FUNDAÇÃO EDUCACIONAL MACHADO DE ASSIS
FACULDADES INTEGRADAS MACHADO DE ASSIS
CURSO DE DIREITO

PIERO ARON ROEHRS DEMO

CRIMES CIBERNÉTICOS
TRABALHO DE CURSO

Santa Rosa
2019

PIERO ARON ROEHRS DEMO

CRIMES CIBERNÉTICOS
TRABALHO DE CURSO

Monografia apresentada às Faculdades Integradas Machado de Assis, como requisito parcial para obtenção do Título de Bacharel em Direito.

Orientador: Prof. Rafael Lago Salapata

Santa Rosa
2019

PIERO ARON ROEHRS DEMO

CRIMES CIBERNÉTICOS
TRABALHO DE CURSO

Monografia apresentada às Faculdades Integradas Machado de Assis, como requisito parcial para obtenção do Título de Bacharel em Direito.

Banca Examinadora

_____
Prof. Me. Rafael Lago Salapata – Orientador

_____
Prof. (titulação e nome)

_____
Prof. (titulação e nome)

Santa Rosa, __ de dezembro de 2019.

DEDICATÓRIA

Dedico este trabalho monográfico à minha família, que sempre me apoiou ao longo de toda a minha trajetória acadêmica.

AGRADECIMENTOS

Aos meus pais pelo apoio e compreensão nesta jornada, por sempre acreditarem na minha capacidade e nos meus sonhos.

A todos os professores pelos ensinamentos e pelo auxílio nessa jornada acadêmica. Faço um agradecimento em especial ao Orientador Prof. Rafael Lago Salapata, que possuo uma imensa admiração, pela excelente orientação oferecida, e por sempre ter se empenhado no desenvolvimento da presente Monografia.

As conquistas dependem de 50% de inspiração, criatividade e sonhos, e 50% de disciplina, trabalho árduo e determinação. São duas pernas que devem caminhar juntas.

Augusto Cury

RESUMO

O tema deste projeto de pesquisa envolve crimes cibernéticos. Delimitou-se a temática de estudo enfatizando os aspectos dogmáticos mais importantes de tais espécies de delito e analisando os mecanismos de combate aos crimes cibernéticos previstos no sistema penal brasileiro contemporâneo. Considerando-se que se vive em um mundo globalizado, em que os meios de comunicação e entretenimento estão encurtando distâncias entre pessoas e mesclando culturas, problematiza-se em torno das melhores formas de tipificar, investigar e punir condutas relacionadas com a atividade cibernética. O presente estudo tem por objetivo examinar uma possível deficiência estatal na tipificação criminal de condutas graves praticadas no ambiente cibernético, situação que acaba gerando sérios problemas no atual ambiente social brasileiro e resultando punição insuficiente dos transgressores da norma penal. Trata-se de uma pesquisa de natureza hermenêutica, que se desenvolveu especialmente por meio de consulta bibliográfica, exame de artigos científicos e da legislação. Quanto ao tratamento dos dados, a pesquisa foi qualitativa, com método de abordagem hipotético-dedutivo. O trabalho é dividido em três capítulos: No primeiro capítulo, traça-se uma análise crítica sobre o surgimento e desenvolvimento da *internet*, bem como os reflexos por ela produzidos nas relações sociais e no próprio Direito. No segundo capítulo, analisam-se os crimes cibernéticos no Brasil contemporâneo, a partir de um enfoque dogmático e analítico. No terceiro capítulo, são examinados os procedimentos investigatórios aplicáveis a tais espécies de delitos, inclusive no âmbito transnacional. Ao final da pesquisa, comprovou-se a hipótese inicialmente levantada, no sentido de que, no ambiente social brasileiro, dificuldades de tipificação específica de crimes cibernéticos geram uma deficiência de punibilidade. Mostra-se necessário, assim, criar mecanismos técnicos e legais para que, em ambiente cibernético, bens jurídicos relevantes à sociedade sejam adequadamente tutelados pela norma penal, tanto no que se refere ao aperfeiçoamento de meios investigatórios, quanto no que toca à própria aplicação da lei.

Palavras-chave: Direito Penal - crimes cibernéticos – *internet* - investigação policial.

ABSTRACT

.

The theme of this research project involves cybercrime. The theme of the study was delimited by emphasizing the most important dogmatic aspects of such species of crime and analyzing the mechanisms for combating cybercrime foreseen in the contemporary Brazilian criminal justice system. Considering that we live in a globalized world, in which the media and entertainment are shortening distances between people and mixing cultures, it is problematized around the best ways to typify, investigate and punish behaviors related to cybernetic activity. The present study aims to examine a possible state deficiency in the criminal classification of serious conduct practiced in the cyber environment, a situation that ends up generating serious problems in the current Brazilian social environment and resulting in insufficient punishment of offenders of the criminal law. This is a hermeneutic research, which was developed especially through bibliographic consultation, examination of scientific articles and legislation. Regarding data treatment, the research was qualitative, with a hypothetical-deductive approach. The work is divided into three chapters: In the first chapter, a critical analysis on the emergence and development of the Internet is outlined, as well as the reflexes produced by it in social relations and in Law itself. In the second chapter, cybercrime in contemporary Brazil is analyzed from a dogmatic and analytical approach. The third chapter examines the investigative procedures applicable to these types of crimes, including at the transnational level. At the end of the research, the hypothesis initially raised was proved, in the sense that, in the Brazilian social environment, difficulties of specific typification of cybercrime generate a deficiency of punishability. Thus, it is necessary to create technical and legal mechanisms so that, in a cybernetic environment, legal assets relevant to society are adequately protected by criminal law, both with regard to the improvement of investigative means and with regard to the application of the law itself.

Keywords: Criminal Law – cyber crimes - *internet* - police investigation.

LISTA DE ILUSTRAÇÕES.

LISTA DE ABREVIAÇÕES, SIGLAS E SÍMBOLOS.

CF - Constituição Federal

CC - Código Civil

CP – Código Penal

CPC - Código de Processo Civil

CPP – Código de Processo Penal

STF - Supremo Tribunal Federal

STJ - Superior Tribunal de Justiça

TJRS - Tribunal de Justiça do Rio Grande do Sul

TFR - Tribunal Federal de Recursos

DL - Decreto-Lei

Nº Número

Art. Artigo

Pág. Página

§ Parágrafo

ARPA - Agência de Pesquisas e Projetos Avançados

SUMÁRIO

INTRODUÇÃO

O tema deste trabalho de conclusão de curso reside na análise dos crimes cibernéticos e de seus aspectos mais relevantes, compreendidos a partir do processo de criação da *internet,* contextualizado em um cenário de avanço comunicacional que redundou no fenômeno da globalização – este que propiciou grandes avanços à humanidade, mas que também ensejou o surgimento de novas espécies de condutas sociais desvaliosas. Pretende-se examinar, nesse passo, como a legislação brasileira se desenvolve diante dessas novas práticas criminosas, especialmente considerando-se que o ordenamento jurídico brasileiro vem se mostrando bastante deficiente no tocante à temática.

É indiscutível que a globalização tem trazido diversas vantagens para toda a sociedade mundial, podendo integrar rapidamente distantes localidades geográficas e proporcionando mais agilidade na integração social.

Sua aplicação em diversos campos da sociedade mundial, como nas áreas da cultura, política, entre outras, tornou-se muito importante e o Direito não poderia ficar de fora desses avanços. Sabe-se que o desenvolvimento global é inevitável e como todos os outros sistemas sociais, a norma deve acompanhar a evolução da sociedade.

Infelizmente, todas as facilidades oferecidas pela tecnologia vêm acompanhadas de sérios riscos para as pessoas. Sabendo-se que a identidade dos agentes não é facilmente revelada, novas espécies de condutas têm-se desenvolvendo no ambiente social, reclamando especial atenção acadêmica e institucional.

O assunto que se abordará vem se tornando de extrema relevância ao ordenamento jurídico, pois envolve relações jurídicas do cotidiano da sociedade contemporânea. E tais espécies de condutas nocivas vêm experimentando um crescimento tão significativo na sociedade atual, que reclamam respostas adequadas e eficazes dos mecanismos de combate e prevenção delituosa.

Este trabalho se realizou a partir de uma pesquisa bibliográfica, mediante levantamento de referências teóricas encontradas em livros, artigos e trabalhos científicos. Quanto ao tratamento dos dados, a pesquisa é qualitativa, pois visa

interpretar fatos em busca de solução para o problema proposto. Quanto aos fins, caracteriza-se pela formulação de hipóteses, atentando para procedimentos técnicos, documentais e bibliográficos.

Considera-se essa pesquisa muito importante para toda a comunidade jurídica, bem como, para a sociedade, tendo em vista a evolução tecnológica ocorrida nas últimas gerações. Essa transformação não trouxe consigo apenas benefícios, mas também muitos malefícios e, junto deles, novos tipos de crimes.

Como objetivo geral, o presente estudo tem por finalidade, apresentar como a deficiência estatal na tipificação criminal de condutas graves praticadas no ambiente cibernético, pode acabar gerando sérios problemas no ambiente social brasileiro e resultando na punição insuficiente dos transgressores. Como objetivos específicos, procuraram-se examinar os principais tipos de ocorrência do ilícito virtual, bem ainda os problemas relacionados com a tipificação de tal conduta, seguindo os desafios que circunstanciam a investigação e a importância, nesse contexto, da cooperação internacional.

A disposição deste trabalho está dividida em 03 (três) capítulos de desenvolvimento. O primeiro capítulo aborda o passado da *internet*, como ela foi criada e como acabou se tornando verdadeiro fenômeno da globalização. Nesse capitulo discute-se, também, os limites da liberdade de expressão, especialmente em ambiente virtual, bem como a necessidade de ponderação de seu exercício com outros direitos fundamentais, como intimidade, a honra, o patrimônio e a proteção de dados pessoais. Salienta-se, ainda, como a internet tem sido utilizada constantemente para a prática de condutas abusivas, especialmente no que toca a crimes como injúria racial, calúnia e difamação. Por fim, desenvolve-se uma pequena abordagem sobre o relacionamento entre Direito e Informática, diante da necessidade atual de interdisciplinaridade entre as duas áreas – destacando-se discussões travadas entre aqueles que defendem uma maior liberdade em ambiente virtual, sem intervenções estatais, e aqueles que sustentam a necessidade de uma maior regulamentação da área, por parte do Estado.

O segundo capítulo conceitua os tipos de crimes informáticos usualmente praticados no Brasil, passando pelo Princípio da Legalidade, ressaltando a necessidade de tipificação específica, clara e objetiva de condutas nocivas praticadas pelo computador, para que assim se possa puni-las adequadamente. Examinaram-se, por outro lado, tipos penais já em vigência relacionados ao ambiente virtual,

destacando-se a Lei 12.737/2012 e a Lei 12.964/2014. Por fim examina-se a dificuldade de firmar a competência jurisdicional para julgamento de tais condutas (Justiça Federal ou Justiça Estadual).

No último capítulo, de maneira sucinta, tendo em vista o alto grau de complexidade da investigação desses tipos de crime, abordam-se algumas técnicas e linhas investigativas usadas pela polícia especializada, culminando com a análise da relevância de procedimentos de cooperação internacional na investigação, uma vez que esses crimes usualmente envolvem condutas praticadas além das fronteiras nacionais.

1 REDE MUNDIAL E COMPUTADORES (INTERNET), LIBERDADE DE EXPRESSÃO E CYBER CRIMES

A partir do final do Século XX, a *internet* revolucionou a sociedade global, alterando sensivelmente os comportamentos humanos em um fenômeno comunicacional que ainda causa impactos profundos no modo de vida do homem contemporâneo. O sistema jurídico, em tal contexto, precisa estar em constante atualização, nem sempre acompanhando a contingência e rapidez do mundo dos fatos.

É inegável que a informação nunca esteve tão acessível, mesmo que paralelamente a este benefício tenha-se que conviver com riscos e ameaças nunca previstos em tempos remotos.

No presente capítulo desta monografia desenvolver-se-á uma introdução às origens, características e aplicabilidades da rede mundial de computadores, sob óticas históricas e culturais.

Partindo-se de tal enfoque, nesta seção serão igualmente abordadas temáticas voltadas ao estudo das relações sociais contemporâneas, bem como aos limites da liberdade de expressão em uma sociedade de informação, como a atual.

Em tal cenário, Direito e Informática se entrelaçam no desafio de normatizar a tecnologia e a inovação, em atenção a direitos humanos que devem ser protegidos em um mundo no qual intimidade, liberdade e proteção de dados se encontram constantemente ameaçados.

1.1 ASPECTOS HISTÓRICOS E CULTURAIS LIGADOS AO SURGIMENTO E DESENVOLVIMENTO DA INTERNET NO MUNDO E NO BRASILO

Com a finalidade de automatizar o cálculo de tabelas balísticas, em 1946 foi criado o primeiro computador digital, denominado ENIAC. Fabricado com funções bélicas, ele permitiu realizar cálculos balísticos de trajetória que exigissem um grande conhecimento em matemática. Embora tenha sido um computador de difícil manutenção e de grande tamanho comparado com os computadores atuais, o ENIAC foi um importante marco na história da computação (FILHO, 2007).

Sendo o meio de comunicação em massa, mais difundido na população nos últimos anos, a rede mundial de computadores (internet), dada sua facilidade de modernizar a vida das pessoas que convivem em sociedade, teve seu início em 1957.

Criada principalmente para fins exclusivamente militares, a internet era a base de apoio das comunicações feitas entre as forças de ataque norte americanas, caso sofressem uma investida inimiga, que pudesse limitar ou colocar em risco a comunicação feita pelos meios convencionais com suas tropas. Teve seu nascimento no mesmo momento que começava a guerra fria, em meados de 1960, após o fim da Segunda Guerra Mundial, onde Estados Unidos da América e a União soviética travavam uma batalha pelo comando político, econômico, tecnológico e militar de todo o mundo. (FEITOSA, 2012, p.25).

Vendo que estava se tornando extremamente impotente pela avançada qualidade de transmissão de informações dos russos, que em 1957 lançou seu primeiro satélite espacial. Os Estados Unidos, se comprometeram a levar o homem à lua e criar um sistema de defesa à prova de destruição, assim foi criada a Agência de investigação de Projetos Avançados (Advanced Research Project Agency) – ARPA que ficou responsável de desenvolver uma tecnologia superior ou igual à dos soviéticos. Fabrízio Rosa ensina:

> A fagulha que acabaria por acender a revolução da conectividade ocorreu em 1957, quando a União Soviética pôs em orbita o primeiro satélite espacial, o Sputnik: quatro meses depois, o presidente americano Dwight Eisenhower anunciava a criação de uma agencia federal norte-americana, nos moldes da NASA, conhecida como Advanced Research Projects Agency- ARPA, com a missão de pesquisar e desenvolver alta tecnologia para as forças armadas. (ROSA, 2005, p. 31).

A ARPA foi uma agência que tinha como finalidade a de desempenhar ações destinadas às pesquisas militares com cunho tecnológico em defesa do território estadunidense, e prevenir qualquer surpresa tecnológica de outros países, se tornando um importante mecanismo de uma guerra tecnológica travada com a União Soviética. (FEITOSA, 2012, p. 26)

No ano seguinte, em 1958, foi criada a National Aeronautics e Space Administration (NASA), tendo como foco a corrida espacial. Com atribuições semelhantes e fazendo parte do Departamento de Defesa americano, a NASA começou a tomar conta desse segmento de pesquisa. Por consequência, a ARPA foi

enfraquecendo, tendo assim que modificar a perspectiva de sua área de atuação, incluindo novos projetos, cujos resultados somente poderiam ser avaliados em longo prazo. Além disso, a ARPA começou a desenvolver parcerias com instituições de ensino, tornando sua atuação mais técnica e cientifica. Sendo assim, seu foco foi mudando, passando a investir em assuntos que até então não eram adequadamente explorados, como a pesquisa computacional. (ABREU, 2009, p .02).

Com o passar dos anos houve uma necessidade de construir uma rede capaz de integrar computadores que estivessem em locais distantes, de modo que, por intermédio dela, fosse permitida a comunicação de dados.

O professor Gabriel Cesar Innelas explica que:

> A partir dessa preocupação, o Departamento de Defesa dos Estados Unidos elaborou um Sistema de Telecomunicações, desenvolvido pela Agência de Projetos e Pesquisas Avançadas, a ARPA, criando assim uma rede denominada ARPAnet, que operaria através de inúmeras e pequenas redes locais, denominadas LAN (Local Area Network), que significa rede local responsável em ligar computadores num mesmo edifício, sendo instaladas em locais estratégicos por todo o País, os quais foram interligadas por meios de redes de telecomunicação geográficas, denominadas WAN (Wide Area Network), que significa rede de longo alcance, responsáveis pela conexão de computadores por todo o mundo, e assim, caso houvesse um ataque nuclear contra os Estados Unidos da América, as comunicações militares e governamentais não seriam interrompidas, podendo permanecer interligadas de forma contínua. (INELLAS, 2009, p.1)

Assim, em 1969 foi criada a ARPANET, inicialmente interligada à Universidade da Califórnia (Los Angeles e Santa Bárbara), à Universidade de Stanford (Santa Cruz) e à Universidade de Utah (Salt Lake City). (UMBATH, 1987).

Segundo, António Cruz:

> Esta agência criou uma rede experimental chamada ARPANET, que utilizava uma tecnologia chamada ‘packet switching’ (troca de pacotes) para o transporte de informação, tecnologia está que é a base do que conhecemos por internet. Nessa altura, apenas organismos militares e grandes universidades estavam ligados entre si pela Arpanet, mas a rede foi crescendo, e com o tempo foi permitida a entrada de empresas. (CRUZ, 2011)

A ARPANET continuou crescendo e levando em conta que a guerra fria já estava chegando ao seu final, os Estados Unidos resolveram expor ao mundo o que a agência havia desenvolvido para aumentar ainda mais o incremento tecnológico de seu país e protegendo seu futuro.

No ano de 1973, realizou-se a primeira conexão internacional, a qual interligou a Inglaterra e a Noruega. Na década de 1980, a rede se expandiu pelos Estados Unidos e permitiu a interligação entre universidades, órgãos militares e governo. Finalmente, para que ocorresse o grande salto da utilização da internet foi essencial a criação do protocolo World Wide Web (WWW) e do Hypertext Markup Language (HTML), tornando popular o uso de páginas web e transformando a internet em uma rede mundial de computadores. (KUROSE, ROSS, 2010).

No Brasil a introdução da internet se deu de forma lenta e progressiva. Uma série de ações dos governos federais que passaram pelo poder, deram início ao desenvolvimento das telecomunicações no Brasil, já que o país necessitava um Sistema Nacional de Telecomunicações que buscasse facilitar o transporte de informações em todo território nacional. (FEITOSA, 2012, p. 30).

A almejada integração nacional de uma rede de telecomunicações de grande alcance iniciou-se pouco antes do primeiro governo militar tomar o poder, porém os militares logo compreenderam a importância de uma rede de comunicações que facilitasse e contribuísse para a proteção do país.

Como resume Dias e Cornils:

> No início do governo de Jânio Quadros (janeiro a agosto de 1961), foi criado o Conselho Nacional de Telecomunicações (CONTEL) e, em seguida, no governo de João Goulart (setembro de 1961 a março de 1964), foi aprovado e regulamentado o Código Brasileiro de Telecomunicações (CBT), inspirado nos estudos conduzidos pelo Estado Maior das Forças Armadas (EMFA). (DIAS, CORNILS, 2004).

Até essa época o setor de telecomunicações era dominado por empresas privadas, sendo ele de baixíssima qualidade, também beneficiava somente parte da população, deixando as regiões mais distantes e a população mais carente desprovida dessa tecnologia. Em 1964 o governo militar, promoveu a implantação do Código Brasileiro de Telecomunicações (CBT), regulamentado pela Lei nº 4.117, de 27 de agosto de 1962.

Em 1961, o Instituto Brasileiro de Geografia e Estatística (IBGE) passou a utilizar o computador UNIVAC (Universal Automatic Computer). Sequencialmente, em 1964, foi criado o Centro Eletrônico de Processamento de Dados do Estado do Paraná, empresa pública com finalidade e funções relacionadas com a informática, como desenvolvimento e consultoria em tecnologia da informação (TI), redundando crescimento da internet no Brasil. (SILVA, 2016).

Com o surgimento do Ministério das Comunicações, surgiram também normas operacionais do Sistema Nacional de Telecomunicações (SNT), sendo que então as telecomunicações ficariam sob o controle das empresas estatais. Já a radiodifusão ficaria a cargo da iniciativa privada. (TELEBRASIL, 2004, p.14).

No início da década setenta, o aumento do uso de equipamentos eletrônicos fez com que o Ministério das Comunicações começasse a ter outras preocupações, como à da transmissão eletrônica de dados. Com as limitações das redes clássicas, os responsáveis pelos órgãos de administração do setor de telecomunicação de vários países providenciaram a instalação de novas redes para a transmissão de dados. (BENAKOUCHE, 1997, p. 125).

Todo esse processo de introdução ao uso de computadores e telecomunicações acabou na criação do primeiro computador brasileiro, desenvolvido pela Universidade Federal de São Paulo (USP). Em 1979, além disso, foi criada a Secretaria Especial de Informática, vinculada ao Conselho de Segurança Nacional, com a finalidade de assessorar na formulação da Política Nacional de Informática (PNI) e coordenar sua execução, como órgão superior de orientação, planejamento, supervisão e fiscalização, tendo em vista, especialmente, o desenvolvimento científico e tecnológico no setor.

Em 1984, o poder executivo deixou de ter competência sobre a política para o setor de informática, assim as entidades acadêmicas entraram para o debate, pois viam nessa tecnologia um importante passo para a capacitação de seus membros. (FEITOSA, 2012, p. 33).

Assim depois de um intenso debate público, foi aprovado pelo Congresso Nacional, a chamada Lei de Informática – Lei nº 7.232 de 29 de outubro de 1984, que "normatizou os princípios básicos de capacitação tecnológica e reserva de mercado e democratizou o processo decisório através da criação do Conselho Nacional de Informática e Automação" (TIGRE, 1987, p. 33)

Outro passo importante para consolidação da *internet* no Brasil foi a conexão com à Bitnet, que transportava informações da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), do Laboratório Nacional de Computação Cientifica (LNCC) e da Universidade Federal do Rio de Janeiro (UFRJ), em 1988. Em 1992 foi extinta a Secretaria de Especial de Informática, treze anos depois de sua criação, e para encampar suas atribuições foi criada a Secretaria de Política de Informática. Também nesse mesmo ano foi implementada no Brasil a primeira rede conectada à internet, que interligava as principais universidades brasileiras. (WEND, NOGUEIRA, 2012).

A internet, finalmente, foi disponibilizada comercialmente no Brasil em 1995, ano em que também ocorreu a criação do Comitê Gestor da Internet no Brasil, com a finalidade de coordenar e integrar todas as iniciativas de serviços de internet no país, com qualidade técnica, inovação e disseminação de serviços ofertados. (ADACHI, 2009, p. 37).

1.2 RELAÇÕES SOCIAS NA SOCIEDADE DE INFORMAÇÃO E LIBERDADE DE EXPRESSÃO

O acesso à *internet* e a consequente democratização da comunicação criaram condições para a ocorrência de um fenômeno que, nas últimas décadas, alcançou proporções globais: uma verdadeira “ressignificação das relações sociais, das relações de poder e principalmente da maneira das pessoas se comunicarem” (MOLINA, 2013).

Foi o que já observara, anteriormente, Lèvi, ao sustentar que transformações experimentadas por novas tecnologias comunicacionais acabaram por influenciar o homem a desenvolver novas formas de pensar (2010), exatamente na linha do que leciona Castells ao definir que a sociedade interligada em redes estabeleceu verdadeira *autocomunicação de massas*, esta, capitaneada, justamente, pela internet (2009).

Em tal contexto, Leonardo Valles Bento expõe que a liberdade de expressão está estruturalmente relacionada com a democracia. Um direito de caráter individual e difuso, pois permite ao indivíduo expressar-se publicamente e o outro envolve outros direitos do cidadão, como o acesso a informação, o direito de reunião e associação (2014).

Quanto à aplicação dos princípios relativos à liberdade de expressão na internet, Bento os considera essenciais para o exercício da liberdade individual. Entretanto, ele finaliza dizendo que qualquer limitação a esse direito deve ser imposta com o alvo de proteger outros direitos fundamentais, obedecendo aos requisitos supramencionados, e em acordo com os preceitos do devido processo legal. (BENTO, 2014),

Assim sendo, a internet se tornou um canal para expressão das ideias e da livre circulação de informações. Porém como nenhum direito é absoluto, a liberdade de expressão pode ser restringida de forma legítima, especialmente quando houver dano ou risco de dano à segurança coletiva (interesse público acima do interesse privado). (ADRIANO ROCHA, 2017, p 30).

Nesse cenário, deve-se contextualizar o objeto de pesquisa, confrontando os limites da liberdade de expressão frente ao uso indevido da internet para cometimento de crimes cibernéticos.

Com o uso irresponsável da internet, nessa sociedade de informações em que se vive, além de riscos à segurança pessoal e comercial, percebe-se a vulnerabilidade à honra e imagem, além da possibilidade de criação de margem para a disseminação de discursos de ódio contra grupos minoritários, alvos de preconceito. (ADRIANO ROCHA, 2017, p. 15).

A Constituição Federal da República Federativa do Brasil deixa claro o direito à livre manifestação do pensamento como garantia individual, porém ela veda o anonimato, isto é, desde que se identifique o responsável - para preservar essencialmente o direito ao contraditório e a eventual reparação de danos - qualquer pessoa tem o direito de expressar suas opiniões.

Pedro Lenza explica:

> A constituição assegurou a liberdade de manifestação do pensamento, vedado anonimato. Caso durante a manifestação do pensamento se cause dano material, moral ou à imagem, assegura-se o direito de reposta, proporcional o agravo, além da indenização. (lenza, 2012, p.981)

É muito fácil se esconder atrás da cortina do anonimato, assim, a identificação raramente acontece pela internet. Além disso, não há grande preocupação dos usuários em confirmar a autoria ou veracidade das informações que estão sendo

disseminadas em ambiente virtual, o que possibilita a perpetuação de práticas delituosas.

Fica claro que a lei permite ao indivíduo manifestar seus pensamentos livremente, mas faz uma ressalva: aquele que exercer seu direito arbitrariamente ou exceder-se no exercício do mesmo, violando direito alheio, estará passível de sanção estatal. Essa limitação constitucional impede os excessos que possam causar dano à integridade moral ou até mesmo psicológica de outro individuo, direitos igualmente protegidos pela Constituição Federal.

Na sociedade contemporânea, por conseguinte, fica claro que o Estado tem-se obrigado a intervir na liberdade dos indivíduos, utilizando a tutela penal para reprimir as condutas danosas praticadas em ambiente virtual.

1.3 DIREITO E INFORMÁTICA

Para que se possa conviver em sociedade, a estabilidade social, acaba se tornando um fator preponderante, pois é ela que permite a convivência pacífica de uns com os outros. E sendo uma das bases do progresso da mesma, o Direito favorece o relacionamento de grupos da sociedade. (NADER, 2004, p.25).

Gerando uma insegurança jurídica, a instabilidade decorrente do aumento da violência e da impunidade incute nas pessoas sentimento de descrença no Estado para punir, levando a própria sociedade a se organizar, discutindo a necessidade de normatização de novos direitos, como os direitos informáticos.

Na balança deve-se colocar a relação e as influências recíprocas entre a sociedade e o direito, analisando uma diferença entre o direito e o fator social. O direito, sendo conservador, consegue abrigar somente parte das relações sociais. Já o fator social é mais dinâmico, em se tratando dessas relações. “Deve haver um aperfeiçoamento do Direito frente a evolução da sociedade, se não por via legislativa, ao menos por via judicial jurisprudencial, pautando-se na democracia e no respeito à dignidade do ser humano”. (TEYMISSO, 2017, p. 22).

No modelo atual da sociedade de informação, esta deveria estar em consonância com a evolução do direito. Mas tal modelo, a rigor, pode passar despercebido, pois as facilidades estão tão em evidência no cotidiano que não há uma percepção clara de que se vive em uma sociedade essencialmente informatizada, na

qual os dados fluem a velocidades inimagináveis, tudo influenciando valores sociais e econômicos. (LISBOA, 2016, p.10).

Em um mundo no qual as fronteiras geográficas estão sendo superadas em termos de comunicação, as fronteiras físicas deixaram de ser um entrave para o crescimento globalizado. Sendo a internet um novo meio de comunicação que interliga todo o mundo "Tal designação, além de especificar a estrutura material de comunicação digital, caracteriza também o universo de informações abrigadas e também os seres humanos que navegam nesse sistema". (LEVY, 1999, p. 16).

O Direito, sendo causa e efeito das relações sociais, por si só configura em si um fenômeno social, "pois o Direito não determina a si próprio, sendo concebido a partir de normas e princípios superiores abstratos, tendo como referência a sociedade como fenômeno social que o produz". (TEYMISSO, 2017, p. 23).

Como o Direito é a fonte instrumental de coexistência social, tem por função precípua auxiliar na manutenção da ordem, direção e solidariedade. Corresponde, portanto, ao antigo brocardo: *ubi societas, ibis jus* (onde está a sociedade, está o Direito), sendo a recíproca também verdadeira. Assim não se pode conceber qualquer forma de convivência social sem regras, e nem sociedade sem Direito (REALE, 2002, p. 02).

A partir da segunda metade do século XX, com o surgimento do fenômeno de informatização da sociedade, percebeu-se o surgimento de uma nova classe de bens, podendo ser chamados de bens informáticos, que possuem um caráter material, ou imaterial. Esses bens acabaram inserindo-se no modelo social e econômico, de modo que fica difícil conceber a sociedade atual sem a figura do computador, por exemplo. Redes sociais tornaram-se parte do cotidiano de uma forma tão acelerada que muitas vezes nem se percebe o quanto tais ferramentas podem interferir positivamente ou negativamente nas vidas dos indivíduos. (SILVA, SILVA, MORAES, 2016, p. 05).

Assim, observa-se que a Informática e o Direito acabam se relacionando mutuamente, mas para existir uma sintonia entre ambos é necessário que o Direito, em sua aplicação, seja auxiliado pela Informática e vice-versa. "O Direito Informático surge através do ponto de vista tecnológico da cibernética, que trata da relação entre Direito e Informática até o ponto de vista do conjunto de normas, doutrina e jurisprudência, que venham a regular a complexidade de relações da Informática" (PAIVA, 2011, p. 16).

Já sendo reconhecido por países mais desenvolvidos, o Direito Informático reúne certas características, como a de ser um direito mais especializado e ao mesmo tempo, interdisciplinar e universal. Esse novo ramo do Direito é uma disciplina jurídica que deve ser marcada pelos sistemas normativos contemporâneos, e que busca regulamentar as modernas tecnologias da informação (PIMENTEL, 2000. P.152).

Nos últimos anos, com o crescimento de novas tecnologias e o maior acesso à rede mundial de computadores, a informatização acabou atingindo um nível muito elevado, espalhando-se por quase todos os países do globo, passando a compor, em definitivo o modelo de produção economia do mundo.

Esse fenômeno tem influência direta no mundo jurídico, e exige a demanda de novos mecanismos para solucionar novos tipos de conflitos surgidos dessa nova era. “A internet é uma ferramenta de poder e a utilização em massa de novas tecnologias, e por isso requer uma normatização jurídica e reflexão ética” (PICON, ANTUNES, DUARTE, 2013, p.989).

A regulamentação da internet tem causado um grande número de debates na atualidade. Novas iniciativas governamentais vêm sendo implantadas ao redor do mundo com tal intuito, o que acaba por gerando intenso debate social.

Sendo o tema bastante complexo, considerando as fronteiras que pode romper, redimensionando questões sociais, econômicas, políticas e culturais de um país ou região. O debate acerca da regulamentação envolve a garantia de liberdade individual e coletiva, possibilidade de censura a manifestações e o direito à privacidade. (SEGURADO, 2011, p.46).

Quando se pensa em regulamentar a internet, podem surgir algumas problemáticas, pois uma parcela da doutrina argumenta que isso seria uma clara questão de censura por parte do Estado, o que é vedada pela Constituição brasileira, sendo um ataque à liberdade de expressão. Por outro lado, sem a regulamentação uma maior facilidade de ataques aos direitos fundamentais, além de instigação a crimes como racismo, calúnia, difamação, pornografia infantil, dentre outros. Tem-se, portanto, que a internet necessita de regras para proteção dos direitos fundamentais, mesmo sendo ela uma rede aberta que proporciona o desenvolvimento de práticas colaborativas e não-proprietárias. (SEGURADO, LIMA, AMENI, 2014, p.02)).

Atualmente com a globalização, a informação tem um caráter vital nos campos sociais, políticos e nas grandes empresas, nas quais a informação pode ser vital para se manter competitiva e estruturada. Para isso os mecanismos de proteção devem

procurar garantir essa segurança, integridade, confidencialidade de dados. Um ataque a essa informação pode causar grandes prejuízos tanto financeiramente como moralmente. Assim, como o direito constitucional brasileiro permite a apreciação do Poder Judiciário a qualquer violação ou ameaça a um direito, há a necessidade de serem criados mecanismos legislativos que auxiliem o julgador na proteção dos direitos e garantias fundamentais das pessoas que utilizam o serviço computacional virtual. (TEYMISSO, 2017, p. 26).

O Direito da Informática ou Direito da Internet teria como principal elemento a introdução da Internet. E mesmo que tenha ela causado uma revolução no mundo, ela ainda deve estar interligada com o mundo jurídico.

É importante salientar que todo esse objeto do estudo do Direito na Informática, apareceu antes do Direito relacionado com a Informática realmente existir. “Isso porque o Direito sempre deve dar resposta a uma situação de conflito, mesmo que não haja ainda nenhuma previsão legal sobre o assunto”. (CASTRO, 2014, p. 4).

Para que todo esse problema não se torne um calcanhar de Aquiles da sociedade pós-industrial, já que todo nosso cotidiano vai sendo modelado junto ao meio informático, recorre-se à proteção proporcionada pelo Direito Penal (ASCENÇÃO, 2002, p. 255).

Assim deve-se ter em mente que, nos dias atuais, não se pode conceber uma ordem jurídica na qual não exista previsão legislativa acerca das interações com a Internet. Diante disso, o sistema jurídico deve se adaptar à evolução da sociedade, uma vez que o Direito só tem real utilidade quando consegue realmente normatizar o convívio social.

Com a tecnologia evoluindo exponencialmente, tanto quantitativa quanto qualitativamente, acabou culminado no surgimento de novos conflitos entre novas tecnologias e a sociedade, junto com o surgimento de novos valores de liberdade, privacidade, censura e o grande aumento da presença de aparelhos informáticos no cotidiano das pessoas, trouxe muitos benefícios, mas também alguns malefícios. (TEYMISSO, 2017, p. 25).

Como esse conceito de informação e tecnologia já está arraigado na realidade contemporânea, e com o aparecimento cada vez maior de lacunas sociais, o direito deve procurar preenchê-las e compreenda-las. (CORREA, 2000, p. 02)

De fato, mesmo que o Direito possa parecer atrasado com relação à evolução tecnológica, deve buscar incessantemente evoluir ponto de não perder sua eficácia

social, ficando, em relação a tal aspecto, clara a necessidade de mais estudos e regulamentação acerca de crimes cometidos pelo computador ou em ambiente virtual.

No segundo capítulo da presente monografia, a partir de uma abordagem dogmática, passa-se a analisar, especificamente, os crimes cibernéticos usualmente praticados no ambiente social brasileiro.

2 CRIMES CIBERNÉTICOS CLASSIFICAÇÃO: TIPIFICAÇÃO LEGAL E COMPETÊNCIA

Neste segundo capítulo, tem-se por objetivo mostrar como são tratados no Brasil contemporâneo os crimes cibernéticos, especialmente frente ao princípio da legalidade.

A seguir, portanto, examinar-se-ão, sob uma ótica dogmática, as principais condutas tipificadas na legislação brasileira que compreendem delitos praticados em ambiente computacional virtual. Ao final, será analisada a competência jurisdicional para processamento e julgamento de crimes cibernéticos, especialmente se tais delitos devem tramitar na Justiça da Federal ou na Justiça Estadual.

2.1 PRINCÍPIO DA LEGALIDADE E CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS NO BRASIL

O Princípio da Legalidade estabelece as bases do ordenamento jurídico nacional, garantindo a dignidade da pessoa humana. Tem sua origem na limitação do poder estatal frente ao povo e sempre esteve preceituado nas constituições brasileiras. Atualmente ele se encontra previsto no art. 5º inciso XXXIX da Constituição Federal de 1988, dentre os direitos e garantias fundamentais, o qual preceitua: “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal”. Em suma, no Brasil contemporâneo nenhum cidadão comete um crime se não houver previsão legal anterior a seu respeito, não podendo ainda ser responsabilizado ou cumprir pena sem cominação legal prévia.

Sendo o primeiro grande passo para um sistema penal racional e justo, como cita Nilo Batista, esse princípio “Além de assegurar a possibilidade do prévio conhecimento dos crimes e das penas, o princípio garante que o cidadão não será submetido a coerção penal distinta daquela predisposta em lei”. (BATISTA, 2004, p.67)

Para Paulo de Souza Queiros:

> Semelhante princípio atende, pois, a uma necessidade de segurança jurídica e de controle do exercício do jus puniendi, de modo a coibir possíveis abusos à liberdade individual por parte do titular desse poder (o Estado). Consiste, portanto, constitucionalmente, uma poderosa garantia política para o cidadão,

> expressiva do imperium da lei, da supremacia do Poder Legislativo – e da soberania popular – sobre os outros poderes do Estado, de legalidade da atuação administrativa e da escrupulosa salvaguardados direito e liberdade individuais. (QUEIROZ, 2005, p. 26).

O Direito Penal busca construir respostas rápidas e satisfatórias aos conflitos sociais, erguendo bases concretas para compor a segurança jurídica daqueles que estão envoltos pelo sistema jurídico atual.

A tipificação busca classificar condutas humanas em normas penais proibitivas, ou para alguns doutrinadores, em normas negativas, incriminando todos os fatos que possam estar desviados de uma conduta aceita socialmente. Para aqueles que transgridam as normas, impõe-se uma sanção penal, que é geralmente a pena privativa de liberdade. A tipificação penal ainda segue sendo um incansável objeto de estudo por parte dos maiores penalistas brasileiros. (FONSECA, 2002)

Até 2012, o Brasil não possuía nenhuma previsão legal para punir algumas condutas já tipificadas em outros países, somente com o advento da Lei 12.737/2012 ele pode combater algumas espécies de crimes que eram cometidos através da internet. A referida Lei adicionou os artigos 154-A e 154-B e também nova redação aos artigos 266 e 298 do Código Penal Brasileiro. Assim os doutrinadores conseguiram extinguir algumas lacunas do Direito Penal brasileiro, tipificando condutas de pessoas que agem na internet. (DIKSON DELGADO, 2016, p 17)

Já a nomenclatura de Crimes Cibernéticos ou Crimes Informáticos ainda causa muita discussão no meio jurídico e, como se está tratando de uma doutrina em formação, o entendimento não encontrou pacificação. São identificados de diversas formas, porém não existe uma nomenclatura sedimentada acerca de seu conceito. Cumpre, entretanto, destacar que, independentemente do nome atribuído a eles, sempre envolvem o uso de dispositivos informáticos para perpetração da conduta delituosa. (DA SILVA, 2015, p 42).

Fabrizio Rosa conceitua o crime cibernético como sendo:

> (...)“A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar. O ‘Crime de Informática’ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados,

> compilados, transmissíveis ou em transmissão; 3. Assim, o 'Crime de Informática' pressupõe dos elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública. (ROSA, 2002, p. 53)

A internet trouxe um nível de tecnologia de informação jamais imaginado por pessoas que viveram em tempos antigos. É ela atualmente utilizada para inúmeras finalidades, inclusive para negociações comerciais, relacionamentos interpessoais, diversão, trabalho e, em alguns casos, cometimento de atividades ilícitas.

Sobre o assunto, Wendt e Nogueira concordam que "a utilização da internet tem sofrido um aumento exponencial a cada ano que passa, muito em virtude da evolução tecnológica e do barateamento dos computadores e dispositivos móveis de acesso à rede mundial". (WENDT, NOGUEIRA, 2012, p.14).

Infelizmente, esse aumento também trouxe sérios riscos paras os usuários. E com a facilidade de ocultar a sua identidade, atrai diversos tipos de criminosos, circunstância agravada por uma sensação de impunidade relacionada aos ilícitos que ocorrem no ambiente virtual.

No combate aos crimes cibernéticos no âmbito penal, a investigação, perícia e principalmente a legislação, têm reflexos importantes no adequado andamento do processo criminal – e, como consequência, na punição dos indivíduos que praticam tais espécies de conduta, lesando bens jurídicos tutelados pela norma penal. Esses mecanismos também acabam se tornando peça chave, portanto, para inibição de novas condutas delituosas. Além de tudo, crimes cibernéticos costumam interferir significativamente no cotidiano das pessoas, ficando claro que a confiança advinda de uma prevenção e repressão eficaz é ponto central para evitar riscos de roubo, fraude e uso indevido de informações cibernéticas. (ABREU, 2001, p.12).

Algumas dessas condutas ainda se encontram sem a devida regulamentação legal, tornando difícil a punição e a identificação dos agentes responsáveis, e com o avanço tecnológico fica visível o atraso entre as normas do Código Penal brasileiro e

o momento no qual se vive, tornando árdua a tarefa do operador do direito, de conciliar os institutos penais com a constante mudança de tecnologia. (PACHECO, 2011, P. 06).

Com a evolução tecnológica, novas formas de conduta ilícita ou delitiva vão surgindo, e classificações acabam se tornando obsoletas. Entretendo há a algumas classificações doutrinárias que se revelam consistentes. Crimes cibernéticos próprios e impróprios; ações prejudiciais atípicas; crimes cibernéticos abertos; crimes exclusivamente cibernéticos são alguns exemplos de terminologia aplicável à temática, que serão examinadas a seguir.

Crimes cibernéticos *impróprios* são tipos de crime realizados com o uso do computador, nos quais a máquina se torna o instrumento utilizado para a prática da conduta ilícita que afeta o bem jurídico da vítima. Essas condutas há muito já estão tipificadas no ordenamento brasileiro, porém são atualmente realizadas também com a utilização do computador. Por exemplo, o crime de ameaça que pode ser cometido tanto por redes sociais, como verbalmente entre duas pessoas. Para Damásio de Jesus:

> (...) 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, 2016)

Já os crimes cibernéticos *próprios* são aqueles em que o sujeito utiliza necessariamente o computador como objeto e meio para sua execução. Aqui se enquadra não só a invasão de dados não autorizados, mas toda a interferência ilícita - seja no intuído de modificar, inserir ou alterar - que atinja diretamente o *software* ou *hardware* do computador e só podem ser realizados por meio do computador.

A invasão de dado não autorizados se refere ao acesso a dispositivo computacional alheio, não autorizado, mediante rompimento de segurança, com o intuito de alteração ou a destruição de dados.

Nesta linha Damásio de Jesus também escreve:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados. Neles, a informática por computador e se realizem ou se consumem também em meio eletrônico (segurança dos sistemas, titularidade das informações e

> integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado. (DAMÁSIO, 2016).

A Lei 12/737/12 tipificou criminalmente várias condutas que podem ser consideradas crimes próprios, cuja previsão legal não existia no ordenamento jurídico brasileiro, como a invasão de dispositivo informáticos, a interrupção ou perturbação dos serviços de *internet*.

Já para os Delegados de Polícia Emerson Wendt e Higor Vinícios Nogueira Jorge, "crimes cibernéticos" são aqueles delitos praticados contra ou por intermédio de computadores, e para fins didáticos, os doutrinadores apresentam uma classificação para as denominadas "condutas indevidas praticas por computador".

Essas "condutas indevidas praticas por computadores", são divididas, segundo eles, em "crimes cibernéticos" e "ações prejudiciais atípicas", sendo que os "crimes cibernéticos" dividem-se em "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos". (WENDT, NOGUEIRA, 2012, p.18)

As "ações prejudiciais atípicas são aquelas ações praticadas" com o envolvimento ou por meio da rede mundial de computadores, que geram danos e que podem causar algum transtorno ou prejuízo para a vítima, mas que não tem previsão legal, ou seja, o criminoso causa algum problema para a vítima e como não há previsão legal, não pode ser punido na esfera criminal. Por exemplo, o indivíduo que produz um vírus ou que invade o computador de outra pessoa para conseguir informações ou algum histórico de pesquisa na internet não poderá ser responsabilizado na esfera penal, pois esses fatos não são criminosos. Por outro lado, ele pode ser responsabilizado na esfera cível, como pagar alguma indenização em virtude dos danos materiais ou morais produzidos. Essa questão só poderá ser resolvida com a aprovação de normas capazes de criar nova tipificação penal para tal conduta. ". (WENDT, NOGUEIRA, 2012, p.14).

Por outro lado, os chamados *"crimes cibernéticos"* são divididos em *"crimes exclusivamente cibernéticos"* e *"crimes cibernéticos abertos"*. Os crimes exclusivamente cibernéticos são aqueles crimes cometidos exclusivamente pelo computador ou por outro meio tecnológico com acesso à internet, crimes que não poderiam ser cometidos sem o criminoso ter acesso a esses dispositivos. Aqui pode-se usar como exemplo o crime de aliciamento de crianças praticado via internet, redes sociais, sala de bato papos, previsto no art. 241-D do Estatuto da Criança e do Adolescente (Lei 8069/90)

> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso. Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Nas mesmas penas incorre quem: I – Facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso. II – Pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.

Seguindo a mesma linha os crimes cibernéticos abertos, são aqueles crimes praticados da forma tradicional, e que também podem ser praticados através do computador ou seja, o computador é só um meio para prática delituosa, são crimes que já possuem tipificação. Aqui podemos usar como exemplo crimes de ameaça, estelionato, crimes contra honra, racismo, crimes que podem ou não ser praticados com o uso do computador.

Veja a ilustração a seguir para ficar mais claro:

Ilustração 1: Classificação Crimes Cibernéticos
Fonte: Crimes Cibernéticos – Ameaças e procedimentos de investigação – (Emerson Wendt, Higor Vinicios Nogueira Jorge, 2012).

Abaixo uma apresentação com essa classificação e com exemplos de cada um desses crimes.

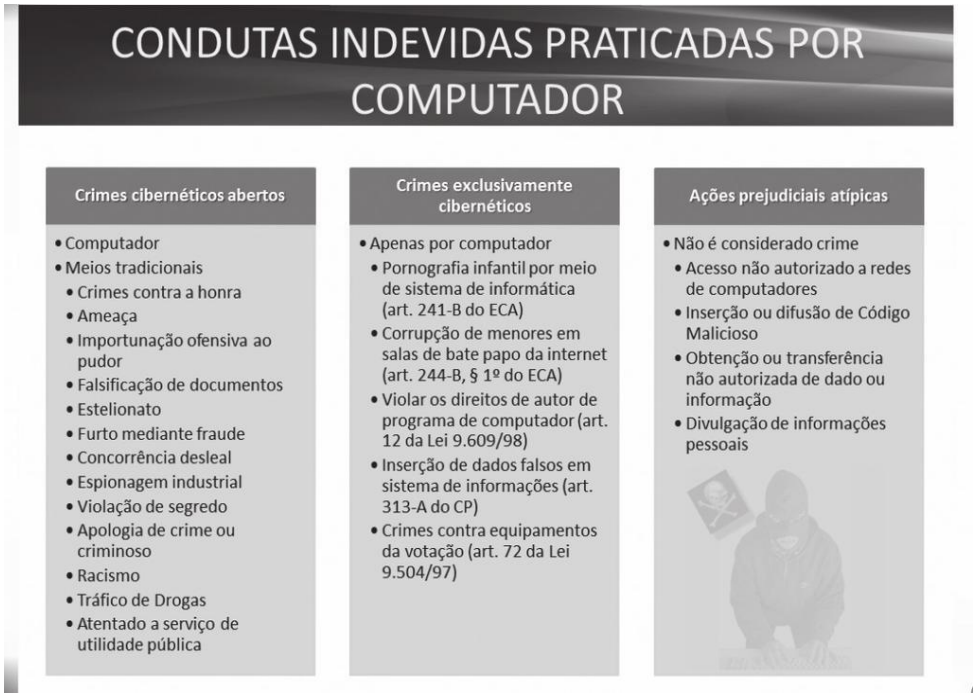

Ilustração 2: Conduta Indevidas Praticadas por Computador
Fonte: Crimes Cibernéticos – Ameaças e procedimentos de investigação – (Emerson Wendt, Higor Vinicios Nogueira Jorge, 2012).

2.2 DA LEI CAROLINA DIECKMANN E MARCO CIVIL DA INTERNET (PERPASSANDO PELA LEI GERAL DE PROTEÇÃO DE DADOS DO USUÁRIO E PELA LEI DE COMBATE A IMPORTUNAÇÃO SEXUAL)

No ano de 2012, a exposição indevida de imagens pessoais da conhecida atriz brasileira Carolina Dieckmann promoveu intensa discussão social, da qual redundou a aprovação e sanção da Lei nº 12.735/12 (esta que, então, passou a ser informalmente conhecida, justamente, como Lei Carolina Dieckmann), diploma que tipificou condutas realizadas mediante uso de sistema eletrônico, digital ou similar, praticadas contra sistemas informatizados. Carolina, à época, teve seu computador invadido e a divulgação das referidas imagens ocorreu por ela não ter aceitado entregar a terceiro a quantia de R$ 10.000,00 (dez mil reais) - então configurando, além de interceptação indevida de *e-mail*, o crime de extorsão.

A nova legislação acrescentou os artigos 154-A e 154-B e concedeu nova redação aos artigos 266 e 298, todos contidos no Código Penal, tornando infração penal a conduta de invadir recursos informáticos, sem motivos ou sem consentimento do proprietário, com pena de detenção de 3 (três) meses a 1 (um) ano, como também aumento da pena em um sexto a um terço se da invasão resultar prejuízo econômico à vítima.

Embora considerada um avanço frente à anterior ausência de legislação, tal previsão pode ser considerada modesta diante da potencialidade danosa de uma invasão que contenha informações sigilosas ou dados íntimos das pessoas. (TEYMISSO, 2017, p. 48).

Um ponto da lei que mereceu críticas foi ter criminalizado somente a invasão com o objetivo de obter vantagem ilícita, não alcançando aquelas invasões que, mesmo sem o intuito de ter alguma vantagem econômica direta, envolvem acesso a informações pessoais, pelo agente criminoso. (TAVARES, 2013, p. 07).

A falha foi posteriormente corrigida pela Lei 13.718, de 24 de setembro de 2018, a qual, dentre outras disposições, introduziu o artigo 218-C ao Código Penal, tipificando o crime de divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia, conduta que pode ser praticada por qualquer meio de execução, inclusive por meio de comunicação de massa ou sistema de informática ou telemática.

Algum tempo depois da edição da Lei Carolina Dieckmann, a Lei 12.965/2014 estabeleceu o chamado Marco Civil da Internet, destacando aspectos essencialmente cíveis das relações cibernéticas, embora até hoje possua disposições capazes de refletir na investigação de *cybercrimes*, já que “a lei procura através da previsão de princípios e garantias tornar a internet um ambiente menos hostil. Tal lei busca manter o equilíbrio entre a liberdade de expressão e transmissão do conhecimento com previsões de segurança”. (TEYMISSO, 2017, p. 49). O Diploma Legal preenche, de fato, algumas lacunas regulatórias até então percebidas no ambiente virtual, principalmente sobre a responsabilidade de provedores e usuários.

O Marco Civil também inovou no parágrafo 3º do seu artigo 19, ao definir que casos relacionados à reputação, à honra, aos direitos de personalidade serão apresentados aos Juizados Especiais - ainda que, em relação a tal aspecto, tenha recebido algumas críticas, pois embora a tramitação seja mais rápida nos

microssistemas dos Juizados, pode resultar em acordos desproporcionais, causando mais dor às vítimas, em razão do abrandamento das penas.

Já quanto à privacidade do usuário, ela passou a proteger seus dados junto aos provedores, dificultando a quebra de sigilo. Acontece que tal burocracia pode retardar uma investigação, já que a obtenção de dados pode dificultar ainda mais a identificação do criminoso. (BERGMANN, 2016, p. 47).

Em se tratando de liberdade de expressão, por outro lado, ela revela a intenção estatal de evitar a censura. O tratamento de dados pessoais do usuário (tanto pelo Poder Público quanto no ambiente privado) e o consequente respeito à sua privacidade e a outros direitos correlatos, todavia, foi matéria que precisou ser complementada pela Lei 13.709/2018, inclusive no que toca à responsabilidade de provedores e de operadoras de telecomunicações. (BRASIL, 2018).

De qualquer sorte, mesmo sendo pioneiro em garantias e vários direitos relacionados ao uso da internet, o Marco Civil e a Lei de Proteção aos Dados Pessoais do Usuário, por si sós, não bastam para proteção contra as várias e constantes tentativas de violações a direitos lesados. O cenário contemporâneo reclama, necessariamente, uma organização estatal dinâmica, no fito de especializar seus órgãos de investigação e repressão, que devem sempre estar atualizados para combater eficazmente as ameaças cibernéticas.

2.3 COMPETÊNCIA PARA JULGAR

O estudo de Crimes Cibernéticos perpassa pela compreensão de toda a complexidade que leva a sua definição, não só por envolver uma tecnologia que está em constante evolução, mas também, por abranger atos que não conhecem fronteiras, gerando problemas de competência territorial. (MACHADO, 2017, p. 18)

A competência jurisdicional, nesse contexto, tem por incumbência delimitar e divisar o âmbito de atuação dos diversos juízes e Tribunais em território brasileiro.

O Código de Processo Penal brasileiro, em seu art. 69, estabelece os critérios que determinam a competência:

> Art. 69**.** Determinará a competência jurisdicional: I - o lugar da infração: II - o domicílio ou residência do réu; III - a natureza da infração; IV - a distribuição; V - a conexão ou continência; VI - a prevenção; VII - a prerrogativa de função.
>
> .

Já na Constituição da Federal, em seu art. 109 e incisos, da competência federal em razão da matéria:

> Art. 109. Aos juízes federais compete processar e julgar: I - as causas em que a União, entidade autárquica ou empresa pública federal forem interessadas na condição de autoras, rés, assistentes ou oponentes, exceto as de falência, as de acidentes de trabalho e as sujeitas à Justiça Eleitoral e à Justiça do Trabalho; II - as causas entre Estado estrangeiro ou organismo internacional e Município ou pessoa domiciliada ou residente no País; III - as causas fundadas em tratado ou contrato da União com Estado estrangeiro ou organismo internacional; IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral; V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente; V-A - as causas relativas a direitos humanos a que se refere o § 5º deste artigo; VI - os crimes contra a organização do trabalho e, nos casos determinados por lei, contra o sistema financeiro e a ordem econômico-financeira; VII - os habeas corpus, em matéria criminal de sua competência ou quando o constrangimento provier de autoridade cujos atos não estejam diretamente sujeitos a outra jurisdição; VIII - os mandados de segurança e os habeas data contra ato de autoridade federal, excetuados os casos de competência dos tribunais federais; IX - os crimes cometidos a bordo de navios ou aeronaves, ressalvada a competência da Justiça Militar; X - os crimes de ingresso ou permanência irregular de estrangeiro, a execução de carta rogatória, após o exequatur, e de sentença estrangeira, após a homologação, as causas referentes à nacionalidade, inclusive a respectiva opção, e à naturalização; XI - a disputa sobre direitos indígenas. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução

Os elementos que estão mencionados tanto do CPP quanto da Constituição isolados ou mesmo combinados, apontam o juiz competente para a decisão de cada demanda. (GRECO, 1998, p. 141)

Assim, pode-se perceber que com uso da internet, do ponto de vista comunicacional, estabeleceu-se uma grande dificuldade de demarcar fronteiras, já que as relações jurídicas que existem podem envolver pessoas de países diversos, e o direito deve intervir para proteger os litígios que podem vir a surgir. (PINHEIRO, 2010, p. 8)

Em âmbito internacional, ao se tratar da competência dos delitos virtuais, deve-se necessariamente conhecer a figura dos crimes à distância, que são aqueles que

têm a ação ou omissão iniciada no Brasil e consumação fora dele ou vice-versa, sendo aplicada, em relação a eles, a teoria da ubiquidade.

Conforme versa o art. 6º do Código Penal:

> Art. 6º - 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.

Em suma, aplica-se a lei penal brasileira sempre que a atividade ou a conduta ocorram em território nacional. Em tais hipóteses, contudo, normalmente se estará diante da competência da Justiça Estadual, a menos que se esteja diante de alguma das situações previstas expressamente do artigo 109 da Constituição Federal.

Tem-se, nesse passo, o crime plurilocal, em que a ação ou a omissão, assim como a consumação, se dá dentro do território nacional; sendo assim, a competência será da Justiça comum brasileira, do local de ocorrência do fato delituoso.

Conforme art. 70 Código Processo Penal:

> Art. 70 - A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução

Convém, contudo, tecer um breve esclarecimento sobre os crimes de pornografia infanto-juvenil e racismo praticados por meio da *internet* e, especialmente, se devem eles ser julgados e processados pela Justiça Federal ou pela Justiça Estadual, e também uma breve menção a outros tipos de crimes que podem ser praticados em ambiente virtual.

A Lei nº 8.069/90 em seu artigo 241-A, tipifica o crime de pornografia infanto-juvenil com utilização da internet nos seguintes termos:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica)

Já no inciso V do art. 109 da Constituição Federal estabelece que:

> Art. 109. Aos juízes federais compete processar e julgar: V – os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente.

Assim sendo, publicar ou divulgar fotos, vídeos ou outros registros de crianças ou jovens por meio da internet, em sites, blogs ou até mesmo na rede social *Facebook* envolve processamento judicial no âmbito da Justiça Federal, pois foram reproduzidos os requisitos dispostos no art. 109 da CF, não apenas em razão da tutela em tratado ou convenção internacional, mas especialmente em razão da internacionalidade do fato. A divulgação ou publicação de material pornográfico infanto-juvenil em sites, blogs ou qualquer comunidade de relacionamento podem ser acessadas de qualquer parte do mundo, desde que conectados à *internet*. (CRIMES CIBERNÉTICOS, 2016, p. 325)

Em sentido diverso, uma troca de fotos por e-mail, realizada por pessoas residentes no Brasil de uma forma individualizada, nos limites do território nacional, não indica internacionalização do fato e a competência jurisdicional, então será da Justiça Estadual.

Sobre a competência em razão do lugar da infração, tem se definido pelo local onde a foto ou vídeo foram publicados. Porém, nem sempre é possível identificar o local da publicação; então a competência passa a ser fixada pelo juízo que proferiu o primeiro despacho decisório. Sendo apurado o local de publicação, para lá os autos devem ser remetidos.

Crimes contra a honra, previstos no Código Penal, e crimes de racismo, previstos na Lei nº 7.716/1989, seguem a mesma sistemática de fixação de competência estabelecida para crimes de pornografia infanto-juvenil. Se praticados de forma individualizada, pela simples troca de e-mails entre pessoas que vivem no Brasil, recomendarão a competência da Justiça Estadual, visto que não se enquadram nas hipóteses do inciso V do art. 109 da CF (não há internacionalização do crime). Os demais casos envolvendo crimes praticados por meio da *internet* devem ser, pelos motivos acima elencados, julgados pela Justiça Federal. (CRIMES CIBERNÉTICOS, 2016, p. 334)

3 INVESTIGAÇÃO CRIMINAL SOB A ÓTICA DO PRINCÍPIO DA INTERVENÇÃO MINÍMA

O escopo deste terceiro capítulo envolve, primeiramente, a análise de algumas linhas de investigações utilizadas pelos órgãos de repressão e, a final, a revelação das dificuldades de implementação da cooperação jurídica internacional para coibição e enfrentamento desse tipo de delito.

3.1 TÉCNICAS DE INVESTIGAÇÃO E LINHAS INVESTIGATÓRIAS APLICÁVEIS AOS CRIMES CIBERNÉTICOS

Depois de elaborada a legislação penal protetiva e preventiva, cabe ao estado garantir a eficácia social da norma, sendo, para tanto, necessário o desenvolvimento de mecanismos de investigação ágeis e competentes, daí se extraindo a importância da especialização da polícia, do Ministério Público e do Poder Judiciário, sendo a investigação criminal um dos processos mais importantes para apuração e combate do ilícito penal.

> O inquérito policial vem a ser o procedimento administrativo, preliminar, presidido pelo delegado de polícia, no intuito de identificar o autor do ilícito e os elementos que atestem a sua materialidade (existência), contribuindo para a formação da opinião delitiva do titular da ação penal, ou seja, fornecendo elementos para convencer o titular da ação penal se o processo deve ou não ser deflagrado. Pontue-se que a Lei no 12.830/2013, ao dispor sobre a investigação criminal conduzida pelo delegado de polícia, deixa consignado que a apuração investigativa preliminar tem como objetivo apuração de circunstâncias, materialidade e autoria das infrações penais (art. 2o, §1º) (TAVORA, ALENCAR, 2016, p. 127).

As funções investigativas, de acordo com a Constituição Federal, ficam a cargo das polícias civis dos estados e da Polícia Federal, restando às Polícias Militares, basicamente, as funções ostensivas de combate à criminalidade. Nesse passo, à Polícia Federal cumpre as investigações em nível federal, percebendo-se, em relação a ela, uma melhor estrutura, se comparada à Polícia Civil e também um maior número de delegacias especializadas com conhecimentos técnicos em crimes cibernéticos. A Polícia Federal, além disso, possui à sua disposição maiores recursos financeiros e tecnológicos, tendo-se tornado uma referência quanto à investigação de crimes cibernéticos.

A rigor, nos crimes cibernéticos a investigação pode ser identificada em duas fases: uma fase de campo e uma fase técnica. (WENDT, JORGE, p. 52).

Na fase técnica da investigação, tenta-se chegar à identificação do equipamento utilizado pelos criminosos. Também se procura uma melhor compreensão do fato ocorrido, analisando as informações fornecidas pelas vítimas. Aqui, a investigação e a confecção do laudo pericial dependem muito da capacitação do investigador e do perito, ficando clara a necessidade de um conhecimento em tecnologia para a busca de provas do delito. (WENDT, JORGE, p. 53).

A Constituição Federal brasileira prevê que o sigilo de dados só pode ser quebrado com autorização judicial. Essa autorização, normalmente, se revela essencial para obtenção de informações capazes de possibilitar a identificação do criminoso. Para Teymisso, a fase técnica segue um caminho:

> Compreensão do fato ocorrido e análise das informações fornecidas pelas vítimas; Orientação à vítima com a finalidade de proteger o corpo de delito e sua segurança virtual; Coleta inicial das provas em ambiente cibernético; Formalização do crime através do registro de boletim de ocorrência; Investigação na internet acerca de prováveis autores; Confecção de relatório das provas apuradas; Representação perante o poder judiciário para expedição de autorização judicial para quebra de dados; Análise das informações prestadas por provedores de conexão e provedores de conteúdo. (TEYMISSO, 2017, p. 57).

Após todo esse processo, com a identificação e localização do criminoso inicia-se a fase de campo, a qual demanda a formação de uma equipe de agentes e policiais, apta a realizar diligências destinadas ao reconhecimento do local do crime e garantir a confiabilidade das provas apuradas. Nessa fase são normalmente expedidos mandados de busca e apreensão para a coleta de materiais comprobatórios, tudo dentro da legalidade, para evitar a invalidação das provas técnicas. (TEYMISSO, 2017, p. 58).

Sempre existe uma enorme cobrança da sociedade para a elucidação de crimes, a fim de que não se estabeleça no ambiente social uma sensação de impunidade. Então, por mais complexa que possa se tornar uma investigação sobre crimes cibernéticos, o Estado não pode esgotar todas as possibilidades para a elucidação desse tipo de delito. Seu caráter transnacional, além disso, recomenda colaboração entre forças policiais de Estados diversos, compartilhamento de informações e aprimoramento tecnológico, tal como se examinará no próximo tópico.

3.2 COOPERAÇÃO INTERNCIONAL

Um dos pontos que mais pode ter ajudado a aumentar o número de crimes cibernéticos, é a sensação de anonimato com o que o criminoso fica, já que se pode cometer o crime de qualquer parte do mundo e usar mecanismos que dificultam o seu rastreamento.

Com a rápida globalização e a instauração da *internet* em todo o mundo, percebeu-se também o crescimento do crime organizado, de atos terroristas, além da fácil movimentação de grandes somas de dinheiro, problemas esses que podem reclamar a cooperação entre países diversos. O Brasil, em tal contexto, não pode desprezar as relações que mantém com outros países, pois o fenômeno flexibilizou sensivelmente o conceito de soberania. É certo que

> (...)globalização representa, portanto, um desafio significativo para o exercício da soberania dos Estados no contexto internacional. Esses desafios, que não são triviais, levaram alguns autores a falar em "crise da soberania" questionando não somente a utilidade do conceito para captar e explicar as características atuais do fenômeno, como também quem seria o "sujeito" da soberania (MIRANDO, 2004, p. 89)

Cumpre destacar que o Direito Internacional evoluiu de uma concepção clássica, *"onde as normas eram conduzidas aos Estados como sujeitos de Direito Internacional para um cenário contemporâneo no qual organizações internacionais, empresas transnacionais, e indivíduos podem assumir também papeis importantes na construção dos rumos da política mundial"*. (TEYMISSO, 2017, p.68).

Outro desafio que o direito enfrenta é a necessidade de convergência dos diversos ordenamentos jurídicos, pois não há como negar a crescente ligação entre as diferentes nações, basta só observar como uma crise em um país pode influenciar diretamente a política ou a economia de outro. Para Valério de Oliveira Mazzuol:

> Verifica-se, com esse fenômeno, que o Direito vai deixando de somente regular questões internas para também disciplinar atividades que transcendem os limites físicos dos Estados, criando um conjunto de normas capazes de realizar esse mister. Esse sistema de normas jurídicas (dinâmico por excelência) que visa disciplinar e regulamentar as atividades exteriores das atividades dos Estados (e, também atualmente, das organizações internacionais e dos próprios indivíduos) é o que se chama de Direito Internacional Público e Direito das Gentes (MAZZUOLI, 2011, p. 44)

Uma das maiores dificuldades na investigação de crimes cibernéticos, em âmbito internacional além da questão tecnológica e do diferente ordenamento jurídico, tem também a demora para se obter informações de provedores de outro país ou do próprio Estado, tendo em vista que há que se respeitar as regras de relacionamentos internacionais como tratados e convenções. Infelizmente pode haver uma certa burocratização do processo, o que pode dificultar o encontro do responsável pelo crime.

O Brasil, nesse contexto, já experimentou embates envolvendo, por exemplo, as aplicabilidades *Whatsapp* e *Facebook*, sendo que ambos já ficaram paralisados em razão de impasse entre seus administradores e o Poder Judiciário, pelo fato de se negarem a cumprir ordens judiciais e quebrar algumas mensagens criptografadas. A Justiça de São Paulo e do Rio de Janeiro determinaram o bloqueio de tais aplicativos de comunicação devido a não colaboração com as investigações sobe o crime organizado, que gerou certa polemica no país.

Resolver o problema não é uma questão das mais fáceis, pois envolve uma legislação adequada, o comprometimento dos países envolvidos, e a eficácia dos órgãos de combate aos crimes cibernéticos. Deve-se também reconhecer que esse tipo de crime vai além das fronteiras nacionais e que toda cooperação e acordo são importantes para uma rapidez das investigações, pois esse tipo de delito ou conduta e o tempo podem ser fundamentais. (BLATT, 2016, p. 83).

Conforme se extrai do sítio do Ministério da Justiça e Segurança Pública brasileiro, o Brasil é signatário de diversos a acordos e tratados internacionais na área de cooperação jurídica internacional, atuando ativamente nesta área, especialmente por intermédio do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional da Secretaria Nacional de Justiça (DRCI/Senajus), órgão designado como *Autoridade Central* nas relações com outros Estados. No âmbito penal, os pedidos de cooperação jurídica internacional (especialmente, a Carta Rogatória e o Auxílio Direto) são encaminhados às Autoridades Públicas competentes (Juízes, membros do Ministério Público, Delegados de Polícia e Defensores Públicos) para cumprimento de atos de comunicação processual (citações, intimações e notificações), atos de investigação ou instrução (oitivas, obtenção de documentos, quebra de sigilo bancário, quebra de sigilo telemático, por exemplo) ou ainda algumas medidas de constritivas de ativos, como bloqueio de bens ou valores. (BRASIL, 2019).

O DRCI/Senajus também é ponto de contato brasileiro com diversas redes de cooperação internacional (IberRed, Groove, RRAG, por exemplo), este que se realiza atualmente de forma célere, direta e desburocratizada, servindo, essencialmente, para resolver problemas no cumprimento de diligências solicitadas, para estabelecimento de estratégias conjuntas de atuação, entendimentos conjuntos e promoção de diálogo sobre alterações de procedimentos, em um mundo, notadamente, que também passa por constantes mudanças (BRASIL, 2019).

Importante salientar, neste diapasão, que em matéria de cooperação jurídica internacional o Brasil tem se mostrado um país essencialmente *demandante*, na medida em que mais de 80% (oitenta por cento) dos pedidos processados por aquele Departamento se referem a demandas de Autoridades brasileiras para o exterior. O próprio Ministério da Justiça e Segurança Pública brasileiro tem reconhecido, em tal cenário, que tal disparidade revela a importância da cooperação para a efetividade da justiça brasileira, no que toca a crimes transnacionais, como usualmente se percebe no caso de crimes cibernéticos (BRASIL, 2019).

O caminho adequado para combate de delitos virtuais e cibernéticos, portanto, parece estar sendo adequadamente trilhado. É preciso, todavia, persistir e avançar nesta área, pois a tecnologia, sabidamente, é rápida na promoção de inovações, sendo que os meios investigatórios não podem ficar alheios a esta realidade. Os Estados precisam estar organizados para proteção de seus cidadãos em relação a condutas danosas que não obedecem a regras nem se limitam a fronteiras físicas.

CONSIDERAÇÕES FINAIS

Impulsionando o processo de globalização, as novas tecnologias estão fazendo surgir uma nova era. Uma era em que dispositivos tecnológicos, como celulares, computadores e a própria internet, tornam-se indispensáveis para grande parte de sociedade contemporânea. E isso acaba tendo uma repercussão social e cultural sem precedentes, sendo que a informação passou a ser muito importante em um cenário de grande competição mundial.

Neste cenário, nota-se uma série de nomenclaturas distintas e diferentes entendimentos doutrinários em relação ao que sejam crimes cibernéticos ou virtuais. Há doutrinadores que consideram crimes virtuais qualquer conduta típica, ilícita e culpável praticada com envolvimento de dispositivos informáticos, independentemente da menção explícita destes na Lei Penal. Já outra parte da doutrina acredita que há a necessidade de tipificação específica desse tipo de condutas, apontando para a falta de amparo na legislação vigente para punição dos responsáveis pela infração penal.

Nesse trabalho se buscou abordar esses dois entendimentos, considerando crimes cibernéticos tanto condutas especificamente tipificadas na legislação penal, como crimes de livre execução, eventualmente praticados com utilização de dispositivos tecnológicos. Observaremos também que embora essas condutas demandem um tratamento legislativo especializado, também se perfectibilizam com a realização de tipos penais tradicionais, eventualmente praticados no meio virtual. Acredita-se, no entanto, que leis voltadas especificamente para essa modalidade de crime devem ser elaboradas e implementadas pelo Estado brasileiro.

O grande aumento de crimes cibernéticos vem exigindo uma atitude mais proativa das autoridades, para que o cidadão assim tenha sua segurança devidamente defendida. Obviamente que não se pode esquecer, por outro lado, que o Direito Penal deve atentar ao princípio da intervenção mínima, revelando-se como *“ultima ratio”* para a inibição de condutas contrárias ao saudável convívio social. Não obstante, o Estado não pode esquivar-se de suas responsabilidades perante os novos meios de interação social verificados no mundo comunicacional contemporâneo.

Importante salientar, além disso, que a liberdade de expressão deve ser protegida no ambiente virtual, pois compõe um dos pilares da democracia. Violar esse

direito abalaria fundamentalmente essa estrutura social, erigida por meio de séculos de luta. Restrições ao fluxo comunicacional, embora pareçam antidemocráticas em um primeiro momento, podem ser pensadas para proteção da intimidade e de danos pessoais em ambiente virtual, cumprindo ao Estado corrigir excessos, para o bem da maioria.

Outro importante problema analisado no curso da pesquisa relaciona-se com a omissão da legislação penal quanto ao tipo penal da invasão de dispositivo sem fins ilícitos, conduta grave não alcançada pela norma penal, mas apenas pela norma cível.

Abordaram-se, ademais, os crimes contra a honra perpetuados na *internet*, prática que aumentou exponencialmente nos últimos anos, já que a cada dia aumenta o número de usuários da rede para fins didáticos, laborais ou entretenimento.

Realizou-se uma análise sobre a legislação brasileira, tendo-se constatado que no âmbito social algumas condutas nocivas ao corpo social, recentemente engendradas em ambiente virtual, não são abrangidas pela norma atual; ainda que outras já estejam contempladas em projetos de lei.

Concluiu-se que, além da legislação brasileira sobre crimes cibernéticos ainda não ser suficiente para combate de tal espécie de criminalidade, existe a dificuldade quanto à investigação criminal no Brasil, pois ela não está oferecendo resultados eficientes, demonstrando um despreparo das estruturas das instituições penais para o combate a esse tipo de crime.

De fato, inferiu-se que os investigadores acabam encontrando uma série de dificuldades na investigação, como a demora na concessão de mandados judiciais, na realização de perícias e no atendimento de acesso a dados armazenados por determinados provedores.

No Brasil, a atribuição para a apuração das condutas indevidas praticadas por computador pertence à Polícia Federal e às policias civis dos Estados e do Distrito Federal, mediante investigações realizadas por meio do Inquérito Policial, instrumento este que deve seguir as normas do Código de Processo Penal brasileiro.

A Polícia Federal atua, essencialmente, nos crimes capazes de afetar os interesses da União e outras Instituições Federais. Como possui melhores condições estruturais, acaba por desenvolver uma melhor investigação. Já as polícias civis dos estados, com algumas exceções de delegacias especializadas em crimes virtuais, normalmente não reúnem condições para realizar investigações desse tipo de crime,

muito também pela falta de agentes capacitados e equipamentos, sobrecarga de serviço e desvios de função.

É imprescindível, também, referir que a cooperação internacional possui papel fundamental na investigação de crimes cibernéticos, especialmente envolvendo pornografia infantil, já que o agente que cometeu a conduta ilícita usualmente está domiciliado em outro país e seus dados estão disponíveis em provedores de internet no estrangeiro. Essa cooperação envolve uma uniformização normativa para facilitar as comunicações entre os países, polícia e Poder Judiciário, sendo recomendável uma padronização no acesso a provedores por parte dos investigadores, para que sua atuação possa gerar uma repressão eficaz a tais crimes.

Em suma, portanto, comprovou-se a hipótese levantada ao início da pesquisa, no sentido de que no ambiente social brasileiro, dificuldades de tipificação específica de crimes cibernéticos geram uma deficiência de punibilidade, sendo realmente necessário criar mecanismos técnicos e legais para que, em ambiente cibernético, bens jurídicos relevantes à sociedade sejam adequadamente tutelados pela norma penal, tanto no que se refere ao aperfeiçoamento de meios investigatórios, quanto no que toca à própria aplicação da lei.

REFERÊNCIAS

ABREU, Karen Cristina Kramer. “**História e usos da Internet**”. Biblioteca on-line de Ciências da Comunicação, 2009. Universidade da Beira Interior. Covilhã. Disponível em:<http://www.bocc.ubi.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf >. Acesso em18/04/2019.

ABREU, Leandro Farias dos. **A Segurança das Informações nas Redes Sociais**. Disponível em: <http://www.fatecsp.br/dti/tcc/tcc0023.pdf > Acesso em: 18/03/2019.

ADACHI, Tomi. Comitê Gestor da Internet no Brasil (CGI.br**): Uma Evolução do Sistema de Informação Nacional Moldada Socialmente**. Tese de Doutorado. Universidade de São Paulo, 2009.

ASCENSAO, José de Oliveira. **Direito da Internet e da Sociedade da Informação**. Rio de Janeiro: Forense, 2002.

BATISTA, Nilo. **Introdução crítica ao Direito Penal brasileiro**. Rio de Janeiro, Revan. 2000.

BENAKOUCHE, Tâmara, “**Redes técnicas - redes sociais: a pré-história da Internet no Brasil**”, Revista USP, n. 35, São Paulo, SP, 1997.

BENTO, Leonardo Valles. Liberdade de Expressão na Internet: Alguns Parâmetros Internacionais e o Direito Brasileiro. *In* **Revista de Direito UNISC,** Santa Cruz do Sul, nº. 43, p.73-97, maio-ago 2014.

BLATT, Erick Ferreira. **Ferramentas de investigação nos crimes cibernéticos utilizadas pela Polícia Federal**. Rio de Janeiro: Mallet, 2016.

BRASIL. Constituição Federal. **Diário Oficial da União**, Brasília, DF, 5 out. 1988. Disponível em: < http://www.senado.leg.br/atividade/const/constituicaofederal.asp#/con1988/%20CON1988_05.10.1988/CON1988.pdf >. Acesso em: 15/03/2019.

BRASIL, Decreto nº 84.067. **Diário Oficial da União**, Brasília, DF, 03 out. 1979. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/19701979/D84067.htm>. Acesso em: 28 mai. 2019.

BRASIL. Lei nº 13.709. **Diário Oficial da União**, Brasília, DF, 14 ago. 2018.

BRASIL. Lei nº 13.718. **Diário Oficial da União**, Brasília, DF, 24 set. 2018b.

CASTELLS, Manuel. **Communication Power.** New York: Oxford University Press, 2009.

CASTRO, Luís Fernando Martins. **Direito da Informática e do Ciberespaço**. 2014. Disponível em: < http://noosfero.ucsal.br/articles/0006/4224/12.2-Castro-ARTIGODireito_do_Ciberespaco.pdf > Acesso em: 05 de setembro.2019.

CRIMES CIBERNÉTICOS, **Roteiro de Autuação, Ministério Público Federal**. Brasília, 2016.

CRUZ, António. Ensinar. Disponível em: < http://www.antoniocruz.net/ensinar/internet/manuais/internet-01-internet.pdf >. Acesso em: 22/04/2019.

CORREA, Gustavo Testa. **Aspectos jurídicos da Internet**. São Paulo: Saraiva, 2000.

DA SILVA, Ana Carolina Calado. **O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira.** 2015. Disponível em: < http://www.egov.ufsc.br/portal/conteudo/o-estudo-comparado-doscrimes-cibernéticos-uma-abordagem-instrumentalista-constitucional >. Acesso em 22/05/2019.

DESLANDES, Suely Ferreira. **A Construção do Projeto de Pesquisa. In: MINAYO, Maria Cecília de Souza (Org.). Pesquisa Social. Teoria, método e criatividade**. Petrópolis: Vozes, 2009.

DIAS, Lia Ribeiro, CORNILS, Patrícia, Alencastro: **o general das telecomunicações**. São Paulo, Plano Editorial. 2004.

FILHO, Cléuzio Fonseca. História da computação: **O Caminho do Pensamento e da Tecnologia**. Porto Alegre: EDIPUCRS, 2007.

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

FEITOZA, Luis Guilherme de Matos. **Crimes Cibernéticos: O estelionato Virtual**. Monografia. Universidade Católica de Brasília. Distrito Federal – 2012.

GRECO, Vicente. **Manual de Processo Penal**. 5ª ed. São Paulo: Saraiva, 1998.

INELLAS, Gabriel César Zaccaria de. **Crimes na Internet**. 2º ed. São Paulo: Editora Juarez de Oliveira, 2009.

KUROSE, J. F.; ROSS, K. – **Redes de Computadores e a Internet**. 5. Ed. Pearson, 2010.

Lei nº 12.735, de 30 de novembro de 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm >. Acesso em: 14/05/2019.

Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 15/05/2019.

LÉVY, Pierre. **As tecnologias da inteligência: o futuro do pensamento na era da informática**. 2. ed. Rio de Janeiro: Editora 34, 2010.

LÉVY, Pierre. **Cibercultura.** São Paulo, 1999.

LENZA, Pedro. **Direito Constitucional Esquematizado**. 16. Ed. São Paulo: Saraiva, 2012.

LISBOA, Roberto Senise. **Direito na Sociedade da Informação**, Santa Catarina, 2016.

MACHADO, Thiago José Ximenes. **Cibercrime e o crime no mundo informático**. Monografia. Universidade Fernando Pessoa. Porto, 2017.

MAZZUOLI, Valerio de Oliveira. **Curso de Direito Internacional Público**. São Paulo: Revista dos Tribunais, 2011.

MIRANDA, Napoleão. **Globalização, Soberania Nacional e Direito Internacional**. Revista CEJ (Brasília), Brasília, 2004.

MOLINA, Márcia Cristina Gomes. A Internet e o poder de comunicação na sociedade em rede: influências nas formas de interação social. *in*: **Revista Metropolitana de Sustentabilidade.** Volume 3, número 3 – 2013. Disponível em: < http://www.revistaseletronicas.fmu.br/ >. Acesso em: 30 mai 2019

NADER, Paulo. **Introdução ao Estudo do Direito**. Rio de Janeiro: Forense: 2004.

OLIVEIRA, Hélio Magalhães. **Engenharia de Telecomunicações**. 1 Ed. Recife: HM, 2012.

PACHECO, Wilfredo Enrique Pires. **Manual de Responsabilização Penal dos Hackers, Crackers, e Engenheiros Sociais**. Disponível em: < https://www.conjur.com.br/dl/guia-crimes-digitais.pdf >. Acesso em: 22/03/2019.

PAIVA, Mário Antônio Lobato de. **A Ciência do Direito Informático.** 2011.

PERRIN, Stephanie. **O Cibercrime**. Disponível em: < https://vecam.org/archives/article660.html >. Acesso em: 20/03/2019.

PICON, Leila Cássia; ANTUNES, Solange; DUARTE, Isabel Cristina Brettas, O Papel do Direito na Sociedade da Era Informacional, 2013.

PIMENTEL, Alexandre Freire. O **direito cibernético: um enfoque teórico e lógico aplicativo**. - Rio de Janeiro: Renovar, 2000.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Saraiva, 2010.

QUEIROZ, Paulo de Souza. **Direito Penal:** Introdução crítica. São Paulo: Saraiva, 2001.

REALE, Miguel. **Lições preliminares de direito**. São Paulo: Saraiva, 2002.

ROCHA, Adriano Aparecido. **Cibercriminalidade**. Monografia. Faculdade de Ensino Superior e Formação Integral. Garça. São Paulo – 2017.

ROSA, Fábrizio. **Crimes de Informatica**. 2º ed. Campinas: Bookselle, 2005.

SEGURADO, Rosemary. Política da Internet: **A regulamentação do Ciberespaço**, 2011.

SEGURADO, Rosemary; LIMA, Carolina Silva Mandú de; AMENI, Cauê S. **Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França**. São Paulo, 2014.

SILVA, Luana Matias da; SILVA, Marianne Facundes da; MORAES, Dulcimara Carvalho. **A Internet como ferramenta tecnológica e as consequências de seu uso: aspectos positivos e negativos**. 2016.

SILVA, Tânia Ventura. Crimes Cibernéticos: **A era da informação traz ameaça para a sociedade**, 2016. Disponível em: <

http://www.conteudojuridico.com.br/artigo,crimes-ciberneticos-a-era-da-informacaodigital-traz-ameaca-para-sociedade,56091.html >. Acesso em: 22/05/2019.

TAVARES, Tarcísio Alves. **Análises Iniciais e Críticas à Lei 12.737/2012- Lei Carolina Dieckmann**, 2013. Disponível em:< http://www.unipac.br/site/bb/tcc/tcc0463074a098a0f1e76f9ad1376e21e2b.pdf > Acesso em: 25 de setembro.2019.

TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. Salvador: Juspodivm, 2006

TELEBRASIL ASSOCIAÇÃO BRASILEIRA DE TELECOMUNICAÇÕES, **Telebrasil: 30 anos de sucessos e realizações**. Rio de Janeiro, Graphbox. 2004.

TEYMISSO, Sebastian Fernandes Maia. **Análise dos Mecanismos de Combate aos Crimes Cibernéticos no Sistema Penal Brasileiro**. Monografia. Universidade Federal do Ceará. Fortaleza – 2017.

TIGRE, Paulo Bastos, **Indústria Brasileira de Computadores: perspectivas até os anos 90**, Rio de Janeiro, 1987.

UMBACH, Kenneth W. **The Internet: A Califórnia Police Perspective**. 1997. Disponível em: < http://www.library.ca.gov/CRB/97/02/97002a.pdf >. Acesso em: 27/05/2019.

WENDT, Emerson, NOGUEIRA, Higor Vinicius Jorge. **Crimes Cibernéticos: Ameaças e procedimentos de investigação**. São Paulo, Brasport, 2012.