato;
> V – é assegurado o direito de resposta, proporcional ao agravo, além de indenização por dano material, moral ou à imagem;
> IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
> XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício ao exercício profissional;
> XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade de do Estado;
> LXXII – conceder-se-á habeas data:
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constante de registros ou banco de dados de entidades governamentais ou de caráter público;
> b) para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo (BRASIL, 1988).

Ademais, todas essas atribuições conectam-se também à liberdade informática. Conforme assevera Paesani (2006, p. 21): “A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição”.

Além disso, a Lei Suprema dispõe de princípios responsáveis por nortear o Estado Democrático Brasileiro, sendo assim, se torna interessante abordar os princípios constitucionais-penais, que afetam diretamente na produção dos tipos penais que visam frear os cibercrimes.

3.6.1 Princípio da Legalidade

De acordo com o art. 5º, inciso XXXIX da Constituição Federal, o princípio da legalidade determina que: “Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.” Assim, essa vertente constitui uma efetiva limitação ao poder punitivo estatal.

Depreende-se que não há qualquer crime cibernético sem lei que os definam ou penas sem prévia cominação legal. Ademais, o Código Penal eclodiu no ano de 1940, em um marco temporal onde o espaço cibernético ainda não existia, por isso, subsiste a necessidade de produzir normas específicas as quais possam evitar o uso de analogias em decisões e penalidades.

> Pelo princípio da legalidade alguém só pode ser punido se, anteriormente ao fato por ele praticado, existir uma lei que o considere crime. Ainda que o fato seja imoral, antissocial ou danoso, não haverá possibilidade de se punir o autor, sendo irrelevante a circunstância de entrar em vigor, posteriormente, uma lei que o preveja como crime (Mirabete, 2008, p. 39).

Deste modo, caso não haja legislações exclusivas relacionadas aos crimes virtuais, o agente criminoso encontra um espaço repleto de atipicidade jurídica, e o poder Estatal perde seu caráter intimidativo inerente à legislação penal. Ressalta-se que, não haverá aplicação retroativa se na época do delito não havia quaisquer códigos que dispunham sobre a ilicitude, por isso a importância de promover uma visão mais rica em detalhes no que tange a produção de leis destinadas aos delitos virtuais.

> Não basta que a lei penal esteja em vigor anteriormente à prática do fato pelo agente para que possa ser efetivamente aplicada. Todos devem, ainda, ter a possibilidade de compreender exatamente o conteúdo da proibição, para que possam se comportar de acordo com a norma. Portanto, para que não seja ofensiva ao princípio da legalidade, a lei penal deve ser certa, clara, precisa e o mais simples possível, permitindo a sua mais exata compreensão (Greco, 2015, p. 25).

Além disso, conforme o acórdão julgado pelo Supremo Tribunal Federal, a saber:

> O exame da sequência cronológica ora referida permite constatar que, na data em que alegadamente cometidos, em território americano (Estado do Texas), os fatos supostamente delituosos (dezembro de 2011), a conduta do súdito estrangeiro em questão não se revestia, ainda, de tipicidade penal no âmbito do ordenamento positivo brasileiro, circunstância essa que impede a observância, no caso, do requisito da dupla tipicidade, pois – não custa relembrar – ninguém, absolutamente ninguém, pode ser incriminado por comportamento que, no momento de sua prática, a legislação penal ainda não considerava ato delituoso (CF, art. 5º, inciso XXXIX, c/c o CP, art. 1º) (STF, 2014).

Não basta a existência da lei, ela deve ser pormenorizada de modo que sua aplicação seja efetiva, pois se tornará o principal direcionamento a ser seguido pelos operadores do sistema jurídico, assim, os usuários poderão usufruir dos benefícios da Internet com mais segurança, visto que seus direitos estão assegurados no ordenamento legal brasileiro.

3.6.2 Princípio da Intervenção Mínima

A lei penal é a forma mais severa que o Estado possui para restringir determinados bens jurídicos, assim, o Direito Penal é utilizado apenas quando as demais alternativas e ramos do direito não forem suficientes para dirimir a problemática, portanto, *ultima ratio.* Essa premissa é válida também para os delitos virtuais, e o código será aplicado somente quando não existir a capacitação de outras áreas.

> É possível afirmar que o princípio da intervenção mínima, como limite do princípio constitucional da legalidade, possui três funções primordiais dentro do ordenamento jurídico: 1) estabelecer as hipóteses de incidência das leis penais; 2) indicar os limites da restrição da liberdade de ação humana, para que seja alcançada pela norma penal; e, 3) estabelecer a necessidade da incidência da consequência jurídica do delito (Lopes, 2009, p. 73).

O instrumento e voga é corolário ao princípio da subsidiariedade, bem como o princípio da fragmentariedade do Direito Penal, visto que este deve interferir minimamente na vida dos cidadãos, devido seus grandes impactos, por isso o Poder

Estatal deve se ater cautelosamente aos demais recursos para evitar desta forma, menos dano à sociedade.

3.6.3 Princípio da Territorialidade

Torna-se notório que o ambiente virtual, denominado ciberespaço não possui limitações territoriais, conforme supracitado. Desta forma, o delito cibernético pode ocorrer em qualquer lugar, ademais, essa esfera detém um caráter global, sendo um verdadeiro desafio para o Direito. Posto isto, conforme disposto no art. 5º do Código Penal, os delitos cibernéticos praticados em território nacional, serão aplicadas as leis brasileiras quando o provedor estiver neste local.

Contudo, uma exceção a este dispositivo é o princípio da extraterritorialidade, contido no artigo 7º do mesmo diploma legal. Assim, estando o agente localizado fora do país, aplica-se a lei brasileira nos casos envolvendo o referido artigo ou nos acordos e tratados nesse sentido (SOUZA NETO, 2009, p. 58-60). Por isso é necessário a adesão do Brasil em Convenções Internacionais, visando assim, evitar lacunas e fornecer segurança jurídica à população.

Além disso, as mudanças ocasionadas no meio cibernéticos já impactam diretamente as normas legais, inclusive àquelas dispostas na Carta Magna, de modo que é necessário proteger os bens jurídicos dos grandes avanços tecnológicos que impactam negativamente nas relações humanas, infringido a liberdade e até mesmo a dignidade da pessoa humana. Logo, a efetiva tutela Estatal deve estar preparada para reprimir o sujeito ativo que visa através do ilícito cibernético, lograr vantagens em desconformidade com a ordem jurídica brasileira.

3.6.4 Princípio da Lesividade

De acordo com o princípio da lesividade ou princípio da ofensividade, toda conduta que causa danos a outrem, sobretudo aos bens jurídicos tutelados, estará sujeito à órbita normativa. Conforme preconiza o axioma *nulla necessitas sine injuria,* não há necessidade de penalizar ou reprimir onde esses bens não forem ofendidos ou ameaçados.

Ademais, conforme o art. 5º da Constituição Federal: “Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e residentes no País a inviolabilidade do direito [...] à liberdade” (BRASIL, 1988). Logo, a aplicação da lei penal depende de manifestação externa e intencionada a pratica de lesionar os objetos protegidos pela esfera jurídica.

Ao cometer um crime virtual intentando ferir a liberdade, privacidade ou intimidade, por exemplo, o agente atinge os ditames dispostos na Lei Suprema, afrontando gravemente os princípios basilares de um Estado Democrático de Direito. Por isso a necessidade de elaborar atividades legislativas específicas, voltadas a punir e combater tais comportamentos lesivos.

4 LEGISLAÇÃO REGULAMENTADORA DOS CRIMES CIBERNÉTICOS

Conforme abordado no tópico supracitado, a legislação brasileira relacionada aos crimes cibernéticos ainda é muito limitada, visto que na prática, não possui alta efetividade. Ademais, desde a eclosão da Internet, o campo virtual tornou-se palco para uma série de práticas criminosas, além disso, após a adesão desta ferramenta em nosso país, não havia uma regulamentação exclusiva para esse tipo de delito.

O desenvolvimento tecnológico e o barateamento dos aparelhos eletrônicos possibilitaram um grande crescimento dos usuários na rede mundial de computadores, concomitantemente, forneceu uma grande atração àqueles dispostos a aplicar práticas criminosas. Infelizmente, o Direito não conseguiu acompanhar esse aumento exponencial, ao passo que, após o surgimento da Internet, gradativamente foi surgindo leis esparsas regulamentando pontos específicos.

Sendo assim, abordar-se-á de modo cronológico algumas leis que visam combater os crimes digitais ou pontos esparsos em crimes diversos, assim, há de se ter uma noção sobre sua real intenção e respectiva efetividade.

4.1 A CONVENÇÃO DE BUDAPESTE

Criada em 2001 pelo Conselho da Europa, Estados Unidos, Canadá, Japão e África do Sul, a Convenção de Budapeste também conhecida como Convenção contra a Criminalidade Cibernética, dispõe em seu preâmbulo ser detentora de: “uma política comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional” (Convenção de Budapeste, 2001, p. 1).

O Brasil se tornou signatário em 2020, desde então, se unindo a mais de 60 (sessenta) países, como: EUA, Argentina, Canadá, entre outros. Sendo assim, além de expandir as relações internacionais, a Convenção supre lacunas na seara criminal, fornecendo parâmetros os quais contribuem com o desenvolvimento da persecução penal aos crimes que transcendem fronteiras geográficas. “Não há fronteiras demarcadas no ambiente cibernético. Isso derruba um dos principais pilares do chamado Estado Moderno” (Medeiros, 2002, p. 147).

É importante destacar que após a eclosão do período pandêmico, o Brasil começou a ampliar os serviços digitais e promover a inclusão desses meios aos seus cidadãos, assim, os crimes cibernéticos se tornaram cada vez mais desenfreados, em decorrência do aumento do uso tecnológico e da necessidade de se adequar a essas circunstâncias.

> No que tange ao Direito da Internet, de natureza e abrangência internacionais, “os estudos dos internacionalistas devem rumar para uma análise de quais instrumentos legais poderão ser aplicados ao caso concreto e se é possível promover a adoção de princípios básicos de democracia, soberania, leis e tratados internacionais. (Vasconcelos, 2003, p. 52-53).

Posto isto, percebe-se que uma harmonização e padronização de normas internacionais a esse tipo de convenção, são imprescindíveis para que os países estejam em consonância com os preceitos legais, respeitando os princípios básicos de modo conjunto, promovendo desta maneira, uma justiça mais célere e desenvolvida.

A Convenção de Budapeste se tornou uma aliada no combate aos crimes cibernéticos, possuindo um rol específico de infrações e violações de delitos praticados nesse âmbito, essa organização facilitará na resolução dos processos relacionados aos delitos virtuais, com as seguintes temáticas, a saber:

> Hodiernamente, porém, os tipos penais presentes na Convenção são divididos em cinco modalidade: a) Infrações contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos; b) Infrações relacionadas com computadores; c) Infrações relacionadas com os conteúdos; d) Infrações respeitantes a violações do direito de autor e direitos conexos; e) atos de natureza racista e xenófoba praticados através de sistemas informáticos (Pereira, 2013, p. 145).

Assim, apesar de o Brasil ainda está engatinhando sobre a legislação digital, fazer parte de uma Convenção Internacional desse porte fornece um grande norte, bem como estrutura um arcabouço para penalizar as condutas supracitadas.

4.2 LEI Nº 11.829/08: ALTERAÇÃO NO ESTATUTO DA CRIANÇA E DO ADOLESCENTE (ECA)

No ano de 2008 a Lei nº 11.829/08 alterou o Estatuto da Criança e do

Adolescente, inserindo alguns artigos os quais intentavam combater à pornografia infantil, criminalizar a obtenção e posse desse tipo de material, além de outras condutas relacionadas à pedofilia na internet. Ademais, embora as condutas já estivessem tipificadas no Código Penal, não havia um tratamento diferenciado para os menores. Ademais, foram criados novos tipos penais, em decorrência da geração de fotos ou vídeos de crianças em cena de sexo explícito ou pornográfica.

A dimensão moderna proporcionada por essa lei está disposta no art. 241-C, o qual expõe que, ao simular a participação de criança ou adolescente em cenas de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual, implica-se deste modo, ato criminoso, com pena de 1 (um) a 3 (três) anos e multa.

> Nesse prisma, a Lei passou a alcançar não só as situações reais como também aquelas que envolvem pseudo-imagens, cartoons, desenhos animados, pinturas. As pseudo-imagens são aquelas criadas artificialmente (mediante a utilização de recursos computacionais gráficos ou qualquer outro método), que aparentam ser a reprodução fotográfica de uma criança real em situação de exploração sexual, dificultando a distinção de cenas reais.

De modo geral, a Lei nº 11.829/08, apresentou alterações bastante relevantes, visto que passou a tipificar diversas condutas até então inexistentes em nossos códigos jurídicos, preenchendo assim, as respectivas lacunas, conferindo inclusive, modernidade ao texto do Estatuto da Criança e do Adolescente (ECA), tornando-se também um marco necessário para a ampliação de um olhar mais cauteloso em relação aos crimes virtuais.

4.3 LEI Nº 12.015/09: ALTERAÇÃO NO CÓDIGO PENAL E ECA

No ano seguinte, eclodiu a Lei nº 12.015, fornecendo alterações no Código Penal e no Estatuto da Criança e do Adolescente (ECA). A relação da primeira lei com os crimes cibernéticos está na ampliação do conceito de estupro elencado no art. 213: “Constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso”. Assim, a norma traz uma interpretação muito mais ampla e difere do dispositivo anterior o qual declarava que, para existir estupro, deveria haver

conjunção carnal.

O “estupro virtual” enquadra-se nos trechos do artigo em voga, como: “constranger alguém mediante grave ameaça” e “praticar outro ato libidinoso”, entende-se, portanto, que é aquele desenvolvido para satisfazer a libidinagem de outrem. Assim, na prática, o constrangimento da vítima pode ocorrer somente por meio de ameaça, onde o agente pode intentar obter dados íntimos e particulares, por exemplo.

Ademais, torna-se essencial saber se houve ou não consentimento entre os atos praticados nesse tipo de delito, assim, pois durante o processo de investigação criminal será avaliado a interação entre o sujeito ativo e passivo, por meio dos registros localizados no IP dos dispositivos, sejam eles: fotos, vídeos, mensagens, etc.

Além disso, a lei em questão tipificou o crime de corrupção de menores no ECA, assim, aquele que realiza condutas com o a intenção de corromper ou facilitar a corrupção de menor de 18 (dezoito) anos, com ele praticando infração penal ou induzindo-o a praticá-la, através de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet, conforme o art. 244-B, §1º da referida norma legal. Ao inserir “quaisquer meios eletrônicos” o legislador refere-se às inúmeras facetas dispostas no ciberespaço, sobretudo as redes sociais, as quais são os principais meios visados pelos agentes criminosos hodiernamente.

4.4 LEI Nº 12.735/12: LEI AZEREDO

No ano de 1999 foi proposto pelo deputado Luiz Piauhylino, o primeiro Projeto que visava punir àqueles que cometiam os chamados crimes cibernéticos ou digitais. Todavia, apenas 04 (quatro) anos depois o projeto 84/99 foi aceito pela Câmara e modificado por outro deputado. Além disso, o conteúdo ainda levou muitos anos para ser analisado, em decorrência de sua alta divergência em relação à matéria.

Sendo assim, somente em 2012 foram sancionadas pela então presidente Dilma Rousseff, duas leis que tratavam dos crimes cibernéticos, tipificando condutadas executadas através do uso de sistemas eletrônicos, digitais e afins. A primeira delas foi a Lei nº 12.735/12, advinda do Projeto n. 84/99, o qual

permaneceu mais de uma década no Congresso Nacional, sendo inclusive objeto de várias críticas em relação a sua constitucionalidade. Logrou a denominação “Lei Azeredo” por ter sido iniciada pelo deputado Eduardo Azeredo, seu respectivo relator.

Na época o dispositivo recebeu demasiadas críticas, e chegou a ser apelidado de “AI-5 Digital”, fazendo alusão ao decreto emitido durante a Ditadura Militar do governo de Artur da Costa e Silva, o qual promoveu um período mais rígido no Brasil e a censura nos meios de comunicação. Para termos uma ampla noção das divergências em relação ao consenso da aprovação dessa lei, dos 23 (vinte e três) artigos presentes, apenas 04 (quatro) foram sancionados, dentre eles somente 02 (dois) possuíam conteúdo penal e os outros foram vetados pela presidente.

Além disso, a maior parte do projeto foi considerado inconstitucional, afirmam Gills Lopes Souza e Dalliana Vilar Pereira, que o mesmo criminalizava de forma generalizada, tipificando, inclusive a conduta culposa, o que diverge da Convenção de Budapeste. Assim, caso um cidadão que repassasse um vírus por e-mail, sem conhecimento ou mensagem instantânea, recairia sobre o ilícito, podendo ser punido com reclusão de 3 a 5 anos. Concordam também, que tal configuração poderia instaurar insegurança entre os cidadãos virtuais e que o referido projeto extrapola os limites da razoabilidade e proporcionalidade.

4.5 LEI Nº 12.737/12: LEI CAROLINA DIECKMANN

Posto isto, em 2011, a atriz Carolina Dieckmann teve seu dispositivo invadido por um hacker, que obteve acesso aos dados pessoais da mesma, incluindo fotos de cunho inteiramente íntimo. Por conseguinte, o agente publicou 36 imagens na web, ademais, a mesma recebeu ameaças de extorsão para que o conteúdo fosse retirado da Internet.

O caso abriu uma discussão em nível nacional sobre até que ponto os usuários teriam segurança em relação a sua privacidade digital, e de que os mecanismos de proteção de dados já não seriam suficientes para evitar possíveis invasões. Desta forma, o Direito obteve uma intensa responsabilidade: assegurar a liberdade e privacidade dos cidadãos na era digital.

No ano posterior, eclodiu a Lei nº 12.737/12, a qual detinha como principal objetivo inibir os criminosos de praticar os delitos virtuais, acrescentando os artigos 154-A e 154-B no Código Penal, elencados no rol dos delitos que atentam contra a liberdade individual. O primeiro tipo penal aborda o crime exclusivamente cibernético denominado: “invasão de dispositivo informático”, o qual será desmembrado especificamente em um capítulo mais adiante.

Assim, a entrada em vigor da referida lei, representou significativa mudança no nosso ordenamento jurídico, haja vista tratar de crimes cada vez mais constantes na hodierna sociedade, tipificando condutas que não eram previstas, de forma específica, como infrações penais (Almeida et al., 2015).

Além disso, o dispositivo alterou o crime de falsificação de documento particular, do art. 298 do Código Penal, para inserir no rol os cartões de crédito e de débito, ou seja, fato de grande relevância para a sociedade como um todo, visto que falsificar cartões na internet se tornou comum, possibilitando o surgimento de fraudes.

4.6 LEI N° 12.965/2014: MARCO CIVIL DA INTERNET

Para ter uma noção mais ampla sobre a velocidade das medidas legais elaboradas no âmbito nacional em relação aos crimes virtuais, após a criação da Internet no Brasil no fim da década de 1980, somente em 2014 foi gerado o Marco Civil da Internet, o qual regulamenta o uso dessa ferramenta em nosso país, através de princípios, garantias, direitos e deveres em relação àqueles que tem acesso à rede, incluindo também a atuação do Estado.

As denúncias públicas realizadas por Edward Snowden, ex-consultor técnico da Agência Central de Inteligência (CIA) dos Estados Unidos, sobre a prática de vigilância mundial e não autorizada por este país em inúmeras esferas, inclusive governamentais, onde o Brasil estaria no rol dos investigados, se tornaram fatores estimulantes para o assunto obter maior visibilidade e se tornasse uma pauta prioritária.

Em vista disso, trata-se de uma norma principiológica, a qual visa sobretudo: liberdade de expressão, garantia da neutralidade da rede e a proteção à privacidade do usuário. O uso da internet no âmbito nacional tomou grande proporção

gradativamente, mas não existia um conjunto de regras jurídicas que de fato assegurassem os direitos e deveres dos usuários na internet, assim, o Marco Civil procurou regulamentar o modo como os direitos constitucionais entre outros permanecessem assegurados.

Além disso, esse dispositivo legal apresenta como ponto central a neutralidade da rede, tratando computadores e informações disposta no ciberespaço como iguais, sem quaisquer distinções, isso evita a ingerência desregradas dos provedores de Internet.

4.7 LEI Nº 13.185/2015: LEI DE COMBATE À INTIMIDAÇÃO SISTEMÁTICA (BULLYING)

A lei em voga foca na capacitação dos docentes e equipes pedagógicas para implementar ações de prevenção e solução de problemas referentes a essa temática, bem como a orientação de pais e familiares, mas o nosso enfoque diz respeito ao cyberbullying, que pode ser encontrado no art. 2º, parágrafo único: “Há intimidação sistemática na rede mundial de computadores (cyberbullying), quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial” (Brasil, 2015).

Portanto, esse dispositivo também se tornou uma benéfica inovação no que tange à prevenção dos delitos virtuais, procurando prevenir os violentos ataques que ocorrem diariamente no ciberespaço, em uma era onde a tela do dispositivo se transforma em uma armadura para práticas delituosas e ofensivas.

4.8 LEI Nº 13.709/2018: LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Em agosto de 2018 foi sancionada pelo então presidente Michel Temer a Lei Geral de Proteção de Dados do Brasil, a qual regulamenta e estabelece regras relacionadas à coleta, armazenamento, tratamento e compartilhamento de dados pessoais, além disso, impõe mais proteções e penalidades em casos de descumprimento.

A LGPD traz alguns princípios que as organizações devem obedecer, como

por exemplo: o princípio da finalidade, da adequação, da necessidade e da transparência. Em caso de vazamento de dados, estes serão analisados pela Autoridade Nacional de Proteção de Dados (ANPD), e julgados de acordo com a gravidade de cada caso concreto.

As empresas também serão orientadas se deverão ou não divulgar o vazamento publicamente, portanto, esses descumprimentos colocam em risco inclusive a própria reputação da pessoa jurídica. Além disso, as multas serão aplicadas de modo proporcional, que vão de 2% sobre o faturamento anual, limitando-se a 50 (cinquenta) milhões de reais, ou multa diária, onde os valores não podem ultrapassar o valor supracitado.

4.9 DECRETO Nº 10.222/2020: ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA

Após a reunião envolvendo órgãos públicos, entidades privadas e o meio acadêmico acerca dos aspectos da segurança cibernética, o decreto nº 10.222/20 foi criado com o intuito de expandir a resiliência brasileira frente às ameaças virtuais, promovendo deste modo, diversas diretrizes, as quais possuirão validade até 2023.

Entre as ações propostas, inclui-se:

> O fortalecimento das ações de governança cibernética; o estabelecimento de um modelo centralizado de governança em nível nacional; a promoção de um ambiente participativo e colaborativo entre setor público e privado; o aumento do nível de proteção do governo; elevar a proteção das Infraestruturas Críticas Nacionais; aprimorar o arcabouço legal sobre segurança cibernética; incentivar a concepção de soluções inovadoras em segurança; ampliar a cooperação internacional; ampliar a parceria entre setor público, privado, academia e sociedade; e aumentar o nível de maturidade da sociedade no que diz respeito à segurança cibernética. (Conjur, 2020).

Apesar de o decreto ser de grande valia para o país em decorrência da vigente demanda e do aumento dos ataques virtuais, não traz especificações práticas para que tais ações sejam concretizadas. Percebe-se, portanto, que o legislador brasileiro peca principalmente na maneira de produzir os dispositivos em geral, pois se tornam muito abrangentes, deixando de ser verdadeiramente efetivos.

Em comparação aos outros países, o Brasil ainda está muito atrasado em

termos de organização e orientação na promoção dos dispositivos legais que regulem o uso dos meios digitais, bem como combater os referidos delitos. Faz-se necessário a construção de um modelo mais robusto e direcionado a práticas precisas, e não meramente simbólicas.

4.10 LEI Nº 14.132/2021: CRIME DE PERSEGUIÇÃO

O crime de perseguição, popularmente conhecido como “stalking”, também foi alvo de regulamento do ordenamento jurídico no ano de 2021, uma grande novidade que proporcionou maior segurança em relação à proteção virtual, afinal, torna-se muito fácil perseguir um indivíduo atrás da tela de um dispositivo informático, sem qualquer identidade, pautando-se no anonimato.

Assim, a lei em questão acrescenta o art. 147-A ao Código Penal, para prever o crime de perseguição e revoga o art. 65 da Lei das Contravenções Penais:

> Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade (Brasil, 1940).

Sendo assim, ao utilizar os termos “por qualquer meio”, o legislador inclui não apenas a perseguição material, mas também o meio digital. Ademais, caso o agente ameace de alguma forma a integridade física ou psicológica do sujeito passivo, restringindo a capacidade de locomoção, invadindo ou perturbando a esfera de liberdade ou privacidade deste, poderá ser condenado a pena de reclusão de 6 (seis) meses a 2 (dois) anos, e multa.

5 OS EMPECILHOS NA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

O predominante uso diário da tecnologia ampliou consideravelmente as relações contemporâneas, bem como todos os nichos sociais. Em decorrência desse alto dinamismo, a polícia investigativa encontra diversas dificuldades para lograr a materialidade do delito dos crimes cibernéticos, e por consequência, os agentes responsáveis por essas práticas, afinal, é imprescindível a realização de uma investigação clara e objetiva para a obtenção de êxito na *persecutio criminis,* assim, e o processo possa respeitar os ditames legais.

Além de observar o meio pelo qual o delito foi praticado, os investigadores devem se ater as peculiaridades dos indícios deixados pelo agente. Contudo, em relação aos crimes virtuais, os rastros são muito voláteis e instáveis, podendo ser: excluídos, alterados ou perdidos a qualquer momento, além disso, nesse tipo de diligência é necessário ter extrema cautela para que não haja quaisquer adulterações durante o processo de produção de prova.

Outrossim, após receber uma notícia de um crime cibernético, a autoridade responsável pela investigação deve primeiramente identificar o meio pelo qual foi gerado o delito, como: website, e-mail, mensagem instantânea, comunidades virtuais, rede sociais, entre outros. De modo geral, as evidências dos crimes virtuais possuem formatos específicos, são inconstantes e costumam estar insertas em conjunto com outros dados, existe sempre uma conjuntura de informações quando se trata de dados dispostos no ambiente cibernético.

Desta forma, se torna oportuno abordamos os principais empecilhos encontrados pela Polícia Judiciária na busca do agente criminoso dos crimes cibernéticos. Tendo em vista que as evidências deixadas pelo mesmo são muito mutáveis e podem ser facilmente ocultadas ou excluídas em apenas um comando, é necessário expandir a capacitação, bem como reciclagens para habilitar os responsáveis pela investigação preliminar a lidar com esse novo panorama.

5.1 A RELEVÂNCIA DO PROCEDIMENTO INVESTIGATIVO NA FASE PRÉ-PROCESSUAL DOS CRIMES CIBERNÉTICOS

A *persecutio criminis* se inicia a partir da investigação criminal, logo, os

elementos advindos desse procedimento implicarão diretamente na decisão processual. Desta maneira, por se tratar da fase pré-processual, possui grande relevância na obtenção da veracidade dos fatos e no encontro do agente delituoso.

Apesar de o inquérito ser prescindível para o oferecimento da acusação ou queixa, conforme o art. 12 do Código de Processo Penal se trata de um procedimento de extrema relevância, e se torna útil inclusive na defesa do investigado, pois podem surgir provas ou indícios da não participação do mesmo em determinado delito, inclusive os cibernéticos, objeto de estudo.

No entanto, alguns doutrinadores defendem a imprescindibilidade do inquérito policial, a saber:

> Apesar dos problemas que possam ter, a fase pré-processual (inquérito, sumário, diligencias prévias, investigação etc.) é absolutamente imprescindível, pois um processo penal sem a investigação preliminar é um processo irracional, uma figura inconcebível segundo a razão e os postulados básicos do processo penal constitucional (Lopes Jr., 2011, p. 209).

Assim, a investigação no âmbito dos delitos virtuais possui o mesmo objetivo dos demais, ou seja, obter indícios de materialidade e autoria do crime, contudo, por ser tratar de um ilícito praticado através de um dispositivo informático com o auxílio ou não da internet, o fato pode ser praticado/consumado em qualquer lugar do globo, por isso a investigação é muito mais complexa e requer maior atenção, tendo em vista que os seus vestígios podem se perder no ciberespaço a qualquer momento.

5.2 TECNOLOGIA

Tratando-se de crimes virtuais existem inúmeras dificuldades técnicas as quais colocam o investigador longe do agente delituoso. A primeira diz respeito a localização do suspeito, pois nem sempre será possível identificar o endereço de IP (Internet Protocol), responsável por obter a localização exata dos computadores. Porém, esse tipo de evidência pode ser facilmente ocultada utilizando servidores de proxies variados, como no caso de redes Wi-Fi abertas ou Lan Houses, onde não há um controle exclusivo ou limitado por parte do usuário, mas um uso coletivo dos dispositivos e conexões.

Para ter acesso à rede, o usuário precisa passar pelo servidor proxy, serve como um intermediário que faz ponte entre a origem e o destino das requisições feita pelo usuário, logo, é utilizado como um controle de acesso e filtro de conteúdo. Em vista disso, os agentes criminosos utilizam tais servidores, sobretudo o modo anônimo, para cometer o ato infracional, assim, as vítimas não conseguem saber a real origem da conduta, e as regras de bloqueio não conseguem ser efetivas para impedir a continuidade do ataque.

Visto que o usuário pode ter acesso a diferentes proxies, se um deles não estiver de acordo com os demais e não resguardar ou fornecer as informações dos usuários, não será possível identificar os mesmos através desse protocolo. Além disso, a capacidade técnica dos agentes responsáveis pela persecução penal é essencial para que haja plena eficácia na busca pela materialidade do delito.

É muito comum encontrarmos agentes públicos sem quaisquer conhecimentos específicos dos meios tecnológicos, mas esse não é o único problema, a maioria dos órgãos não possui uma estrutura organizacional específica para atuar no desenvolvimento das investigações dos crimes digitais, caracterizando desta forma, falha no sistema estatal, o qual possui o dever de fornecer os meios necessários para resguardar e assegurar os bens jurídicos da sociedade.

> As tecnologias, em todos os tempos, alteraram as formas de retentiva e lembrança, funções usuais com que os homens armazenam e movimentam suas memórias humanas, seus conhecimentos. Na atualidade, as novas tecnologias de comunicação não apenas alteram as formas de armazenamento e acesso das memórias humanas como, também, mudam o próprio sentido do que é memória. Através de imagens, sons e movimentos apresentados virtualmente em filmes, vídeos e demais equipamentos eletrônicos de comunicação, é possível a fixação de imagens, o armazenamento de vivências, sentimentos, aprendizagens e lembranças que não necessariamente foram vivenciadas in loco pelos seus espectadores (Kenski, 1997, p. 59).

Um exemplo na alteração de armazenamento de arquivo e por consequência de provas, é o “Cloud Computing” ou Computação nas Nuvens, sendo um serviço que permite a execução e guarda de arquivos e programas diretamente na Internet, ou seja, não é necessário o meio físico para ter acesso, logo, não estarão insertos no dispositivo computacional ou eletrônico, mas em servidores responsáveis por esse tipo de serviço.

Em vista disso, se o agente decidir obter ilicitamente ou adulterar qualquer

arquivo, e em seguida armazená-lo nas nuvens, será muito mais dificultoso ao investigador encontrar as referidas informações, portanto, a tecnologia se tornou também uma grande aliada àqueles que visam praticar condutas infratoras, e um empecilho aos agentes públicos.

A criptografia utilizada para a proteção de dados não é uma novidade, na antiguidade clássica, essa ferramenta foi utilizada na Grécia e Roma antiga para proteger determinadas informações, estas por sua vez, eram transformadas em algoritmos específicos para se tornarem incompreendidas, ocultando para alguns o real teor do material.

O objetivo criptográfico é transformar quaisquer mensagens em um texto codificado, desta forma, haverá confidencialidade da informação, logrando assim uma troca de informações sigilosas entre emissor e receptor. Hodiernamente é possível verificar a presença dessa técnica na maioria dos aplicativos, como o Whatsapp, por exemplo, ferramenta responsável por troca de mensagens instantâneas e a mais popular entre os brasileiros, o objeto neste caso, é preservar a intimidade, liberdade e privacidade.

Figura 1- Criptografia Simétrica: Decodificação

Fonte: (UFRJ, 2008)

Depreendemos, portanto, que apesar das inúmeras facilidades promovidas pela era digital, no quesito investigação criminal, a própria tecnologia se torna um fator embaraçoso, visto que auxilia o criminoso a se ocultar de inúmeras maneiras no espaço virtual. Contudo, é necessário a compreensão e discernimento sobre a legalidade dos processos por parte inclusive dos agentes.

De acordo com o entendimento da 6ª Turma do Superior Tribunal de Justiça,

a conservação das provas em uma investigação criminal é obrigação do Estado, assim, a perda desses elementos impedirá a ampla defesa, prevista no art. 5º, LV da Constituição Federal. O julgado anulou as provas produzidas em interceptações telefônicas e e-mails que foram apagadas pela Polícia Federal, estando deste modo, em desconformidade com o devido processo legal.

> A superveniência do julgamento do HC 122.922/RJ tornou sem objeto a Reclamação 3.467/RJ – ajuizada para assegurar a liminar, deferida nos autos do HC 122.992/RJ –, que foi julgada prejudicada. Ocorre que, como afirmado pelos impetrantes, na inicial, apesar de lhes ter sido franqueado o acesso aos autos, parte das provas obtidas, a partir da interceptação telemática, foi extraviada, ainda na Polícia Federal, e o conteúdo dos áudios telefônicos não foi disponibilizado da forma como captado, havendo descontinuidade nas conversas e na sua ordem, não sendo, portanto, tais provas encartadas nos autos do Inquérito Policial e da Ação Penal, as quais são consideradas de fundamental importância ao esclarecimento dos fatos apurados, pois, segundo alegam, 'dentre os e-mails interceptados e não disponibilizados estão todos aqueles da empresa alvo da investigação, ou seja, aqueles que encerram com @casaevideo.com.br, vinculados ao provedor Embratel, inclusive a conta do e-mail do principal denunciado (LUIGI MILONE)' (Conjur, 2014, p. 15e).

Depreende-se a partir do caso em tela que, é necessário que os profissionais responsáveis pela persecução penal estejam plenamente capacitados para lidar não apenas com o conhecimento técnico referente aos aplicativos e dispositivos em geral, mas também o procedimento legal como um todo, caso contrário, irá caracterizar grave falha na função do Estado em propiciar o combate aos crimes virtuais.

5.3 LEGISLAÇÃO

O Direito Brasileiro, assim como a tecnologia, possui grande dinamicidade e está em constante mudança, deste modo, deve acompanhar as modificações e novidades advindas das interações sociais para exercer de modo eficaz o seu papel, buscando obter uma conjuntura mais pacífica para assegurar a proteção dos bens jurídicos.

Percebe-se que as leis relacionadas aos cibercrimes não são robustas o suficiente para conter de modo pragmático desse tipo de delito, pois pecam pela falta técnica, dando margens, inclusive interpretações dúbias, dificultando a aplicabilidade.

> A segurança jurídica consiste no conjunto de condições que tornam possível às pessoas o conhecimento antecipado e reflexivo das consequências diretas de seus atos e de seus fatos à luz da liberdade reconhecida. Uma importante condição da segurança jurídica está na relativa certeza que os indivíduos têm de que as relações realizadas sob o império de uma norma devem perdurar ainda quando tal norma seja substituída.

Portanto, caso não subsista no poder do Estado leis plenamente efetivas que possam de fato garantir uma segurança jurídica, seus cidadãos tornar-se-ão efetivamente vulneráveis à prática delituosa. O mesmo ocorre em relação ao processo de investigação, tendo em vista que o mesmo é regido pela própria legislação e necessita não apenas de um rol taxativo de regras normativas, mas de uma força legal que promova eficácia aos processos judiciais.

De acordo com Maciel (2012, p. 1) “a guarda de dados é relevante pelo fato de tais registros serem fundamentais para identificação de usuários, seja para produção de prova civil ou mesmo para subsidiar investigação criminal”.

Assim, a proteção dos dados dar-se-á também pelo uso cauteloso dos internautas, não somente por força normativa. Mas o que se observa são leis esparsas que visam apenas preencher lacunas decorrentes de fatos contemporâneos, como no caso da Lei Carolina Dieckmann, a qual será explanada pormenorizadamente mais adiante.

> O fator criminógeno virtual cresce de forma a fazer surgirem crimes novos, além de potencializar alguns dos já existentes. Muitos desses crimes são cometidos através da internet ou com o uso do computador. Desse modo, é criada uma nova esfera de atuação delituosa, a saber, os chamados crimes virtuais ou cibercrimes (como são chamados os crimes praticados com o uso do computador ou crimes praticados pela internet). De certo, a informática proporciona uma fácil interação entre as pessoas e, caso não seja utilizada de forma correta, acaba por ser uma meio eficaz na prática de delitos (Polegatti; Kazmierczac, 2012, p. 1-2).

Além disso, os mesmos ressaltam que:

> Dessa forma, torna-se necessária a atuação do Estado no sentido de coibir esse tipo de conduta, sendo necessária a criação de tipos penais ainda não previstos na legislação e que envolvam o mundo virtual, uma vez que não é permitido, em Direito Penal, utilizar analogia em relação às tipificações já existentes (Polegatti; Kazmierczak, 2012, p. 8).

Outro exemplo que exibe a falta de leis próprias no âmbito virtual é a celebração de contratos por essa via. O Código Civil e o Código de Defesa do Consumidor sanam, em parte, os conflitos atinentes a respeito desse tema, “faltando uma norma específica que assegure os asseios da comunidade virtual” (Vedovate, 2005, p. 13).

Apesar do princípio da analogia não ser utilizado no Direito Penal por atingir o princípio da taxatividade, a prática contrasta com a teoria, neste sentido:

> São exemplos de normas aplicadas, com a utilização da analogia, aos crimes virtuais: Calúnia (art. 138 do Código Penal); Difamação (art. 139 do Código Penal); Injúria (art. 140 do Código Penal); Ameaça (art. 147 do Código Penal); Furto (art. 155 do Código Penal); Dano (art. 163 do Código Penal); Apropriação indébita (art. 168 do Código Penal); Estelionato (art. 171 do Código Penal); Violação ao direito autoral (art. 184 do Código Penal); Pedofilia (art. 247 da Lei nº 8.069/90 – Estatuto da Criança e do Adolescente); Crime contra a propriedade industrial (art. 183 e ss. da Lei nº 9.279/96); Interceptação de comunicações de informática (art. 10 da Lei nº 9.296/96); Interceptação de E-mail Comercial ou Pessoal (art. 10 da Lei nº 9.296/96); Crimes contra software – “Pirataria” (art. 12 da Lei nº 9.609/98). (Carneiro, 2012, p. 1).

Conforme abordado por Furlaneto Neto e Guimarães (2003, s/p), existem no âmbito cibernético os denominados ilícitos prejudiciais, os quais não são considerados crimes, mas geram prejuízos da mesma maneira, como por exemplo: danos contra dados e informações, programas maliciosos, propagação de vírus, entre outros que não possuem uma regulamentação normativa e se tornam muitas vezes condutas atípicas.

Assim, as legislações que tratam do assunto não abrangem um campo extenso para conter de fato a atuação do criminoso, todavia “as soluções legais a serem buscadas deverão objetivar a circulação de dados pela Internet, controlando a privacidade do indivíduo sem cercear o acesso a informação” (Atheniense, 2004, p. 1). Além da legislação local, a cooperação internacional é imprescindível no controle e regulamentação desse tipo de ilícito, conforme asseverado alhures.

5.4 DIREITO PENAL SIMBÓLICO

Apesar de o ordenamento jurídico brasileiro possuir alguns avanços no que tange a normatização dos crimes cibernéticos, como foi visto no capítulo anterior,

nem todas essas leis possuem plena efetividade na prática, tornando-se meramente simbólicas. O Direito Penal Simbólico é identificável por meio de duas características principais: não se destina a cumprir sua real missão – tutelar efetivamente os bens jurídicos, em nosso entendimento – e obedece a propósitos de pura jactância de classe política (Hassemer, 1998, p. 27).

É possível perceber que se trata de um falso analgésico social, capaz de sanar, sobretudo, o clamor popular, como ocorreu com a Lei nº 12.737/12, mais conhecida como Carolina Dieckmann, a qual foi criada a partir da persistente pressão popular e midiática.

> Assim, portanto, haverá de ser entendida a expressão “direito penal simbólico”, como sendo o conjunto de normas penais elaboradas no clamor da opinião pública, suscitadas geralmente na ocorrência de crimes violentos ou não, envolvendo pessoas famosas no Brasil, com grande repercussão na mídia, dada a atenção para casos determinados, específicos e escolhidos sob o critério exclusivo dos operadores da comunicação, objetivando escamotear as causas históricas, sociais e políticas da criminalidade, apresentando como única resposta para a segurança da sociedade a criação de novos e mais rigorosos comandos normativos penais (Neto, 2009, p. 1).

Além disso, de acordo com Bauman:

> Os perigos que mais tememos são imediatos: compreensivelmente, também desejamos que os remédios o sejam – “doses rápidas”, oferecendo alívio imediato, como analgésicos prontos para o consumo. Embora as raízes do perigo possam ser dispersas e confusas, queremos que nossas defesas sejam simples e prontas a serem empregadas aqui e agora. Ficamos indignados diante de qualquer solução que não consiga prometer efeitos rápidos, fáceis de atingir, exigindo em vez disso um tempo longo, talvez indefinidamente longo, para mostrar resultados (Bauman, 2008, p. 149).

Destarte, essa espécie de lei possui determinada formulação defeituosa no sentindo técnico, o que a torna inaplicável na prática, deste modo, a adoção de um direito penal simbólico afronta então o princípio da intervenção mínima, pois quando o legislador opta por uma “resposta instantânea” a esses clamores, acaba de certo modo, reduzindo à tutela dos bens jurídicos mais significativos.

5.5 INEFICÁCIA DO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO (154-A DO CÓDIGO PENAL)

A Lei nº 12.737/12 mais conhecida como Lei Carolina Dieckmann tipificou o crime de “invasão de dispositivo informático”, de modo que o art. 154-A e 154-B foram inseridos no Código Penal Brasileiro com o intuito de preservar à intimidade e privacidade. Além disso, é o único tipo penal exclusivamente cibernético, por isso faz-se necessário uma análise mais detalhada, para que na prática, se observe a (in) eficácia dos tipos penais concernentes aos crimes cibernéticos.

Assim, este dispositivo legal eclodiu após o caso envolvendo a atriz Carolina Dieckmann, onde o agente invadiu o dispositivo informático da mesma, se apoderou de dados pessoais, inclusive fotos íntimas, vencendo todos os obstáculos do aparelho, e por conseguinte, realizou chantagens e extorsões visando benefícios de modo ilícito, por meio da publicação de alguns arquivos na Internet.

Apesar da incessante imposição dos meios digitais resultantes da era moderna, torna-se dificultoso acompanhar essas mudanças, não apenas para a sociedade, mas principalmente para o Código Penal, o qual deve estar atento às transformações da sociedade para evoluir de modo concomitante ao meio cibernético.

> Sabe-se, por certo, constituir a comunicação telemática, o atual meio mais difundido de transmissão de mensagens de toda a ordem entre pessoas físicas e jurídicas. O e-mail tornou-se uma forma padrão de enviar informes e mensagens profissionais e particulares, seja para fins comerciais, seja para outras finalidades das mais diversas possíveis. As redes sociais criaram, também, mecanismos de comunicação, com dispositivos próprios de transmissão de mensagens. Torna-se cada vez mais rara a utilização de cartas e outras bases físicas, suportando escritos, para a comunicação de dados e informes. Diante disso, criou-se novel figura típica incriminadora, buscando punir quem viole não apenas a comunicação telemática, mas também os dispositivos informáticos, que mantém dados relevantes do seu proprietário (Nucci, 2019, p. 774-775).

O objetivo principal do delito, portanto, é invadir a privacidade individual ou profissional do indivíduo, ou seja, lesionar um direito constitucional. Conforme o art. 5º, X, da Carta Magna: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação”.

Ademais, se trata de um crime de menor potencial ofensivo, exceto em sua forma qualificada ou majorada pela divulgação, comercialização e transmissão a terceiro. Além disso, é admissível o acordo de não persecução penal, previsto no art.

28-A do Código de Processo Penal.

5.5.1 Sujeitos do delito

No caso do art. 154-A o sujeito ativo do delito pode ser qualquer pessoa, logo, não exige nenhuma qualidade ou condição especial do agente. Em visa disso, existem casos em que haverá diversos sujeitos utilizando apenas um aparelho eletrônico, como é o caso de computadores compartilhados. De acordo com Márcio Cavalcante:

> Em regra, a vítima é o proprietário do dispositivo informático, seja ele pessoa física ou jurídica. No entanto, é possível também identificar, em algumas situações, como sujeito passivo, o indivíduo que, mesmo sem ser o dono do computador, é a pessoa que efetivamente utiliza o dispositivo para armazenar seus dados ou informações que foram acessados indevidamente. É o caso, por exemplo, de um computador utilizado por vários membros de uma casa ou no trabalho, onde cada um tem perfil e senha próprios. Outro exemplo é o da pessoa que mantém um contrato com uma empresa para armazenagem de dados de seus interesses em servidores para acesso por meio da internet (‘computação em nuvem’, mais conhecida pelo nome em inglês, qual seja, cloudcomputing) (Dizer Direito, 2012).

Ademais, se trata de um tipo penal complexo, o legislador neste caso, não regulamentou de modo prático a questão supracitada, pois apenas estabelece a conduta de invadir sem autorização expressa ou tácita do titular do dispositivo, mas não das informações em si, visto que a tutela deveria recair expressamente no titular dos dados armazenados, todavia não foi um fato observado pelo legislador durante a elaboração do artigo em voga.

5.5.2 Conduta

Sendo assim, em relação ao objeto material, trata-se de coisa alheia móvel capaz de armazenar e processar automaticamente informações e programas, como, por exemplo: notebooks, computadores, celulares, tablets, etc. Deste modo, o tipo em questão tutela também o direito à liberdade individual no contexto da privacidade pessoal ou profissional do ofendido, visto que sua divulgação pode acarretar dano a outrem.

O artigo 154-A e 154-B do Código Penal eclodiram visando punir dois comportamentos distintos: invadir dispositivo informático alheio mediante violação de segurança ou a instalação de vulnerabilidades no respetivo bem. Ademais, a conduta criminosa recai sobre o dispositivo propriamente dito, por isso o seu caráter exclusivamente cibernético. De acordo com o caput:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa. (Brasil, 1940).

Assim, caso o agente vença o mecanismo de segurança, como uma senha, por exemplo, e obtenha tais informações, será considerado crime somente se o dispositivo informático possuir essa configuração, posto isso, se por algum motivo o proprietário não acioná-lo, a conduta será atípica, portanto, é elementar do tipo penal. Logo, A ausência de dispositivo de segurança, ou o seu acionamento, impede a configuração típica, tendo em vista que o legislador optou por não proteger a intimidade das pessoas que escolhem ou até mesmo, eventualmente, esquecem de ativar o mecanismo de segurança nos dispositivos informáticos.

Outra conduta punível ocorre quando o cibercriminoso instala vulnerabilidades no dispositivo em decorrência de brechas no sistema computacional, como por exemplo: bugs, vírus, spam, malware, etc., ou seja, softwares maliciosos para atacar, degradar e impedir a utilização correta do equipamento.

Deste modo, o parágrafo primeiro aborda inclusive o liame comercial desse tipo de prática, segundo o caput: “Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput” (Brasil, 1940).

Assim, essas condutas recaem sobre dados e informações demasiadamente relevantes, destarte, o dispositivo visado pelo agente precisa ser alheio. Além disso, em relação à voluntariedade, nesta, subsiste o dolo, a vontade inteiramente consciente de invadir o dispositivo de outrem, violando os termos até então mencionados.

5.5.3 Consumação e tentativa

Posto isto, vislumbra-se neste caso um crime formal, o qual se consuma no momento em que o próprio sujeito ativo invade o aparato informático do sujeito passivo, seja através da violação indevida ou instalando vulnerabilidades, não necessariamente ligado à rede mundial de computadores. A tentativa é admissível por se tratar de um delito plurissubsistente, o qual exige pluralidade de sujeitos ativos, fracionando assim o *iter criminis.*

> [...] imagine-se a hipótese na qual o agente é descoberto quando procurava invadir o dispositivo informático alheio, durante suas tentativas de violar indevidamente o mecanismo de segurança, para os fins previsto no tipo penal em estudo. Nesse caso, estaria caracterizado o crime tentado (Greco, 2016, p. 523).

Deste modo, assim como ocorre no *caput*, será possível a tentativa na modalidade equiparada, ou seja, ocorrerá a consumação quando o agente produzir, oferecer, distribuir, vender ou difundir dispositivo informático ou programa de computador com o intuito de realizar a conduta prevista no art. 154-A do Código Penal.

5.5.4 Ação Penal

A ação penal recai tanto para quem vende mecanismo quanto àqueles que visam vencer os obstáculos de segurança, incluindo quem distribui esses softwares maliciosos. Seja no caput ou parágrafo primeiro, a ação penal recairá nas duas condutas, o que pode ser observado no art. 154-B do Código Penal:

> Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (Brasil, 1940).

Em regra, o crime do art. 154-A só se procede mediante representação da vítima. No caput podemos perceber facilmente a vítima, trata-se do dono do

dispositivo informático que teve o seu código de segurança vencido e, portanto, o agente criminoso se apoderou ou adulterou os dados nele inserido. Assim, o mesmo deve representar para que haja a persecução penal, logo, é necessário então que o mesmo faça o pedido.

Todavia, o parágrafo primeiro não diz respeito a pessoa que vence o código ou coloca o software malicioso, mas sim quem vende tais ferramentas. Neste caso, não existe vítima, pois é indetermina. Em vista disso, surgiram duas correntes: a primeira menciona que o parágrafo primeiro tomou letra morta, pois o legislador não previu a ação penal pública incondicionada para esse caso, não sendo em regra objeto de ação penal por não ter quem a represente. Enquanto segunda a corrente dispõe que, no silêncio do legislador, deve-se aplicar a ação penal pública incondicionada.

Deste modo, apesar do crime de invasão de dispositivo informático ter sido uma novidade bastante aceita e popular no Código Penal, refere-se a um tipo detentor de muitas lacunas, decorrentes inclusive da dissertação breve e confusa legislador, o qual cedeu à pressão popular para gerar um artigo específico destinado a esse fim, deixando, porém, de se ater a vários detalhes, gerando assim uma norma penal simbólica.

> Por acharem ser emergencial a aprovação da lei, os legisladores fizeram o tramite do seu projeto com certa rapidez para satisfazer a população, o que acabou sendo um erro, pois não foi feita uma análise racional e correta perante suas normas, tendo alguns doutrinadores advertido falhas da respectiva legislação (Granato, 2015, p. 36).

A redação equivocada nesse caso gera não apenas lacunas legislativas, mas impactam diretamente na praxe forense da investigação dos crimes cibernéticos, devido a sua alta celeridade ocasionada pelo clamor popular e midiático, deixando de disciplinar os meios processuais essenciais para garantir a eficácia da norma penal incriminadora.

Ademais, o modo como essa lei foi produzida expõe a maneira como o Estado tutela as mudanças advindas da tecnologia, fator de grande relevância para o reconhecimento de medidas protecionistas direcionadas aos eventuais danos ocasionados à sociedade decorrente do âmbito virtual.

O cerne da questão pode ser encontrado através da análise deste artigo, afinal, a mesma foi elaborada com o objetivo de punir condutas consideradas criminosas geradas na esfera cibernética, contudo, o art. 154-A é utilizado apenas como mera repressão estatal, concedendo benefícios relativos aos crimes de menor potencial ofensivo, com aplicação de pena de 3 (três) meses a 1 (um) ano, e multa. Nota-se, portanto, que o dispositivo não consolidou a capacidade intimidadora necessária para prevenir tais delitos.

É necessário ter muita cautela ao criar leis, estas, devem ser produzidas observando-se os princípios plurais e democráticos de direito, e não elaboradas como fatos isolados, com penalidades frágeis e rasas em delitos que lesam preceitos e garantias constitucionais.

Destarte, o imediatismo na elaboração de dispositivos criminais com tamanha celeridade e inobservância, faz com que o Direito Penal se torne o primeiro instrumento para a solução de conflitos, o que é vedado no ordenamento jurídico de acordo com o princípio da intervenção mínima.

6 CONSIDERAÇÕES FINAIS

A revolução tecnológica desenvolvida após a eclosão da Internet trouxe inúmeros benefícios à sociedade. O ciberespaço é um ambiente amplo, infinito e ilimitado, assim, a conduta delituosa se tornou mais pragmática àqueles que visam lesionar os bens jurídicos, como por exemplo, a liberdade e privacidade, dispostos no art. 5º da Constituição Federal. Sendo assim, além de ferir elementos assegurados pelo Estado e gerar dados aos cidadãos, caso não sejam estudados e analisados cautelosamente, os crimes cibernéticos possuem o poderio para produzir diversos transtornos no sistema jurídico brasileiro, sobretudo em relação à *persecutio criminis.*

Em vista disso, essa monografia buscou analisar no primeiro capítulo, o modo como a população está vulnerável em decorrência do mau uso dos meios digitais, além disso, se não existe um arcabouço normativo que sustente de forma robusta o combate aos delitos virtuais, o ambiente virtual tornar-se-á, portanto, uma terra sem lei ou regramentos, repleto de atipicidade. Além disso, é importante observar que, não basta apenas o desenvolvimento do tipo penal, o mesmo deve promover plena efetividade, caso contrário, será apenas mais um elemento simbólico incluso de maneira esparsa nos códigos legais.

Nesse sentido, o segundo capítulo desmembrou os principais conceitos sobre os crimes cibernéticos, bem como suas respectivas nuances, além de explorar os essenciais princípios norteadores que influem diretamente da produção das normas concernentes aos delitos virtuais, além disso, merecem uma atenção especial tendo em vista o seu caráter *sui generis*.

Posto isto, o terceiro capítulo expõe de modo cronológico algumas leis e decretos que visam prevenir os crimes cibernéticos, todavia, a maioria dessas normas recebem inúmeras críticas, pois notoriamente não detém natureza intimidadora, e são detentoras de penas rasas e textos confusos.

Assim, a própria legislação se torna um fator que dificulta a investigação dos crimes cibernéticos, visto que a persecução penal se baseará somente pelas disposições do ordenamento jurídico.

O último capítulo examinou os principais empecilhos encontrados durante o processo de investigação criminal, e os seus respectivos impactos na persecução

penal. Caso a Polícia Judiciária (Polícia Civil e Polícia Federal) não esteja efetivamente habilitada para lidar com as novidades do meio digital, a busca pela materialidade do delito, bem como o seu respectivo agente será prejudicada, pois como foi apresentado, o sujeito ativo possui inúmeras formas de se ocultar no meio virtual, e o desconhecimento dos meios tecnológico por parte do Estado, acarretará prejuízos vultosos em todos os sistemas.

Além disso, como o objeto do trabalho tem como centro os empecilhos na investigação dos crimes cibernéticos, foi incluído neste rol a própria legislação, fez-se necessário, portanto, realizar uma análise minuciosa acerca do único crime exclusivamente cibernético, disposto no art. 154-A do Código Penal e advindo da Lei nº 12.727/12, denominado “invasão de dispositivo informático”.

Assim, através de um exemplo concreto se tornou possível vislumbrar a desordem do legislador ao produzir esse tipo de dispositivo, deixando de promover plena eficácia.

Outrossim, caso não haja uma normatização robusta, o número de fatos atípicos ascenderá, pois de acordo com o princípio da legalidade, não há crime (ou contravenção penal) sem prévia definição legal; igualmente, inexiste pena sem prévia cominação legal.

Diante disso, percebe-se, por exemplo, que ao inserir a expressão “violação indevida de mecanismo de segurança” o próprio legislador limitou demasiadamente a conduta do agente, pois caso o sujeito passivo não possua qualquer mecanismo de segurança, como uma senha, não haverá crime, além disso, o legislador não previu a ação pública incondicionada relativa àqueles que vendem o software malicioso, deixando a cargo da doutrina e jurisprudência a respectiva decisão.

Logo, depreende-se que, a proteção de um bem jurídico torna-se falha, caso o legislador não esteja atendo a elementar do tipo penal, no caso supracitado, para que seja considerado crime, a questão fica alienada a necessidade de “violar” o dispositivo informático.

Assim, o aumento de pena destinado aos infratores, é um fator imprescindível para que esses dispositivos não se tornem tão rasos e precários, afinal, bens jurídicos tão relevantes como à intimidade e liberdade, não pode figurar somente como um crime de menor potencial ofensivo sujeito a pena de multa, a era digital requer um regramento muito mais robusto, concentrado e analítico.

Sendo assim, conclui-se que, os crimes cibernéticos apesar de predominantes nas relações sociais, ganham cada vez mais espaço por encontrarem brechas e lacunas no sistema jurídico, os quais geram inclusive empecilhos no processo de produção de provas, além disso, a legislação é o meio propulsor dessa deficiência sistemática, pois um ordenamento com leis penais vagas, sem deter a atenção devida do legislador no processo de produção normativa, torna a sociedade cada vez mais vulnerável aos ataques cibernéticos.

Por fim, destaca-se que a presente pesquisa visou explicitar o atual cenário legislativo concernente aos crimes virtuais, para que se evite a expansão dessas infrações no cenário nacional decorrentes dos obstáculos em voga, afinal, o legislador possui uma das maiores responsabilidades decorrente do Direito: exprimir os anseios jurídicos presentes em sua época.

REFERÊNCIAS

ALMEIDA, Jessica *et al.* Crimes Cibernéticos. **Periódicos do Grupo Tiradentes**. Aracaju, v. 2, n. 3, mar. 2015.

ANGELO, Tiago. Decreto sobre segurança cibernética é bem-vindo, mas deixa a desejar. Revista **Consultor Jurídico**, São Paulo, 7 de fevereiro de 2020. Disponível em: https://www.conjur.com.br/2020-fev-07/decreto-presidencial-cria-estrategia-nacional-seguranca-cibernetica. Acesso: 26 mar. 2024.

ARAS, Vladmir. **Crimes de informática**: Uma nova criminalidade. Disponível em: https://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em: 5 abr. 2024.

ATHENIENSE, Alexandre. **Crimes virtuais, soluções e projetos de Lei**. DNT. [s.l.]. Disponível em: http://www.dnt.adv.br/noticias/direito-penal-informatico/crimes-virtuais-solucoes-e-projetos-de-lei/. Acesso em: 27 mar. 2024.

BAUMAN, Zygmunt. **Medo líquido**. Rio de Janeiro: Jorge Zahar, 2008.

BORGES, Fabiani. **Terrorismo Cibernético e a Proteção de Dados Pessoais**. Disponível em: https://fabianiborges.jusbrasil.com.br/artigos/218335957/terrorismo-cibernetico-e-a-protecao-de-dados-pessoais. Acesso em: 15 ago. 2024.

BRASIL. **Lei nº Lei 11.829, de 25 de novembro de 2008.** Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em: 20 mar. 2024.

BRASIL. **Lei nº 12.015, de 07 de agosto de 2009.** Altera o Título VI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, e o art. 1º da Lei nº 8.072, de 25 de julho de 1990, que dispõe sobre os crimes hediondos, nos termos do inciso XLIII do art. 5º da Constituição Federal e revoga a Lei nº 2.252, de 1º de julho de 1954, que trata de corrupção de menores. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12015.htm. Acesso em: 20 mar. 2024.

BRASIL. **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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 16 mar. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 16 mar. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 16 mar. 2024.

BRASIL. **Lei nº 13.185, de 6 de novembro de 2015**. Institui o Programa de Combate à Intimidação Sistemática (Bullying). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em 16 mar. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 16 mar. 2024.

BRASIL. **Lei nº 14.132, de 31 de março de 2021.** Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14132.htm. Acesso em: 16 mar. 2024.

BRASIL. **Constituição Federal de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 01 abr. 2024.

BRASIL. **Código Penal Brasileiro, de 7 de dezembro de 1940.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 01 abr. 2024.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020.** Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 25 mar. 2024.

BRASIL. **Supremo Tribunal Federal.** Conflito negativo de competência. Justiça Federal x Justiça Estadual. Inquérito Policial. Divulgação de imagem pornográfica de adolescente via whatsapp e em chat no facebook. Art. 241-1 da Lei 8.069/90. Recurso Extraordinário nº 628.624, Relator: Min. Marco Aurélio, Relator p/ Acórdão: Min. Edson Fachin, Tribunal Pleno, julgado em 29.10.2015. Acórdão eletrônico repercussão geral, Mérito, DJe-062, Divulgação em: 05 abr. 2016, Publicação em: 06 abr. 2016. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/465717092/conflito-de-competencia-cc-150564-mg-2016-0338448-1/inteiro-teor-465717102. Acesso em: 08 abr. 2024.

BRASIL. **Supremo Tribunal Federal.** Inadmissibilidade da extradição (causa principal) torna viável o atendimento do pedido de prisão preventiva (medida

revestida de cautelaridade e impregnada de caráter ancilar e meramente acessório). Questão de ordem que se resolve no sentido do indeferimento do pedido de prisão cautelar. STF – PPE: 732, Distrito Federal nº 9999906-02.2014.1.00.0000, Relator: Min. Celso de Mello, Data de Julgamento: 11 nov. 2014, Segunda Turma, Data de Publicação: 02 fev. 2015. Disponível em: https://stf.jusbrasil.com.br/jurisprudencia/311630611/prisao-preventiva-para-extradicao-ppe-732-distrito-federal-9999906-0220141000000/inteiro-teor-311630617. Acesso em: 21. jan. 2024.

BRASIL. **Supremo Tribunal de Justiça.** Penal e Processual Penal. *Habeas Corpus* Substitutivo de Recurso Ordinário. Utilização do remédio constitucional como sucedâneo de recurso. STJ – HC: 160662 RJ 2010/0015360-8, Relatora: Min. Assusete Magalhães, Data de Julgamento: 18 fev. 2014, T6, Sexta Turma, Data de Publicação: DJe 17 mar. 2014. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/864482320/habeas-corpus-hc-160662-rj-2010-0015360-8/inteiro-teor-864482321?ref=juris-tabs. Acesso em: 05. abr. 2024.

CABETTE, Eduardo. O novo crime de invasão de dispositivo informático. Revista **Consultor Jurídico**, São Paulo. 4 de fevereiro de 2013. Disponível em: https://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico. Acesso em: 20 mar. 2024.

CARVALHO, Freedy. **Você na era digital: os desafios da revolução da comunicação.** Disponível em: http://www.mk2.com.br/mk2/voce-na-era-digital-os-desafios-da-revolucao-na-comunicacao.asp. Acesso em: 07 mar. 2024.

CARNEIRO, Adeneele. Crimes Virtuais: Elementos Para uma Reflexão Sobre o Problema na Tipificação. In: **Âmbito Jurídico**, Rio Grande, 15, n. 99, abr. 2012. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=11529. Acesso em: 25 mar. 2024.

CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Trad. Maria Luíza X. de A. Borges. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. **O poder da identidade**. São Paulo: Paz e Terra, 1999.

CASTRO, Carla Rodrigues Araújo. **Crimes de informática e seus aspectos processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2001.

CAVALCANTE, Márcio. Primeiros comentários à Lei 12.737/12, que tipifica a invasão de dispositivo informático. 15 de dezembro de 2012. Disponível em: https://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html. Acesso em: 05 mar. 2024.

CHALEZQUER, Charo Sábada. SALA, Xavier Bringué. **A Geração Interativa na Ibero-América**: crianças e adolescentes diante das telas. Faculdade de Comunicação, Universidade de Navarra, Espanha, 2009.

CONSUTOR JURÍDICO. **PF deleta provas de ação penal e STJ anula interceptações**. 25 de fevereiro de 2014. Disponível em: https://www.conjur.com.br/2014-fev-25/pf-deleta-provas-acao-penal-stj-anula-grampos-telefone-mail. Acesso em: 20 mar. 2024.

COSTA, Ana Maria Nicolaci da. **Na malha da rede:** Os impactos íntimos da internet. Rio de Janeiro: Campus, 1998.

CRUZ, Paulo Márcio. BODNAR, Zenildo. **A transnacionalidade e a emergência do Estado e do direito transnacionais**. In Revista Eletrônica do CEJUR, V. I., n. 04, 2009.

DESLANDES, Maria; ARANTES, Álisson. A extensão universitária como meio de transformação social e profissional. In: Sinapse Múltipla, v. 6, n. 2, p. 179-183, 2017.

DUARTE NETO, Júlio Gomes. O Direito Penal simbólico, o Direito Penal mínimo e a concretização do garantismo penal. In: Âmbito Jurídico, Rio Grande, XII, n. 66, jul 2009. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/o-direito-penal-simbolico-o-direito-penal-minimo-e-a-concretizacao-do-garantismo-penal/. Acesso em: 8 mar. 2024.

FERREIRA, Ivette Senise. **A criminalidade informática.** In Direito & internet: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no Meio Ambiente Digital**. 2. ed. São Paulo: Saraiva, 2016.

FURLANETO NETO; GUIMARÃES, José. Crimes na Internet: Elementos para uma Reflexão Sobre a Ética Informacional. **Revista CEJ**. Brasília, n. 20, p. 69, jan./mar. 2003. Disponível em: <https://egov.ufsc.br/portal/conteudo/crimes-na-internet-elementos-para-uma-reflex%C3%A3o-sobre-%C3%A9tica-informacional-0. Acesso em: 13 mar. 2024.

GARCIA, Flúvio Cardinelle Oliveira. **Limites espaciais da jurisdição penal brasileira.** 2007. Dissertação (Mestrado em Direito Processual Penal), Pontifícia Universidade Católica de São Paulo, São Paulo, 2007.

GRANATO, Fernanda Rosa de Paiva. **A influência do discurso midiático e do clamor popular na recente produção legislativa penal brasileira**: os delitos eletrônicos e a Lei 12.737/12 (Lei Carolina Dieckmann). Disponível em: https://repositorio.ufjf.br/jspui/handle/ufjf/5778. Acesso em: 04 mar. 2024.

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

GRECO, Rogério. **Curso de Direito Penal**: introdução à teoria Geral da parte especial. Crimes contra a pessoa. 9. ed. Niterói: Impetus, 2012. v. 2.

HASSEMER, Winfried. Preservação do ambiente através do Direito Penal. **Revista**

Brasileira de Ciências Criminais, São Paulo, v. 6, n. 22, p. 26-35, abr./jun. 1998.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. São Paulo: Juarez de Oliveira, 2004.

KENSKI, Vani Moreira. **Tecnologias e ensino presencial e a distância**. 2 ed. São Paulo: Papirus, 2003.

LEMOS, André. Palestra: Cibercultura. 2003. Disponível em: http://www.facom.ufba.br/ciberpesquisa. Acesso em: 05 mar. 2024.

LOPES JR., Aury. **Direito Processual Penal**. 9. ed. São Paulo: Saraiva, 2012.

LOPES JR., Aury. **Direito Processual Penal e sua conformidade constitucional**. 8. ed. Rio de Janeiro: Lumen Juris, 2011. v. 1.

LOPES, Maurício Antonio Ribeiro. **Princípio da Insignificância no direito penal**. São Paulo: Revista dos Tribunais. 2000.

MACIEL, Rafael Fernandes. Marco civil da internet: o porquê, para o quê e omissões. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 17, n. 3333, 16 ago. 2012. Disponível em: https://jus.com.br/artigos/22433. Acesso em: 04 mar. 2024.

MALAQUIAS, Roberto Darós. **Crime Cibernético e prova**: A investigação Criminal em Busca da Verdade. 2. ed. Curitiba: Juruá, 2015.

MEDEIROS, Assis. **Hackers**: entre a ética e a criminalização. Florianópolis: Visual Books, 2002.

MEZZAROBA, Orides; MONTEIRO, Claudia Servilha. **Manual de Metodologia da pesquisa em Direito**. São Paulo: Saraiva, 2003.

MINAS GERAIS, **Superior Tribunal Militar.** Rcrimfo n. 6546 MG 1999.01.006546-1, Relator: Carlos Alberto Marques Soares. Data de Julgamento: 20 abr.1999, Data da Publicação: 16 jun. 1999, v. 02508-99 Veículo DJ. Disponível em: https://stm.jusbrasil.com.br/jurisprudencia/950723/recurso-criminal-fo-rcrimfo-6546-mg-199901006546-1. Acesso em: 08 mar. 2024.

MIRABETE, Julio Fabbrini. **Manual do Direito Penal**: Parte Geral. 24. ed. São Paulo: Atlas, 2008.

MOTTA, Sérgio, 1996, “Comitê gestor”. **Folha de São Paulo**, São Paulo, 16 jun. 1996. Disponível em: https://www.cg.org.br/infoteca/artigos/artigo8.htm. Acesso em: 10 abr. 2024.

MOLES, Ramón J. **Território, tempo y estrutura del ciberespacio**. In: derecho y control em Internet. España: Ariel Derecho, 2000.

MONTEIRO NETO, João. A. **Aspectos Constitucionais e Legais do Crime Eletrônico.** Fortaleza: Atlas, 2008.

NELLAS, Gabriel Cesar Zaccaria de. **Crimes na internet**. São Paulo: Juarez de Oliveira, 2004.

NIETZSCHE, Friedrich. A gaia ciência. Trad. Paulo César de Souza São Paulo: Companhia das Letras, 2009.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 17. ed. Rio de Janeiro: 2017.

NUCCI, Guilherme de Souza. **Direito Penal**. 3. ed. São Paulo: RT, 2007.

NUCCI, Guilherme de Souza. **Manual de direito penal**. 6. ed. São Paulo: Revista dos Tribunais, 2009.

PAESANI, Liliana Minardi. **Direito e Internet**. 6. ed. São Paulo: Atlas, 2013.

PEREIRA, Maria de Assunção do Vale. **Textos de direito internacional.** 2. ed. Coimbra: Coimbra Editora, 2013.

PINHEIRO, Patrícia Peck. **Regulamentação da Web**. Cadernos Adenauer XV, Rio de Janeiro, n. 4, p. 33-44, out/2014. Disponível em: http://www.kas.de/wf/doc/16471-1442-5-30.pdf. Acesso em: 21 mar. 2024.

POLEGATTI, B. C.; KAZMIERCZAK, L. F. **Crimes Cibernéticos: O Desafio do Direito Penal na Era Digital.** Ourinhos, 2012.

RAMOS, Hélio. Revista **Consultor Jurídico**, São Paulo. Crime de invasão de dispositivo informático não é crime impossível. 16 de novembro de 2013. Disponível em: https://www.conjur.com.br/2013-nov-16/helio-junior-invasao-dispositivo-informatico-nao-crime-impossivel. Acesso em: 20 abr. 2024.

RAZZOUK, Denise. **Dependência da Internet: uma nova categoria diagnóstica?** Disponível em: http://www.polbr.med.br/ano98/dpnet.php. Acesso em: 28 mar. 2024.

RECUERO, Raquel. Redes sociais. Para entender a internet: noções, práticas e desafios da comunicação em rede, organizado por SPYER. 2009. Disponível em: http://forumeja.org.br/sites/forumeja.org.br/files/para_entender_a_internet.pdf. Acesso em: 27 mar. 2024.

REINALDO FILHO, Demócrito. A pornografia infantil virtual e as dificuldades para combatê-la: o caso do “Second Life”. **Revista IOB Direito Penal e Processual Penal**. Porto Alegre, v. 8, n. 47, p. 7-15, dez/jan. 2008.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

ROSA, Fabrízio. **Crimes de Informática**. 2. ed. Campinas: BookSeller, 2005.

SIQUEIRA, Marcela, et al. **Crimes Virtuais e a Legislação Brasileira**. Disponível em: https://core.ac.uk/download/pdf/229767447.pdf. Acesso em 08 abr. 2024.

SILVA, José Afonso da. **Comentário Contextual à Constituição**. São Paulo: Malheiros, 2006.

SOUZA NETO, P. A. de. **Crimes de Informática.** Itajaí: Univali, 2009.

SYDOW, Spencer Toth. Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática. 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/pt-br.php. Acesso em: 20 mar. 2024.

TOMAÉL, Maria Inês; ALCARÁ, Adriana; CHIARA, Ivone. **Das Redes Sociais a Inovação**. Brasilia: Revista – Ci, Inf, v. 34 n. 2, p. 93-104, maio/ago, 2005.

VASCONCELOS, Fernando Antônio de. **Internet**: responsabilidade do provedor pelos danos praticados. Curitiba: Juruá, 2003.

VEDOVATE, Ligia. **Contratos Eletrônicos**. In: Revista Intertemas, v. 10, n. 10, Presidente Prudente-SP, 2005.