CENTRO UNIVERSITÁRIO ATENAS

INIMAR JÚNIOR OLIVEIRA SILVA

CIBERCRIME E OS SEUS REFLEXOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Paracatu

2018

INIMAR JÚNIOR OLIVEIRA SILVA

CIBERCRIME E OS SEUS REFLEXOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Monografia apresentada ao Curso de Direito do Centro Universitário Atenas, como requisito parcial para obtenção do título de Bacharel em Direito.

Área de Concentração: Direito Penal

Orientador: Prof. Msc. Diogo Pereira Rosa

Paracatu

2018

INIMAR JÚNIOR OLIVEIRA SILVA

CIBERCRIME E OS SEUS REFLEXOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Monografia apresentada ao Curso de Direito do Centro Universitário Atenas, como requisito parcial para obtenção do título de Bacharel em Direito.

Área de Concentração: Direito Penal

Orientador: Prof. Msc. Diogo Pereira Rosa

Banca Examinadora:

Paracatu – MG, 05 de julho de 2018.

_____

Prof. Msc. Diogo Pereira Rosa

Centro Universitário Atenas

_____

Prof. Msc. Rogério Mendes Fernandes

Centro Universitário Atenas

_____

Prof. Sergio Batista Teixeira Filho

Centro Universitário Atenas

Dedico esta monografia e este momento à minha mãe, Maria Ap. da Silva, que sempre lutou e se esforçou por seus filhos e embora tenha havido diversos momentos difíceis e aparentemente insuperáveis, com toda sua garra, dedicação, esforços e muitos puxões de orelhas (muitos mesmo), transformou o impossível em possibilidades.

Também dedico às minhas irmãs, Ingrid Ap. e Larissa Ed., que sempre me auxiliaram nos momentos difíceis e me irritaram no restante dos momentos, como boas irmãs que são.

Enfim, dedico tudo isso a essas três mulheres, minha família, meu mundo, meus orgulhos, que com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa da minha vida e muito além daqui.

AGRADECIMENTOS

Ao meu orientador Prof. Diogo Pereira, pela sabedoria e paciência.

Aos meus colegas de sala, que mesmo com as crises, brigas, discussões, olhares repletos de intenções assassinas e vontade de matar uns aos outros, tornaram o curso divertido, alegre e bastante enriquecedor, além de transformarem essa longa jornada, chamada de graduação, em uma grande experiência, repleta de momentos inesquecíveis e histórias para posteridade.

Aos professores que tive durante o curso, com exceção de alguns poucos, que transformaram uma pessoa leiga e sem noção em alguém com sede de aprendizado, conquistas e sucesso.

A toda a instituição do Centro Universitário Atenas, com exceção de alguns setores, pelas horas perdidas nas filas, pelos estresses, pelos atrasos com documentos, assinaturas e requerimentos, além das raivas, dificultação com coisas extremamente simples, e muitos outros pontos que tornaram a graduação ainda mais exaustiva.

Gostaria de deixar registrado também o meu reconhecimento à minha mãe e irmãs, pois acredito que sem o apoio delas seria muito difícil, senão impossível, vencer esse desafio.

Enfim, agradeço a todos os que por algum motivo contribuíram para a realização desta monografia.

No Brasil infelizmente o atraso legislativo é grande. O legislador pátrio espera em berço esplêndido que as definições ocorram no exterior para depois debater os mesmos pontos, achar as mesmas soluções, dando uma nova roupagem e apresentando como solução original e inovadora.

Andrade, 2015.

RESUMO

Trata-se de monografia, elaborada como Trabalho de Conclusão de Curso - TCC, a qual tem como assunto basilar os cibercrimes, apresentando uma análise ampla a respeito dos elementos desses crimes, como classificações e características principais, além da problemática dos reflexos destes crimes no ordenamento jurídico brasileiro. Nesse contexto, são inegáveis os enormes benefícios que as tecnologias, aliadas com a internet, trouxeram para a sociedade como um todo. Tais tecnologias estão em constante evolução, provocando avanços e inovações, em uma corrida irrefreável por melhorias, aperfeiçoamentos e criação de mecanismos cada vez mais úteis, sofisticados e inovadores. Porém, os avanços tecnológicos não trazem apenas benefícios para a sociedade. Em contramão aos benefícios que a internet e as tecnologias dispõem temos malefícios, denominados Cibercrimes. O cibercrime e o seu reflexo no ordenamento jurídico brasileiro, é o objeto de estudo e análise desta monografia.

Palavras-chave: Cibercrime. Reflexo. Ordenamento. Jurídico. Brasileiro.

ABSTRACT

This is a monograph, elaborated as a Course Completion Work - CCW, which focuses on cybercrimes, presenting a broad analysis of the elements of these crimes, such as classifications and main characteristics, as well as the problematic of the reflexes of these crimes in the Brazilian legal system. In this context, the enormous benefits that technologies, allied with the Internet, have brought to society as a whole are undeniable. These technologies are constantly evolving, bringing about breakthroughs and innovations, in an unstoppable race for improvements, improvements and creation of increasingly useful, sophisticated and innovative mechanisms. However, technological advances do not only bring benefits to society. Contrary to the benefits that the Internet and the technologies have, we have wrongs, called Cybercrimes. Cybercrime and its reflection in the Brazilian legal system is the object of study and analysis of this monograph.

***Keywords**: Cybercrime. Reflection. Planning. Legal. Brazilian.*

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

A internet e as tecnologias permitiram o alcançasse de diversos avanços e inovações. Por meio delas houve a disponibilização e compartilhamento das mais variadas informações, conteúdos e dados, além de incontáveis benefícios que permeiam toda a sociedade modernizada. Dentre elas, destaca-se a força e o alcance que a internet detém nos dias modernos, excedendo qualquer expectativa que trazia sobre si quando dos primórdios de sua criação, uma vez que ela mostrou estar em constantes avanços e progressos imparáveis.

Indubitavelmente, a internet pode ser dita como a invenção tecnológica mais avançada e a que mais traz benefícios à sociedade atual, sendo ela o veículo de comunicação mais rápido, pratico e acessível, transformando o mundo e as sociedades numa espécie de nação global, que interage entre si, buscando melhorias e inovações. Ainda, dentre as mais variadas tecnologias, a importância da internet tornou-se tão grande que vem se tornando cada vez mais indispensável à vida cotidiana moderna, um bom exemplo disso é o fato de que é na internet que a sociedade atual dispõe de mais tempo gasto, tanto no plano de trabalho como nas atividades de lazer e interações sociais.

No inicio da era digital, para se utilizar da internet arcaica, era necessário valer-se de maquinas e/ou computadores robustos, espaçosos e muitas vezes inacessíveis à população. Porém, com o avanço tecnológico, os computadores foram diminuindo de tamanho, se tornando mais práticos e acessíveis à massa, de modo que atualmente, para acessar a internet, não é mais "obrigatório" possuir um computador, sendo possível acessar e se conectar a rede através de smartphones, *tablets*, notebooks, entre outros dispositivos portáteis que cabem na palma da mão e no bolso.

Por melhor que seja a internet e os benefícios que a envolvem, a progressiva adesão social a essa tecnologia não trouxe exclusivamente benefícios. Paralelamente a estes, a internet possibilitou o surgimento de malefícios e condutas danosas. Neste sentido, conforme a internet ganhava o mundo e os seus benefícios se tornavam cada vez mais conhecidos e notórios, criminosos sentiram-se atraídos por ela, de tal forma que decidiram se aproveitar de conhecimentos específicos quanto a computadores, dispositivos eletrônicos e internet, em conjunto com o anonimato, a ausência de conhecimento popular acerca da utilização segura da internet e a dificuldade de adequação dos Estados, para praticar condutas danosas, maliciosas e ilícitas. Tal fenômeno, devido a sua enorme reincidência, acabou se tornando objeto de estudo e ganhou a atenção dos países, como o Brasil, uma vez que cresceu a necessidade de se combater e legislar acerca de tais práticas.

A ocorrência reiterada de condutas prejudiciais na rede mundial de computadores

fez surgir um popular e errôneo conhecimento de que a internet seria uma ‘‘terra sem lei’’, onde os Estados não teriam força para combater as condutas ilícitas ali praticadas.

Por sua vez, o crescimento destas ações prejudiciais praticadas por meio da internet, e as suas diversas formas, fez surgir novos tipos penais e uma nova forma de criminalidade, a qual, dentre várias outras nomenclaturas, recebeu a alcunha de “Cibercrime”, nomenclatura dada e usada extensivamente aos crimes que envolvam qualquer atividade ou conduta ilícita envolvendo a rede mundial de computadores.

As leis, por seu turno, foram e são criadas com o fim de exercer uma força normativa e coercitiva para que seja possível a convivência harmônica entre os indivíduos da sociedade fundamentada nessas leis, neste ponto, e, seguindo essa premissa, é de suma importância que quaisquer normas ou leis acompanhem de forma linear e progressiva as inovações, interações e mudanças sociais, pois se tal premissa fosse desrespeitada não haveria sentido a criação de leis incapazes de regulamentar a convivência social.

Como qualquer inovação possui seus prós e contras, o uso desenfreado da internet trouxe novos desafios para operadores do Direito. Como regulamentar o uso da internet? As normas já existentes são capazes de amparar o crescimento das relações virtuais e seus conflitos? Devemos fazer interpretações das normas já existentes ou criar novas normas especificas? Como preparar o direito para as constantes e crescentes relações virtuais?

É sabido que o papel do Direito é o de regulamentador das ações dos seres inseridos em uma determinada sociedade. Portanto, a legislação deve estar apta a dirimir as interações referentes à troca de informações e conteúdos pela internet e ao mesmo tempo deve ser capaz de punir práticas delituosas no âmbito cibernético. Nesse sentido, o jurídico e normativo brasileiro, dito ser moroso, aparenta ter encontrado dificuldades e obstáculos na regulação de acontecimentos na esfera informática e virtual.

Diante o exposto, a presente monografia tem por escopo analisar os principais aspectos dos cibercrimes, as suas consequências jurídicas, bem como os seus reflexos no ordenamento jurídico brasileiro.

1.1. Problema

A ocorrência dos cibercrimes no Brasil provocou reflexos em seu Ordenamento Jurídico?

1.2. Hipótese De Estudo

O sistema jurídico brasileiro, por ser regulador das relações juridicamente relevantes, deve, ou, ao menos, deveria acompanhar as mudanças que ocorrem no seio de sua sociedade. Entretanto, apesar da crescente leva de cibercrimes, devido à morosidade do Estado Brasileiro, o Direito não está conseguindo acompanhar e proteger os interesses de uma sociedade que clama cada vez mais por soluções.

1.3. Objetivos

1.3.1. Objetivo Geral

a) Examinar os cibercrimes e os seus reflexos no Ordenamento Jurídico Brasileiro.

1.3.2. Objetivos Específicos

a) Introduzir os aspectos históricos da internet no Brasil;
b) Adentrar nos conceitos, características e classificações de Cibercrimes;
c) Identificar as possíveis legislações e reflexos no Brasil e no seu ordenamento jurídico, quanto aos cibercrimes.
d) Analisar a eficácia da legislação Brasileira atual frente os cibercrimes.

1.4. Justificativa

A chegada do século XXI trouxe consigo o fácil acesso à internet, os cibercrimes e a necessidade dos estados e leis de se adaptarem. Conforme a evolução das tecnologias progrediu, concomitantemente, ocorreu um constante aumento e progresso nos crimes praticados por meio da rede mundial de computadores, o que por sua vez, comprovou que é imprescindível que o Direito acompanhe esta evolução e regulamente a área virtual, com o intuito de resguardar os interesses individuais e coletivos. No Brasil tal necessidade também existe e se mostra cada vez maior.

Na ultima década, no Brasil, foi possível presenciar o crescimento desenfreado dos cibercrimes e suas variáveis, levando os cidadãos brasileiros a procurar amparo no sistema judiciário, aumentando ainda mais a já enorme demanda de processos.

Desta forma, com o aumento dos cibercrimes e o problema da regulamentação de

normas a seu respeito, surgiu o interesse da presente pesquisa, já que se faz necessário a análise do alcance da proteção legislativa do Estado Brasileiro sobre os direitos dos internautas brasileiros, bem como a adequação legislativa do Brasil frente à execução dos crimes cometidos no ambiente virtual.

Ademais, o presente estudo apresenta importante contribuição para o meio acadêmico e social, já que traz uma importante reflexão sobre a eficácia da legislação atual no combate de cibercrimes, que tem assolado cada vez mais a sociedade.

1.5. Metodologia Do Estudo

A presente monografia – de natureza básica – foi realizada, inicialmente, por meio de levantamento bibliográfico, por meio do qual se obteve uma visão ampla acerca do tema, possibilitando a análise, de forma qualitativa, das questões envolvendo o tema da monografia.

Nesse sentido, a presente monografia foi realizada através de pesquisa bibliográfica, que compreendeu uma revisão bibliográfica acerca dos diversos autores e materiais disponíveis, tais como livros, artigos científicos e impressos diversos, entretanto a fonte de pesquisa mais utilizada foram os artigos científicos, tendo em vista a escassez de livros e doutrinas que tratem especificamente do assunto em questão.

1.6. Estrutura do Trabalho

O primeiro capítulo desta monografia apresenta a introdução com a contextualização do estudo, formulação do problema de pesquisa, as hipóteses do estudo, os objetivos gerais e específicos, as justificativas, a relevância e contribuições da proposta de estudo, a metodologia do estudo, bem como definição estrutural da monografia.

O segundo capítulo trata dos aspectos históricos envolvendo a internet no Brasil.

Por sua vez, o terceiro capítulo aborda de forma ampla os cibercrimes, suas características, seus sujeitos, classificações e o lado obscuro da internet.

Já o quarto capítulo aborda trata do Brasil e os cibercrimes, as leis brasileiras que versam sobre estes, além dos reflexos do cibercrime e a eficácia das leis brasileiras atuais.

Por fim, as considerações finais contêm uma breve exposição de toda a monografia, com a resolução de seus objetivos gerais e específicos, trazendo a resolução da problemática e das hipóteses de estudo.

2. A INTERNET NO BRASIL: DO COMEÇO

O pontapé inicial que introduziu a internet no Brasil se deu pela Fundação de Amparo à Pesquisa do Estado de São Paulo – FAPESP, ligada a Secretaria Estadual de Ciência e Tecnologia, que em 1988 realizou a primeira conexão à rede através de uma parceria com um dos mais importantes centros de pesquisa científica dos Estados Unidos, o FERMILAB – Fermi National Accelerator Laboratory. Ainda, na mesma época, a Universidade Federal do Rio de Janeiro (UFRJ) e o Laboratório Nacional de Computação Científica (LNCC) aderiram à internet e conseguiram se conectar por meio de *links* com universidades americanas (VIEIRA, 2003, p.08).

Em meados de 1992 o governo brasileiro juntou-se a crescente expansão da internet e criou a Rede Nacional de Pesquisa (RNP), pelo Ministério da Ciência e Tecnologia (MCT), a qual espalhou pontos de conexão pelas principais capitais do país, criou a infraestrutura de funcionamento da internet e distribuiu o acesso á rede para universidades, fundações de pesquisa e órgãos governamentais no território nacional. Concomitantemente às operações do RNP surgiu uma ONG, IBASE – Instituto Brasileiro de Análise Sociais e Econômicas, que se tornou a primeira instituição brasileira fora do ambiente acadêmico a utilizar a internet, através do Alternex, em 18 de julho de 1989 (VIEIRA, 2003, p.09).

Com tais acontecimentos, aos poucos “A Web, finalmente, ganhava o Brasil.” (VIEIRA, 2003, p.09).

Após tais acontecimentos (VIEIRA, 2003, p.10), nos três anos seguintes, além do gradual crescimento da internet no meio acadêmico e a sua evolução nos Estados Unidos, o que se viu foi uma disputa no Brasil acerca dos direitos de acesso à rede, uma vez que em 1994 o governo feral manifestou interesse e intenção de investir e promover o desenvolvimento da internet no país, por meio de uma ação conjunta entre os Ministérios da Ciência e Tecnologia (MCT) com das Comunicações (MC). Neste sentido, a RNP forneceria a experiência adquirida do meio acadêmico e com a estrutura base, enquanto que a Embratel, na época a empresa do sistema Telebrás responsável por sérvios interurbanos e internacionais, iria explorar comercialmente o acesso à rede.

Contudo, embora naquela época tudo indicasse que a Embratel iria exercer um monopólio estatal do mercado de internet, em 1994 houve a eleição presencial, que trouxe consigo uma agenda política que previa um amplo programa de privações, incluindo a desestatização do setor de telecomunicações. Assim, bastou que Fernando Henrique Cardoso ascendesse ao Palácio do Plano, em 1º de janeiro de 1995, para que a ideia de monopólio estatal do mercado de internet da Embratel serem freados bruscamente (VIEIRA, 2003, p.10).

Em maio de 1995 foi emitida uma declaração conjunta dos Ministérios da Ciência e Tecnologia (MCT) com das Comunicações (MC), determinando que as operadoras estatais não iriam oferecer o acesso à Internet ao usuário final, tarefa esta que caberia à iniciativa privada. O governo naquela época decidiu que as operadoras iriam atender somente o mercado corporativo, devendo fornecer infraestrutura e recursos necessários para viabilizar a montagem de provedores de acesso (VIEIRA, 2003, p.10 e 11).

Em 1996 o governo federal promoveu seu ultimo ato significativo quanto a Internet, criando o Comitê Gestor de Internet (CG), formado por representantes dos Ministérios da Ciência e Tecnologia (MCT) com das Comunicações (MC), universidades, ONGS e provedores de acesso (VIEIRA, 2003, p.11).

Assim, “Nascia a Web brasileira.” (VIEIRA, 2003, p.11).

3. CIBERCRIMES – O PROBLEMA

Com o advento da internet, bens juridicamente relevantes passaram a estar disponíveis e transitarem na internet e no ciberespaço. Essa deslocação de bens, do mundo físico para o virtual, atraiu atenções dos mais variados segmentos da sociedade. Tal deslocação atraiu até mesmo os criminosos, que visualizaram no ambiente virtual grandes possibilidades de auferir vantagens ilícitas em larga escala, de forma segura, sem o uso de violência física e com baixos custos, utilizando-se do anonimato (ANDRADE, 2015).

No ambiente virtual esses delitos ganharam uma nomenclatura: cybercrimes. Tal denominação foi atribuída a todos os crimes cometidos no ciberespaço ou por meio dele (ANDRADE, 2015).

A doutrina, como um todo, quando aborda o assunto dos crimes cometidos na internet ou por meio dela, se dispersa e adota termos diferentes para os crimes cometidos nesta seara, como crimes informáticos, crimes virtuais, crimes digitais, etc. Em consequência a essa ausência de uniformidade, a pesquisa acadêmica acaba sendo prejudicada, ante a grande variação de termos quando se realiza uma consulta (ANDRADE, 2015).

Alguns autores, como ANDRADE (2015), acreditam que a nomenclatura cybercrime seja a mais apropriada quando se trata dos crimes cometidos na internet ou por meio dela, pois se amolda ao modelo internacional de combate a esses crimes, instituído pela Convenção de Budapeste sobre Cybercrimes, modelo este que foi adotado por vários países.

A origem do termo cibercrime esta entrelaçada com o trabalho de um subgrupo das nações do G8, trabalho este que se deu no final da década de 90, em uma reunião em Lyon, na França, que teve como objetivo de análise e discussões os crimes promovidos através de dispositivos eletrônicos ou pela divulgação de dados para a internet. Dessa forma, o termo cibercrime foi oficialmente empregado, entretanto de forma extremamente ampla, uma vez que foi utilizado para descrever todos os tipos de delitos cometidos pela Internet (BARBAI, 2013, p. 48 apud STEPHAINE PERRIN, 2005).

Lado outro, a palavra cibercrime, tal qual utilizada, embora não esteja, ainda, dicionarizada em Língua Portuguesa, é comumente usada pela mídia no Brasil, impressa ou digital (BARBAI, 2013, p. 55).

3.1. Características

Os cibercrimes são cercados de características peculiares que prejudicam e influenciam diretamente na sua análise, investigação, obtenção de provas, combate, punição e

prevenção. DIAS (2010, p. 13 a 17), enumera algumas destas características, sendo elas: a Transnacionalidade e a A-Temporalidade, que trazem a Deslocalização e a Diversidade de Ordens Jurídicas e o Princípio da Territorialidade; além disso, o autor traz outras características, sendo elas: a Permanência; o Automatismo e Repetição; o Anonimato; a Alta Tecnicidade; e por fim a Disseminação e Potenciação dos Danos.

3.1.1. Transnacionalidade e a A-Temporalidade

A primeira e talvez a mais marcante característica do cibercrime seja a sua transnacionalidade, também denominada de caráter transfronteiriço, ou, ainda, extra-territorialidade (DIAS, 2010, p. 13). Essa característica se consubstancia na inexistência de um fator distancia, ou, ainda, de forma mais simplificada, na capacidade de tais crimes serem cometidos dentro de um país e afetar outro. Dificultando ainda mais, o agente consegue aliar a essa característica juntamente com quantidade e velocidade, permitindo realizar enormes transferências de dados em questão de poucos segundos (DIAS, 2010, p. 13). Em consequência a tudo isso:

> A distância continental entre pessoas, dados e serviços reduz-se a um simples clique. Esta característica leva, assim, a um exponencial agravamento dos danos das condutas criminosas, pois podem atingir um número massivo de pessoas e em qualquer lugar que estas se encontrem. (DIAS, 2010, p.13).

Já o caráter a-temporal dos cibercrimes, configura-se na possibilidade de, conforme DIAS (2010, p.14), existir uma separação temporal entre a conduta inicial e o resultado, podendo então ser realizado ataques divididos em fases, “retardados” ou “ao relógio”, como acontecer a sua interrupção, suspensão ou cancelamento fictício. Essa característica é uma das mais apreciadas e aproveitadas pelos criminosos (DIAS, 2010, p.14).

3.1.1.1 Deslocalização

A deslocalização (DIAS, 2010, p. 14 apud VENÂNCIO, p.06, 2006), é a deslocação criminosa para a internet e na internet. Na primeira, nada mais é do que o cometimento de crimes tradicionalmente cometidos por outros métodos, agora são cometidos pela internet. Já a segunda, é a deslocalização de conteúdos entre servidores, para fugir dos moldes da lei, assim, quando detectada alguma atividade proibida ou algum conteúdo ilícito em algum site, por exemplo, quando as autoridades procurassem bloquear o ponto emissor, os cibercriminosos simplesmente transferem aquelas condutas para outro servidor, em outro país,

modificando assim a competência territorial e tornando técnica e juridicamente árdua que as autoridades de um país imponham que servidores de outro país cumpram suas decisões.

3.1.1.2 A diversidade de ordens jurídicas e o princípio da territorialidade

Nos cibercrimes, ante seu caráter transnacional, nota-se a diversidade de ordens jurídicas existentes. Quando se confronta tal diversidade de normas e o princípio da territorialidade (DIAS, 2010, p.15), é possível observar que a qualificações de diferentes tipos de ilícito é outro problema, levando que a um mesmo crime seja aplicado sanções diferentes e paralelamente, que uma conduta possa ser crime em um país e noutro, não, levando à deslocalização.

Quando um crime é cometido é preciso definir qual a lei a ser aplicada, contudo, nos cibercrimes surge outro problema sobre qual lei deveria ser aplicada: a lei onde esta o servidor utilizado para o crime; a lei do local onde o cibercriminoso praticou o crime; a lei onde reside o cibercriminosos; ou as lei(s) do(s) local(is) onde se produziu(ram) os resultados (DIAS, 2010, p.15).

Finalizando, DIAS (2010, p.15) diz que a aplicação do princípio da territorialidade, de forma pura, poderá levar a limitações e ineficácia da investigação e punição dos cibercrimes.

3.1.2. Permanência, Automatismo e Repetição

A permanência do crime é considerada característica principal no cometimento deste e gera o caráter automático e repetitivo da conduta delituosa, provocado o aumento exponencial dos danos. Com o auxilio dessa característica o criminoso manipula o programa informático ou modifica a base de dados, daí a cada novo acesso o computador repete automaticamente o comando ilícito do criminoso, tornando a comissão do crime permanente (DIAS, 2010, p.16).

Por meio do caráter automático e repetitivo, inerente aos computadores e sistemas correlacionados, juntamente com a velocidade e instantaneidade destes, ocorre a multiplicação ilimitada da conduta criminosa, podendo atingir um numero indeterminado de pessoas. (DIAS, 2010, p.16).

Já a possibilidade de repetição favorece a renovação das condutas criminosas, uma vez que detectada uma falha ou brecha na segurança, o cibercriminosos aproveitar-se-á

dela o quanto quiser (DIAS, 2010).

3.1.3. Anonimato

Outra característica dos cibercrimes, e algo apreciado e muito nas redes (DIAS, 2010, p. 16) é a possibilidade navegar, visitar, conversar, realizar comentários, compartilhar textos, imagens e diversos outros tipos dados, além de uma enorme gama de atos, sem ter de se identificar, ou seja, o anonimato.

Em consonância com os dizeres de DIAS (2010, p. 16), os cibercriminosos especializados ou as organizações através deles recorrem desta característica e de técnicas que lhe permitem ocultar ou fraudar sua identidade e as suas condutas, como programas de anonimização e codificação, entre outros, que são aperfeiçoados e transformados diariamente. Ainda, podem os cibercriminosos, além de assegurar o anonimato do agente, ocultar a própria informação, através de mecanismos próprios como encriptação e outros, inclusive muitos disponíveis gratuitamente na rede.

Dessa forma, o cibercriminoso pode "(...) diminuir ou eliminar o risco de ser descoberto ou condenado, apagando todas as provas do ciberrastro" (DIAS, 2010, p. 16).

3.1.4. Alta Tecnicidade

Os cibercrimes, por sua própria natureza, demonstram ser necessário um mínimo de conhecimento especializado acerca da internet, dos computadores e afins. Quando o criminoso possui um elevado conhecimento acerca dessa área, ou seja, uma alta tecnicidade, isso favorece o anonimato, uma vez que os dados podem ser protegidos por programas de encriptação e senhas, de modo que barraram o acesso de terceiros (DIAS, 2010, p.17).

Diante disso, para ser possível a descodificação de dados, manipulação de programas, a identificação do infrator, a busca de rastros das operações virtuais e toda a trama maliciosa, além da recolha de provas digitais passiveis de serem usadas, impõe-se que o investigador destes crimes também possua uma alta tecnicidade, o que torna a investigação tão árdua, aumentando em consequência a impunidade (DIAS, 2010, p.17).

3.1.5. Disseminação e Potenciação dos Danos

A extensa e alta lesividade dos cibercrimes ultrapassa em muito os crimes

tradicionais. Esta situação ocorre devido à rentabilidade deles, uma vez que em relação aos lucros ou benefícios que podem advir do crime, o investimento é mínimo (DIAS, 2010, p.17).

DIAS (2010, p.17), aduz que embora os danos em casos isolados e individuais sejam insignificantes, quando somado os prejuízos de todas as vitimais, pode-se chegar a quantias astronômicas, o autor usa como exemplo a *salami technique* ou a "técnica do salame", que consiste na transferência de pequenas quantias, até mesmo centavos, para a conta do infrator e que quando somadas, perfazem voluptuosas quantias.

DIAS (2010, p.18) apresenta a chamada cifra negra ou obscura, que consiste na quantidade de crimes não levados ao conhecimento das autoridades, e ao adentrar nos cibercrimes, o autor diz que a quantidade elevada de cifra negra tem como causas a ausência de denuncia, a grande tecnicidade, a deficiente segurança, ausência de meios de prevenção, detecção e controle adequados, além da pequena quantidade de detecções e condenações, o que gera o nascimento de um sentimento de imunidade quando se fala dos cibercrimes.

3.2. Os Sujeitos no Cibercrime

3.2.1. Sujeito Ativo – O Cibercriminoso

De acordo com DIAS (2010, p.8), "(...) o cibercriminoso pode ser qualquer um (...)". Dessa forma, quanto ao agente, autor e sujeito ativo dos cibercrimes, não se exige nenhuma qualidade ou condição especial.

Interessante destacar que apesar de qualquer pessoa poder praticar o cibercrime, popularmente, atribui-se a autoria destes crimes aos chamados *hackers.* Contudo, conforme ANANIAS e WANDERLEY (2014, p.38), *hacker* não é o termo mais adequado, haja vista que a expressão inicialmente era usada pra se referir a um individuo com grande habilidade com computadores. Ainda, os autores trazem que tanto para os especialistas no meio como a doutrina preferem se referir aos cibercriminosos como *crackers*, termo este que teria sido criado pelos *hackers*, para não serem confundidos com aqueles.

Os *crackers* possuem claramente intenções ilícitas, como roubo de senhas e espionagem (ANANIAS e WANDERLEY, 2014, p.38).

A não percepção direta do crime, haja vista ser executada pelo computador, a inexistência de presença física do agente e da vitima, a ausência de violência, e, em alguns casos, o anonimato de ambas as partes, facilita o crime, tornando o mais tolerável e com menos riscos para o cibercriminoso (DIAS, 2010, p.8).

DIAS (2010, p.9) realiza uma colocação muito oportuna quanto ao sujeito ativo deste crime, dizendo que embora o perfil do cibercriminoso tenha sido romantizado e descrito como um gênio na área da informativa, computadores e afins, com um Q.I. acima da média, introvertido, antissocial, movido pelo desejo de superação da máquina, esse perfil evoluiu, fazendo surgir novas modalidades criminológicas de delinquentes, não tão jovens ou inteligentes, desprovidos de *tecno-ética* e movidos com o objetivo de extrair informações, usa-la ou vende-la.

3.2.2. Sujeito Passivo – Vitima

Assim como o sujeito ativo do cibercrime, o sujeito passivo não possui condições especiais. Desta maneira, qualquer pessoa pode ser vitima, seja ela uma pessoa física ou jurídica, individual ou coletiva, publicas ou privadas, bastando estar conectado a um sistema ou à rede mundial de computadores (DIAS, 2010, p. 12).

MOURA (2012, p.24) afirma que pesquisas sobre as vítimas dos cibercrimes são unânimes quanto a não confiabilidade de estatísticas. Acrescentando, MOURA (2012, p.24) aduz que:

> Na maioria dos casos a vítima sequer sabe que está sendo atingida pelos agentes. Quando descobrem – observe-se que há uma parcela que continua sem perceber que os crimes estão ocorrendo – preferem calar-se, arcando com os prejuízos sofridos, a estampar páginas de jornais e revistas, admitindo sua vulnerabilidade e perdendo credibilidade, como nos casos de grandes empresários e bancos.

Desta forma, como quaisquer pessoas podem cometer crimes no ambiente cibernético, qualquer indivíduo usuário da rede está sujeito a ser alvo e consequentemente poderá ser vítima (MOURA, 2012, p.24).

3.3. Classificações

As peculiares envolvendo os cibercrimes, suas características, o avanço tecnológico e demais questões a estes atreladas provoca desde os meados da internet diversos debates nos meios acadêmicos e doutrinários, fazendo surgir diversas opiniões e posições e nomenclatura quanto à classificação destes delitos.

3.3.1. Condutas Indevidas Praticadas Na Internet

WENDT e JORGE (2013. p 18), apesar de utilizarem o termo “crimes cibernéticos”, trazem, para fins didáticos, a classificação das “condutas indevidas praticadas na internet”. Tais condutas se subdividem em “condutas cibernéticas atípicas” e “crimes ciberneticos”.

As Condutas Cibernéticas Indevidas Atípicas são aquelas praticadas na internet ou através dela, que, de alguma forma, acarretam transtornos ou prejuízos para as vitimas, contudo, como não existe uma previsão penal especifica no Brasil, não constituem crimes. Encaixa-se nessas condutas a pessoa que, utilizando-se da internet, publica um texto vexatório sobre um desafeto, acarretando violação ao direito da imagem e eventuais reparações civis de ordem moral, contudo, apesar de ser socialmente reprovável, não constitui crime (WENDT e JORGE, 2013. p 19).

Por sua vez, os crimes cibernéticos se dividem em crimes cibernéticos abertos, que são aqueles que podem ser praticados pela forma tradicional ou por meio de computadores, e crimes exclusivamente cibernéticos, que somente podem ser praticados com a utilização dos computadores ou outros recursos tecnológicos que possuam acesso à internet (WENDT e JORGE, 2013. p 19).

3.3.2. Cibercrimes Puros, Mistos e Comuns

NETO e GUIMARÃES (2003, p. 69), apesar de usarem o termo “crime virtual”, trazem uma ótima divisão quanto a estes crimes, podendo então se dividir em puro, misto e comum. Segundo eles, configurar-se-á a forma pura quando “(...) toda e qualquer conduta ilícita (...)” que “(...) tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas.”. Assim, o cibercrime puro seria aquela conduta ilícita voltada para a parte interna de um computador, como o hardware e/ou software, ou seja, são aqueles cibercrimes praticados contra o sistema de computadores em si, seja ele virtual ou físico. Nesta espécie de cibercrimes é que atuam os *crackers,* porém erroneamente conhecidos e chamados pelas sociedades como *hackers*, que, utilizando-se de conhecimentos especializados praticam condutas a seu bel prazer.

Já a forma mista (NETO e GUIMARÃES, 2003, p. 69), seria aquela pratica ilícita em que o uso da internet é uma condição indispensável produzir um resultado naturalístico que de alguma forma ofenda o mundo físico, ameaçando outros bens que não os correlatos a internet ou computadores. Um exemplo desta espécie de cibercrime seria a transferência de valores de contas em bacos.

Por fim, a forma comum dos cibercrimes (NETO e GUIMARÃES, 2003, p. 69) seria a utilização da internet apenas como um instrumento prescindível para pratica de um crime já tipificado pelo ordenamento jurídico. Desta forma, a internet acaba se tornando apenas mais um meio para praticar algum crime. Os autores citam a pornografia infantil como exemplo desta espécie, uma vez que é possível pratica-la através da internet, como a divulgação de conteúdo pornográfico e sites entre pedófilos.

3.3.3. Cibercrimes Próprios e Impróprios

Nessa classificação, nos dizeres de SOUSA (2012, p.12):

> Diremos que são crimes próprios, aqueles praticados através de equipamento de informática visando atingir as suas funções, como por exemplo, provocar lentidão nos sistemas, mudar arquivos de seus locais habituais dificultando assim, sua localização, desconfigurar as características da maquina alvo do delito, ou seja, crimes que dificultem ou impossibilitem a utilização do equipamento de informática.

Ainda, SOUSA (2012, p.13) define que:

> (...) são impróprios os crimes de informática praticados por indivíduos que apenas se utilizam do equipamento de informática como instrumento necessário para cometer o crime. Tais tipos de delitos encontram-se já tipificados na legislação penal pátria e na maior parte das vezes, produzem resultado naturalístico, ou seja, introduz algum a modificação no campo fático, contudo podem ser praticados de outro modo que não seja como auxilio dos meios de informática. São exemplos os crimes de injuria, furto, dentre outros, que já se encontram tipificados em leis penais, podendo ser obviamente praticado de outros modos sem o auxilio da informática.

Assim, pode-se dizer que os cibercrimes próprios são aqueles praticados por meio de um aparelho eletrônico e voltado exclusivamente para ele, suas funções e seus sistemas, enquanto que o cibercrime impróprio seria qualquer crime que utiliza um aparelho eletrônico de forma prescindível, ou seja, de forma dispensável, podendo o crime ser praticado de outra forma que não esteja relacionado a aparelhos eletrônicos ou a internet.

3.4. O Lado Obscuro da Internet: A Deep Web

Nos dias atuais o uso da internet é parte da rotina de diversos usuários, que a utilizam no dia a dia em busca de informações, serviços e entretenimento. Entre os principais meios utilizados para acessar sites, encontram-se os buscadores, que possuem milhões de paginas em seus bancos de dados, sendo o Google, atualmente, o maior agregador de informações na Web (SOARES, 2017, p. 33 e 34). Porém, uma parte da internet se encontra fora do alcance dos buscadores normais, possuindo vários outros sites, fóruns, blogs e afins

escondidos das ferramentas de indexação de conteúdo dos buscadores. Essa área que não pode ser localizada pelos buscadores normais é chamada de *Deep Web* (SOARES, 2017, p.34).

Oportunamente, é necessário distinguir a *Deep Web* da *Dark Web*, dois conceitos bastante confundidos. A *Deep Web*, em síntese, é toda a região da *World Wide Web* que não aparece nos resultados dos buscadores de conteúdo padrão. A *Dark Web*, por seu turno, é uma fração da *Deep Web* que intencionalmente se mantem fora dos mecanismos de busca, com o intuito de que suas comunicações não sejam violadas por terceiros (CALDERON, 2017, p.06).

A *World Wide Web*, uma das varias camadas da internet, é o canal de comunicação que permite a possibilidade de rastreamento e identificação de pessoas e mensagens por terceiros. É uma região pouco mais transparente (CALDERON, 2017, p.35). Esta camada superficial, conhecida por *Surface* Web, é aquela parte da internet que se encontra disponível para todos e para a indexação dos buscadores normais. Aqui os resultados das pesquisas são mostrados por meio de links (ANDRADRE, 2015).

Por seu turno, a *Deep Web* é uma expressão original da língua inglesa, que traduzida significa “Internet Profunda” (BERNARDES, 2016, p.10).

Já a *Dark Web* é àquela parte da *World Wide Web* que intencionalmente não deseja ser encontrada, inspecionada, vigiada ou controlada por quaisquer entidades que circulam a internet (CALDERON, 2017, p.06).

A *Deep web* é cercada de mitos e simboliza uma área da internet que é alvo de muitas ressalvas e criticas em matérias jornalísticas, websites, blogs e afins (SOARES, 2017, p.34). E refere-se àquele conteúdo que está na internet, contudo, por diversas razões, não pode ser ou não é encontrado por mecanismos de busca normais, ou seja, é classificado como invisível, pois todo o seu conteúdo não é de fácil ou livre acesso a qualquer um, além do fato de que os próprios criadores desses conteúdos querem dificultar o acesso a eles (BERNARDES, 2016, p.11).

Acrescente-se que a *Deep Web* é um ambiente extenso, sendo 500 vezes maior que a “*surface*” - internet convencional, e é conhecida por ser separada em camadas, de tal forma que quanto mais profundo se pretende acessar, mais sigiloso e perigoso será o conteúdo encontrado (BERNARDES, 2016, p. 11).

Nesse sentido, pode-se fazer uma comparação da Deep Web e Surface Web através de um iceberg (BERNARDES, 2016, p. 11):

FIGURA 1 – REPRESENTAÇÃO DA INTERNET EM FORMA DE ICEBERG

Fonte: http://info.brandprotect.com/blog/myths-and-truths-about-the-dark-web

A figura do iceberg, como representação visual, começa com uma pequena área exterior que encontrar-se exposta aos olhos, essa fração da Internet, mais superficial, corresponde ao espaço mais conhecido (SOARES, 2017, p.34). Desta forma, a internet seria muito maior do que se vislumbra inicialmente, sendo composta de diversos locais que nem todos os usuários têm acesso e indo desde a superfície com áreas comuns a todos até extensões mais profundas de navegação restrita, atividade hacker, cibercrimes e mercados paralelos (SOARES, 2017, p.35).

Realizando uma simples busca em qualquer navegador comum, é possível constatar um pouco dos grandes mistérios que a *Deep web* tem. Qualquer individuo desavisado, ao se deparar com este termo e busca-lo, ira encontrar como resultado imagens macabras e horripilantes, textos com conteúdo deturbado, arquivos de origem duvidosa e todo o tipo de conteúdo que desafiam a imaginações mais férteis (ANDRADE, 2015). Nesse sentido:

> Na Deep web encontra-se de tudo. É possível, por exemplo, contratar assassinos de aluguel, comprar cartões de créditos roubados e/ou furtados, é onde se abrigam os maiores exploradores de pornografia infantil, sites de venda de órgãos humanos,

> armas químicas e de uso exclusivo das forças armadas, com destaque para o comércio de drogas que é altamente estruturado, difundido e rentável, grupos terroristas articulam-se nos fóruns secretos, grupos que discutem técnicas para matar pessoas por meio de práticas satânicas e dos mais variados tipos de parafilias (ANDRADE, 2015).

No ambiente interno da D*eep web*, além das dificuldades técnicas inerentes à camada, o poder coercitivo dos Estados não consegue atingir a efetividade, pois "É um ambiente onde o caos tecnológico se opera em virtude da topologia da rede, bem como as leis encontram diversas dificuldades de aplicação, é um ambiente onde se abrigam os mais nocivos grupos de cibercriminosos." (ANDRADE, 2015).

Porém, oportuno se faz destacar que apesar de a *deep web* agregar todo o tipo de conteúdo prejudicial e criminoso, existe uma quantidade colossal de informações de alta relevância nessa camada (ANDRADE, 2015).

Quando se volta a falar sobre a problemática dos cibercrimes no Brasil, Leandro Andrade ressalta que:

> O problema no Brasil é que se imiscuem nesse debate interesses nefastos, escusos e danosos à sociedade. Dessa forma, temos a elaboração de leis frágeis, com lacunas jurídicas e técnicas e inócuas que propiciam a insegurança jurídica e que terminam fomentando os cybercrimes. (ANDRADE, 2015).

No Brasil, infelizmente, há um grande atraso por parte do Ordenamento Jurídico (ANDRADE, 2015). De tal forma que:

> O legislador pátrio espera em berço esplêndido que as definições ocorram no exterior para depois debater os mesmos pontos, achar as mesmas soluções, dando uma nova roupagem e apresentando como solução original e inovadora. (ANDRADE, 2015).

Essas manobras por parte do legislador pátrio deixam o país em uma situação precária perante a comunidade internacional, uma vez que o país possuí uma dimensão continental, com forte inclusão digital e escassas leis para regular as demandas cibernéticas. Tais condições fazem do Brasil um dos países preferidos pelos cibercriminosos, tanto para vitimar os nacionais, quanto na promoção do cibercrime direcionado a vítimas de outros países (ANDRADE, 2015).

4. O BRASIL E OS REFLEXOS DOS CIBERCRIMES

A morosidade legislativa no Brasil é uma grande característica do Congresso Brasileiro, de tal forma que em matéria tão volátil quanto o ciberespaço essa lentidão produz resultados negativos (ANDRADE, 2015).

O Brasil possuí um cenário favorável aos cibercrimes, uma vez que o lucro nesses crimes é rápido e o investimento pátrio para coibir e perquirir esses tipos de crimes ainda são muito acanhados, o que acaba incitando os cibercriminosos a cometerem cada vez mais delitos na web (BERNARDES, 2017, p.13). Nesse sentido:

> Legislar sobre um plano pouco conhecido, com características efêmeras, que envolvem tecnologia de ponta e soberanias dos países é tarefa extremamente complexa. Existem muitas variáveis a serem observadas, lacunas técnicas que devem ser preenchidas e interesses dos mais diversos setores da sociedade que devem ser contrapostos, objetivando um equilíbrio saudável. (ANDRADE, 2015)

O mundo se encontra cada vez mais interconectado e globalizado, de tal forma que a criminalidade e a necessidade de identificar e punir o criminoso não se limita mais somente ao mundo físico, mas também ao mundo virtual (BERNARDES, 2017, p.24).

A legislação brasileira que atua como meio de punibilidade pelo Estado, por ser precária, possibilitou que a criminalidade avançasse mais rapidamente do que o ordenamento jurídico quanto ao tema. Dessa forma condutas criminosas estão cada vez mais sofisticadas, enquanto que os meios para se chegar até o agente do crime ainda se encontram em aprimoramento pelo estado, provocando uma insatisfação popular e muitas vezes a impunidade dos infratores cibernéticos.

Quanto ao atraso normativo brasileiro pode-se citar, por exemplo, o atual Código Penal, que é oriundo de 1940. Neste ponto fica fácil constatar que algumas legislações brasileiras, por estarem vigentes há décadas, não conseguiram acompanhar o recente processo de desenvolvimento tecnológico.

Devido ao avanço das tecnológicas, nos dias atuais se mostra difícil, se não, até mesmo raro não encontrar alguém que utilize algum aparelho tecnológico que possua acesso à internet e ao seu vasto mundo de possibilidades. Exemplificando, dados extraídos do *site* do IBGE[1], apontam que no ano de 2016 constatou-se o crescimento do uso da internet em ambiente domestico, chegando a ser utilizada em 69,3% dos 69.318 mil domicílios particulares permanentes do País na época da pesquisa.

A crescente dependência que a sociedade esta criando em relação à internet parece não ter sido prevista pelo ordenamento jurídico Brasileiro, uma vez que, a internet tendo chegado ao território brasileiro em 1988, mesmo que de forma primitiva, as primeiras

[1] www.ibge.gov.br

legislações especificas para lidar com os crimes ali cometidos só foram sancionadas em 2012, depois de muitas vitimas, quando um caso especifico tomou conta do brasil. Trata-se da Lei nº 12.737/2012, apelidada pelos brasileiros de Lei Carolina Dieckmann, que "Dispõe sobre a tipificação criminal de delitos informáticos (...)"[2].

Inegavelmente, o grande despreparo do Direito brasileiro de amparar tal situação decorre do modo como o Estado e sociedade brasileira estão acostumados a lidar com seus problemas: criando-se leis depois de reiterados e visíveis problemas, e, principalmente, após um caso especifico tomar conta da sociedade, da mídia e mostrar-se a evidente necessidade de cuidar de determinado problema, como foi o caso da atriz Carolina Dieckmann que teve fotos intimas divulgadas na internet em 2011. Logo, ante a demora estatal em se regular tal situação, ficou evidente a situação de risco que o Brasileiro encontrava-se.

No Brasil era gritante o problema quando se buscava na legislação pátria um amparo para poder tipificar um cibercrime. Porém, algumas condutas que podem ser praticadas através da internet – cibercrimes comuns, já se encontram reguladas pelo Código Penal e pelo poder Legislativo Brasileiro.

Em 2013 houve o inicio do vigor das leis 12.735/12 e 12.737/12, que modificaram o Código Penal para, então, enfim, passar a tratar de crimes cibernéticos e, ainda, dando outras disposições. Logo no ano seguinte, em 2014, o Brasil, aproveitando-se da grande discussão que estava ocorrendo naquela época acerca da internet e os direitos ali inseridos, promulgou o Marco Civil na Internet, lei 12.965/2014.

4.1. O Direito Brasileiro e a Internet

A expansão da internet, que se deu mais ferozmente do que se podia imaginar em sua criação, surpreendeu os juristas do mundo e os colocou em buscas de soluções para os crescentes e cada vez mais frequentes problemas virtuais.

O Brasil, até o ano de 2012, se encontrava desprovido de legislações hábeis para lidar com os crimes ocorridos na rede mundial de computadores, tornando repressão destes acontecimentos árdua, visto que a legislação até aquele momento vigente era direcionada aos crimes em geral, pouco importando o meio utilizado para a consumação do crime. Aqui, podemos citar a utilização, dentre outros, do Código Penal (CP), da Lei dos crimes de software (ou lei antipirataria, Lei n. 9.609/98), do Estatuto da Criança e do Adolescente (Lei

[2] www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

n. 8.069/90) e da Lei de Segurança Nacional (Lei nº 7.170/83) (SILVEIRA, 2015).

Consequentemente a não existência de legislação especifica, tornava-se difícil a individualização da conduta, dos sujeitos e das provas para uma eventual condenação penal, esta, por sua vez, que exige certeza dentre outros elementos, como autoria, materialidade e etc. (SILVEIRA, 2015).

4.1.1. Lei nº. 12.735/2012 – "A Lei Azeredo"

Criada com a intenção de se coibir a pratica de crimes na rede, a lei Azeredo, nomeada assim em homenagem ao ex-senador que criou o projeto de lei - PL-84/99 (PAGANOTTI, p.126), tem como escopo "(...) tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares.(...)"[3].

Ainda, o artigo 4º desta lei estabelece que a polícia judiciária deverá estruturar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Embora esta lei tenha sido criada para, de certa forma, ser extravagante, recebeu alterações, com o fim de fazer com que seus artigos fizessem parte de tipos penas já existentes à época (OLIVEIRA, 2013, p. 34).

Conforme colocação de OLIVEIRA (2013, p.34), a integração da lei Azeredo simbolizou o pensamento inicial sobre as punições dos cibercrimes utilizando-se apenas dos tipos penais já existentes no ordenamento pátrio.

4.1.2. Lei nº. 12.737/2012 – "Lei Carolina Dieckmann"

Em maio de 2012 um grande alvoroço tomou conta da mídia nacional. Naquele mês ocorreu a divulgação de imagens da vida privada da atriz Carolina Dieckmann em diversos *sites*, ocasionando uma comoção social (SILVEIRA, 2015).

Este acontecimento abriu a oportunidade e conveniência da edição da Lei nº 12.737, de 30/11/2012, apelidada pela mídia de "Lei Carolina Dieckmann", inclusive sendo tal apelido aceito pela sociedade e é como ficou conhecida. Esta lei, dentre outras providências, versa sobre a tipificação criminal dos delitos informáticos, introduziu os artigos

[3] www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm

154-A, 154-B, e alterou os artigos 266 e 298, todos eles do Código Penal (SILVEIRA, 2015).

O crime de "Invasão de Dispositivo Informático", previsto no artigo 154-A do CP configura-se quando alguém "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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" [4]. O crime em questão é comum, doloso e pode-se consumar com uma ou mais conduta e admite a tentativa (SILVEIRA, 2015).

O § 1º, do artigo 154-A do CP, prevê uma forma equiparada do crime, punindo com a mesma pena do "caput" quem "(...) produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput", possuindo as mesmas características do "caput" do artigo 154-A do CP (SILVEIRA, 2015).

Já o § 2º do artigo 154-A do CP prevê causa de aumento de pena de um sexto a um terço, quando há prejuízo de caráter econômico para a vítima, sendo aplicada somente para a forma simples do delito (SILVEIRA, 2015).

Por sua vez, o § 3º do artigo 154-A do CP prevê pena e regime prisional diferenciado – reclusão, quando a invasão possibilitar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido (SILVEIRA, 2015).

Finalizando o artigo 154-A, os parágrafos 4º e 5º, I a IV, do CP, trazem causas de aumento de pena, aplicáveis quando ocorrer a forma qualificada do crime – §3º, artigo 154-A, CP (SILVEIRA, 2015)..

A Lei 12.737/2012, modificando o artigo 266 do CP, estabeleceu, por meio do §1º que incorre na mesma pena do caput daquele deste artigo quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. Ainda, aplicar-se-á em dobro a pena quando o crime for cometido em estado de calamidade publica (§2º, artigo 266 do CP).

Por fim, a Lei 12.737/2012 acrescentou que, para fins de aplicação penal, equipara-se a documento particular o cartão de crédito ou débito (paragrafo único, artigo 298, CP).

[4] Art. 154-A do Código Penal Brasileiro

4.1.3. Lei nº. 12.965/2014 – O Marco Civil da Internet

A lei 12.965/2014, conhecida como Marco Civil da internet, é a lei que finalmente trouxe a regulamentação do uso da internet no Brasil, estabelecendo fundamentos, princípios, garantias, direitos e deveres para quem utiliza a rede, além de diretrizes para atuação do Estado brasileiro quanto ao tema[5].

A promulgação dessa lei se deu após a ocorrência dos incidentes de ciberespionagem de autoria do Governo norte-americano tendo como alvo os chefes de estados de outros países, dentre eles a presidente do Brasil na época da promulgação da lei, Dilma Rousseff (ANDRADE, 2015).

A situação envolvendo a espionagem da Presidente da República e a promulgação do Marco Civil da Internet mostrou "(...) mais um episódio clássico onde as leis brasileiras são calcadas no caso concreto ao invés de se estabelecerem pelas regras gerais do direito." (ANDRADE, 2015).

O Marco Civil disciplina o uso da internet no Brasil, trazendo como fundamento o respeito à liberdade de expressão e estabelecendo princípios, garantias, direitos e deveres para o uso da internet, de tal forma que a mídia Brasileira considera a lei como a Constituição da Internet (ANDRADE, 2015).

A Lei nº. 12.965/2014 não é uma ilha normativa deserta, fechada às demais fontes jurídicas, na verdade, ela é um das varias fontes normativas que disciplinam o comportamento dos indivíduos no mundo virtual (OLIVEIRA, 2014, p.05).

Os demais diplomas legais não serão ignorados, mas serão igualmente estimados na regulação dos fatos jurídicos cibernéticos, previsão do parágrafo único do art. 3º e o art. 6º da lei (OLIVEIRA, 2014, p.05), que estabelecem, respectivamente que:

> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.
>
> Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

Assim, eventuais conflitos entre o Marco Civil da Internet e outros diplomas legais:

> (...) não deverão ser buscados apenas nos critérios tradicionais de solução de

[5] www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

> antinomias (como o da especialidade e o cronológico), mas também na moderna teoria do Diálogo das Fontes, fartamente acatada pela doutrina e pela jurisprudência do STJ. (OLIVEIRA, 2014, p.06)

OLIVEIRA (2014, p. 06) aduz que a Constituição Federal, sendo a lei fundamental do Brasil, dá as coordenadas principiológicas incontestes do ordenamento jurídico, pela qual tramitarão as interpretações que irão emanar do Marco Civil da Internet.

4.2. A eficácia da Legislação Brasileira

O gigantesco numero de usuários da internet, que a cada ano aumenta ainda mais, além de acrescer a quantidade de vítimas faz com que as investigações se tornem mais árduas, haja vista que a maior parte dos usuários são pessoas leigas que têm acesso à internet antes de sequer entender os riscos que ela possui.

A tarefa árdua dos Estados para a prevenção, a investigação, a perseguição, a comprovação da autoria e a punição do cibercriminoso, além de uma característica do cibercrime, também é consequência de todas as demais características dele. Essa situação facilita a propagação destes crimes e dificulta a sua investigação.

O Estado Brasileiro, acostumado a lidar com seus problemas com a criação de leis depois de reiterados casos e o clamor social, se deparou com o real problema dos cibercrimes e começou a posicionar frente a eles. Entretanto, quando o Direito brasileiro necessitou de amparo para punir e resguardar certos direitos relativos a internet, não havia legislações ou um aparato legal hábil para isso, como foi o caso da atriz Carolina Dieckmann e, também, é o caso da ex-presidente, Dilma Rousseff, que foi alvo de ciberespionagem praticada pelo Governo norte-americano.

Os cibercrimes assim como as tecnologias envolvendo a internet e os computadores evoluem lado a lado e em um ritmo surreal, todavia, o Brasil, como já dito, possui uma enorme lerdeza legislativa, principalmente quanto aos cibercrimes. Exemplificativamente, houve a necessidade de acorrer alguns cibercrimes que gerassem comoção nacional para promulgar legislações sobre o tema para só então o Brasil passar a regular os direitos e deveres dos usuários da internet em âmbito nacional e penalizar os cibercriminosos.

É sabido que um dos primeiros passos para se combater um crime é a criação de uma legislação adequada à situação e que preveja as condutas criminosas e as suas sanções. Contudo, não basta apenas a criação de leis, é necessário também um sistema nacional para a

realização do combate aos cibercriminosos. Atualmente, no Brasil há apenas 16 (dezesseis) delegacias especializadas ao combate dos cibercrimes (SAFERNET, 2016). Porém, apenas estas 16 (dezesseis) delegacias especializadas não se mostram suficientes para amparar todo o território nacional.

Além disso, embora as legislações existentes tenham sido criadas de forma muito bem intencionada, elas apresentam falhas, pois, por exemplo, não estabelecem a competência de fiscalização ou punições para as entidades que as descumprirem.

Alguns dos principais problemas quando se trata dos cibercrimes e a sua investigação são "(...) falta de legislação adequada, a falta de metodologia no tratamento da especificidade deste crime, a interoperatividade dos sistemas, e a lentidão da cooperação e falta de partilha de informações tanto entre entidades nacionais diferentes como ao nível internacional." (DIAS, 2010, p. 18).

No Brasil, o combate aos cibercrimes apenas iniciou-se e fica evidente que muito há de feito, uma vez que o estado encontra-se desprovido de meios adequados para a repressão deste mal.

Neste ponto interessante se faz desacatar a existência da SaferNet [6], uma associação civil de direito privado, com atuação nacional, fundada em 2005, com a missão de defender e promover os direitos humanos na Internet e parceria com o Ministério Publico Federal. Esta associação atua recebendo denuncias de cibercrimes contra os direitos humanos e, conforme dados fornecidos em seu *site*[7], durante os 12 anos de existência, forneceu no Brasil 15.983 atendimentos e recebeu 3.925.405 denúncias anônimas, todos relacionados aos cibercrimes.

Apesar de na ultima década o Brasil estar iniciando o seu combate ao cibercrime, com a criação de leis especificas e com o auxilio de alguns órgãos, como as delegacias especializadas e a SaferNet, ainda há um longo caminho a ser percorrido, uma vez que o combate como está ocorrendo ainda não é o bastante para fornecer aos Brasileiros a proteção que necessitam.

5. CONSIDERAÇÔES FINAIS

[6] safernet.org.br/site/institucional
[7] indicadores.safernet.org.br/indicadores.html

Como visto nesta monografia, os cibercrimes revestem-se de uma serie de características que os tornam atraentes para pessoas maliciosas, tendo isso refletido no aumento dos cibercriminosos e no numero de vitimas.

As dificuldades legais quando se trata destes crimes tem seu ápice quanto ao o que se tenta regular, uma vez que parece sequer ser possível definir com exatidão o local onde estes crimes ocorrem ou ainda, quais os possíveis meios que são cometidos.

A enorme divergência de definições, meios de cometer estes crimes, as controvérsias que existem no meio digital e consequentemente nos cibercrimes fazem com que qualquer legislação apresente dificuldades quanto a correta tipificação, ocorrendo então a tipificação insuficientes a amparar os interesses coletivos, sendo que o que se tenta tipificar são diversas condutas ilícitas, mal tipificadas e em constante mutação, que decorrem de um ambiente virtual mal definido e cheio de brechas.

Ainda, os cibercrimes estão cada vez mais organizados, muitas vezes os cibercriminosos estão mais avançados que os Estados e as vitima, soma-se a isso o fato de os cibercrimes possuírem um caráter internacional e percebe-se a enorme dificuldade que qualquer estado possui em combater tal pratica criminosa.

As autoridades e os Estados se vêm diante de uma enorme problemática, que pode ser resumida em uma simples frase: o avanço tecnológico. Diante dessa problemática surgem duvidas como, por exemplo: De que forma pode-se anteceder os cibercrimes, uma vez que estes estão em constante evolução e adaptação?

A evolução tecnológica, embora traga benefícios para a sociedade, também permitir inovações criminais, estando os crimes cada vez mais sofisticados, dificultando a já imensa tarefa de regulamentação. Assim, quando do combate aos cibercrimes, não é simples preencher o tipo penal, ou seja, cumprir todos os requisitos da legislação para que configure crime e uma eventual pena possa ser aplicada, ainda mais que a lei muitas vezes está desajustada da realidade.

A situação do Brasil frente aos cibercrimes é grave, uma vez que embora a internet esteja no mundo há algumas décadas, as legislações de âmbito nacional foram criadas apenas nos meados de 2012, demonstrando o enorme atraso que o Brasil possui com relação ao tema.

Nesse ponto, é possível elencar os reflexos dos cibercrimes no ordenamento jurídico brasileiro, quais sejam, a Lei 12.735/2012 – “A Lei Azeredo”, a Lei 12.737/2012 – “Lei Carolina Dieckmann” e por fim a Lei 12.965/2014 – O Marco Civil da Internet, que

versam especificamente acerca da internet ou dos cibercrimes em sim, além de modificarem o Código Penal.

Ainda, entre os reflexos dos cibercrimes no ordenamento jurídico pátrio soma-se a clara intenção do legislador brasileiro de, embora tardiamente, resguardar e proteger os interesses que agora migraram do ambiente físico para o virtual.

Contudo, criação de instrumentos jurídicos, como é sabido, é um processo burocrático e bastante moroso, desta forma, não consegue acompanhar todas as peculiaridades dos cibercrimes, ou seja, o formalismo da lei não consegue de forma eficaz opor-se à criatividade dos cibercriminosos e às inovações tecnológicas.

Tendo em vista o aumento indiscriminado dos crimes cibernéticos, é necessário que o Estado providencie maneiras eficazes para combater essa nova criminalidade, criando órgãos novos e/ou otimizando aqueles existentes, além de criar legislações que sejam capazes de evitar a impunidade.

Ainda mais, é necessário que o Estado Brasileiro abandone o seu individualismo normativo quando se trata de combate aos cibercrimes, uma vez que ante o caráter transnacional deles, apenas poucos meios nacionais de prevenção, contenção e combate a esses crimes não se mostra a melhor e mais racional medida. Desta maneira, é necessário que o Brasil faça parte dos Tratados internacionais que tratem especificamente sobre os cibercrimes e sua punição, além da cooperação internacional.

Além disso, primordialmente, é preciso que o Estado Brasileiro alerte e consciente a sua população quanto aos perigos da internet, além, é claro, de como fugir das armadilhas criadas pelos crackers.

É necessária também a adoção de uma forma mais flexível e hábil de coibir a pratica e estes crimes, permitindo um combate em tempo real, que possa possibilitar a imediata coleta de provas.

Por fim, algumas das soluções para combater este tipo de criminalidade são as prevenções, a formação especializada dos profissionais que se dedicam a esta área; investimento acompanhado de recursos adequados; uniformização nacional de combate e cooperação; além, da cooperação internacional.

REFERÊNCIAS

ANANIAS, Ricardo A. R. e WANDERLEY, Lucas F.. **Delito Informático e a Lei 12.737/12 (Lei Carolina Dieckamnn)**. In: (Vários) **Anais do IV Congresso De Ciências Jurídicas: Jurisdição, Estado e Cidadania e VII Encontro Científico do Curso de Direito.** 2014. Disponível em: <consensusjuridico.com.br/anais/ANAIS2014.pdf>. Acesso em 02 de Jan de 2018.

ANDRADE, Leonardo. **Cybercrimes na deep web: as dificuldades de determinação de autoria nos crimes virtuais.** Jus.com.br, 2015. Disponível em: <jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicasde-determinacao-de-autoria-nos-crimes-virtuais/2>. Acesso em: 02 de fevereiro de 2018.

ARAS, Vladimir. **Crimes de informática - Uma nova criminalidade**. 2001. Disponível em: <jus.com.br/artigos/2250/crimes-de-informatica/1>. Acesso em 21 de novembro de 2017.

BARBAI, Marcos A. **A criminalidade no espaço digital**: a formulação do sentido. In. DIAS, Cristiane. Formas de mobilidade no espaço e-urbano: sentido e materialidade digital [online]. Vol. 2, 2013. Disponível em: <https://labeurb.unicamp.br/livroEurbano/volumeII/arquivos/pdf/eurbanoVol2_MarcosBarbai.pdf>. Acesso em 02 de Fevereiro de 2018.

BERNARDES, Victor de Freitas. **Dos crimes virtuais cometidos se utilizando do anonimato da deep web**. 2016. 30 f. Monografia (Graduação em Direito) – Universidade Católica de Brasília, Brasília, 2016. Disponível em: <https://repositorio.ucb.br/jspui/handle/123456789/9433>. Acesso em 21 de maio de 2018.

CALDERON, Barbara**. Deep e Dark Web**: A internet que você conhece é apenas a ponta iceberg. Alta Books Editora, 2017.

DIAS, Vera Elisa M. **A Problemática da Investigação do Cibercrime**. 2010. Disponível em <www.verbojuridico.net/doutrina/2011/veradias_investigacaocibercrime.pdf>. Acesso em 20 de maio de 2018.

FERREIRA, L. P. (10 de julho de). **OS "CRIMES DE INFORMÁTICA" NO DIREITO PENAL BRASILEIRO**. 2013. Disponível em: <www.egov.ufsc.br/portal/conteudo/os-%E2%80%9Ccrimes-de-inform%C3%A1tica%E2%80%9D-no-direito-penal-brasileiro>. Acesso em 21 de novembro de 2017.

MOURA, PÂMELA A. R.. **Crime Cibernético E Seus Aspectos No Universo Jurídico**. 2012. Disponível em: <http://ftp.unipac.br/site/bb/tcc/tcc-388a1273480aa73d54b0c9bb36ffff61.pdf>. Acesso em 20 de maio de 2018.

NETO, Mário Furlaneto e GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional**. 2003. Disponível em: <www.jf.jus.br/ojs2/index.php/revcej/article/view/523/704>. Acesso em: 10 de maio de 2018.

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos Principais da Lei nº 12.965, de 2014, o Marco Civil da Internet**: subsídios à comunidade jurídica. Disponível em: <www.senado.leg.br/estudos>. Acesso em 29 de abril de 2018.

OLIVEIRA, Jôline Cristina. **O Cibercrime e as Leis 12.735 e 12.737/2012.** 2013. Disponível em <www.conteudojuridico.com.br/pdf/cj045489.pdf>. Acesso em 30 de Maio de 2018.

PAGANOTTI, Ivan. **Pressão virtual e regulamentação digital brasileira: análise comparativa entre o Marco Civil da Internet e a Lei Azeredo**. Disponível em <revistacomsoc.pt/index.php/cecs_ebooks/article/download/1690/1627>. Acesso em 02 de Fev. de 2018.

PINHEIRO, E. P. **Crimes Virtuais: Uma Análise da Criminalidade Informática e da Resposta Estatal**. 2006. Disponível em: <www.egov.ufsc.br/portal/sites/default/files/emeline.pdf>. Acesso em 21 de novembro de 2017

PINHEIRO, R. C. **Os cybercrimes na esfera jurídica brasileira**. 2000. Disponível em: <jus.com.br/artigos/1830/os-cybercrimes-na-esfera-juridica-brasileira>. Acesso em 21 de nov. de 2017.

SAFERNET. **Delegacias Cibercrimes**. 2016. Disponível em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>. Acesso em: 30 de Abril 2018.

SILVEIRA, Artur Barbosa da. **Os crimes cibernéticos e a Lei nº 12.737/2012**. Conteúdo Jurídico, Brasília – DF: 22 jan. 2015. Disponível em: <www.conteudojuridico.com.br/?artigos&ver=2.52253&seo=1>. Acesso em: 12 fev. de 2018.

SOARES, Welington. **Investigando relações entre a deep web e a web**: uma análise do mito associado à internet profunda a partir do hacktivismo. 2017. 206 f. Dissertação (Mestrado em Comunicação e Linguagens) - Universidade Tuiuti do Paraná, Curitiba, 2017. Disponível em: <tede.utp.br:8080/jspui/handle/tede/1226>. Acesso em 21 de maio de 2018.

SOUSA, George de Oliveira. **Os crimes cibernéticos e suas formas de combate**. 2012. Trabalho de Conclusão de Curso (Graduação em Direito)- Universidade Estadual da Paraíba, Campina Grande, 2012. Disponível em: <dspace.bc.uepb.edu.br/jspui/handle/123456789/5387>. Acesso em 21 de maio de 2018.

VIEIRA, Eduardo. **Os bastidores da Internet no Brasil** – Editora Manole Ltda., 2003.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos: Ameaças e procedimentos de investigação**. – 2. ed. Rio de Janeiro: Brasport, 2013.