REVISTA CIENTÍFICA ELETRÔNICA DO CURSO DE DIREITO – ISSN: 2358-8551
13ª Edição – Janeiro de 2018 – Periódicos Semestral

CRIMES CIBERNÉTICOS E A FALSA SENSAÇÃO DE IMPUNIDADE

CRUZ, Diego [1]
RODRIGUES, Juliana[2]

RESUMO

Roubo de dados e de identidade, calúnia, difamação, bullying, crimes financeiros, pornografia e pedofilia infantil, verbos estes que constituem os crime cibernético praticado no Brasil, de modo que o presente artigo aborda classificação e características das práticas criminosas realizadas através da internet, inclusive traz garantias fundamentais garantidos pela constituição federal, e destaca a sensação de impunidade que os cidadãos de bem sentem com o crescente aumento dos crimes virtuais em todo o Brasil, de modo que tenta esclarecer o fato causador da sensação de impunidade e uma possível solução para a não ocorrência dos cybercrimes ou a diminuição deste.

Palavras – Chave: Crimes, Crimes Cibernéticos, Crimes Virtuais, evolução, globalização.

ABSTRACT

Data theft and identity, defamation, slander, bullying, financial crimes, pornography, pornography and child pedophilia, these verbs that make up the cybercrime practiced in Brazil, so this article discusses classification and characteristics of criminal practices carried out through the internet, including brings fundamental safeguards guaranteed by the federal constitution, and highlights the sense of impunity that the citizens feel regarding the growing number of cybercrime in make Brazil, so that attempts to clarify the causative fact the feeling of impunity and a possible solution to the non-occurrence of cybercrimes or decrease this.

Key-words: Keywords: Crimes, cybercrimes, evolution, globalization, Virtual crimes.

1. INTRODUÇÃO

A história ensina que o progresso é inerente ao homem, e que fomos feitos para evoluir e inovar e incondicionalmente buscar o avanço, contudo com muitos avanços pode-se ter também o retrocesso, em que no meio de tantos benefícios, indivíduos procuram oportunidades para se beneficiar com a falta de conhecimento do que é novo. Desta forma nos deparamos com

[1] Discente do curso de Direito da Faculdade de Ensino Superior e Formação Integral de Garça– FAEF.
[2] Docente do curso de Direito da Faculdade de Ensino Superior e Formação Integral de Garça - FAEF.

a internet, e com os crimes que a envolvem. Vale ressaltar que a internet é um instrumento considerado hoje como o mais benéfico já desenvolvido, em razão das facilidades que proporciona, a título de exemplo compras realizadas através de computadores com internet em que se tem a comodidade e segurança de não sair de casa e poder se comunicar com familiares e amigos em todos os lugares.

No primeiro capítulo será abordado aspectos relevantes ao tema, como o que é a internet e ainda a sua origem, pois muito pouco se sabe de como ela se originou. Também será abordado neste capitulo um breve relato histórico dos crimes e penas, pois como se poderia falar de crimes cibernéticos sem antes trazer conceituar o que é crime e em que momento se pode apontar quando se iniciou e ainda a única solução que foi encontrado até o presente momento para evita-lo, ou seja, as penas. Que através da leitura deste capítulo poderá vislumbrar, que onde havia crimes ou condutas repudiadas pelas sociedades, tribos a solução para tais atos eram as penas.

O segundo capítulo retrata a norma mais importante no Brasil, a constituição federal e a proteção que ela traz acerca da utilização da rede de computadores, tais como a inviolabilidade de dados, e o direito à privacidade. Já o terceiro capítulo apresenta os crimes cibernéticos em espécie, classificando os sujeitos que comentem o ato antijurídico e a classificação dos crimes mais frequentes no brasil com as devidas tipificações e sansões.

E como fechamento da monografia a quarto capítulo apresenta a problemática enfrentada pelo judiciário diante aos crimes cibernéticos, sendo especificado a constituição do judiciário e um breve resumo do procedimento penal, para compreensão do porque se tem a falsa sensação de impunidade.

2. CRIMES CIBERNÉTICOS

Diariamente conectamos aparelhos à Internet, podendo assim afirmar que no século XXI a vida das pessoas está inteiramente interligada com a rede de computadores, seja para acessos a sistemas de interação como o Facebook, mensagens de e-mails, chamadas telefônicas, videoconferências ou para operações bancárias, sendo estes recursos vantajosos. Contudo nem tudo é vantagens, pois através da conexão, que conecta milhões de pessoas com à rede, indivíduos com altas capacidades técnicas ou sem a capacidade que através de alguns sites (endereço virtual, o qual são disponibilizadas informações) aprendem formas de praticar o ilícito.

A principal forma e meio utilizado para cometer crimes é a criação de um dispositivo conhecido como Malware (aplicativo que adentra um sistema, com intenção de repassar

informações a outrem ou causar danos ao sistema operacional de dispositivos eletrônicos), de modo que os vírus um Malware, que depende da interação da pessoa para começar a prejudicar, ou seja mensagens enviadas, por e-mail ou encontrada em sites que influenciam a pessoa abrir estas mensagens e no ato de abertura o vírus adentra o dispositivo. Além do vírus, existe também os Worms (malware ao contrário do vírus que depende de interação da pessoa, este aproveita falhas do dispositivo e se hospeda no sistema). Ou seja, os Malwares são a principal fonte de repasse de informações que originam os cybercrimes. Como se não bastasse os malwares, criminosos utilizam-se da rede para assediar pessoas, realizar discriminações, vender produtos ilegais como drogas, bem como realizar calúnia, injúria e difamação, apologia ao crime, pedofilia, espionagem, estelionato, roubo de identidade e inclusive terrorismo. As práticas dos crimes cibernéticos estão se tornando muito comuns, em razão de uma falsa sensação de impunidade que se tem, no qual os indivíduos que realizam transgressões da lei possuírem uma ilusão de que o ato, por se consumar ser a longa distância e de que os instrumentos utilizados para as práticas do ilícito não fornecerem identidade.

2.1 CLASSIFICAÇÕES DOS SUJEITOS QUE PRATICAM O CRIME E DOS CRIMES CIBERNÉTICOS

Bem como elencado no capítulo acima há sistemas criados que facilitam à consumação dos crimes virtuais, e segundo Túlio Lima Vianna em sua tese de mestrado, os sujeitos que desenvolvem os Malwares, levando em conta o modus operandi em uma forma objetiva, classificam-se em:

> 1 – CRACKERS DE SISTEMAS – piratas que invadem computadores ligados em rede.
> 2- CRACKERS DE PROGRAMAS – piratas que quebram proteções de software cedidos a título de demonstração para usá-los por tempo indeterminado, como se fossem cópias legítimas.
> 3- PHREAKERS – piratas especialistas em telefonia móvel ou fixa.
> 4-DESENVOLVEDORES DE VÍRUS, WORMS e TROJANS – programadores que criam pequenos softwares que causam algum dano ao usuário.
> 5- PIRATAS DE PROGRAMAS– indivíduos que clonam programas, fraudando direitos autorais. 6- DISTRIBUIDORES DE WAREZ – webmasters que disponibilizam em suas páginas softwares sem autorização dos detentores dos direitos autorais. (VIANNA, 2001, Pg. 62,)

Percebe-se então que em relação à forma objetiva destacasse os indivíduos com altas capacidades técnicas, que por diversos motivos incompreensíveis, desenvolvem ou utilizam de tecnologia para prejudicar e se ainda não bastasse o desenvolvimento, elaboram "aulas", para ensinar os que desconhecem. Na forma que Vianna, traz esses sujeitos e os motivos como uma classificação subjetiva sendo;

> 1- CURIOSOS – agem por curiosidade e para aprender novas técnicas. Não causam danos materiais à vítima. Lêem os dados armazenados, mas não modificam nem apagam nada. Muitos seguem códigos de ética próprios ou de um grupo ao qual são filiados.
> 2- PICHADORES DIGITAIS – agem principalmente com o objetivo de serem reconhecidos. Desejam tornar-se famosos no universo cyberpunk e para tanto alteram páginas da Internet, num comportamento muito semelhante aos pichadores de muro, deixando sempre assinado seus pseudônimos. Alguns deixam mensagens de conteúdo político, o que não deve ser confundido com o ciberterrorismo.
> 3- REVANCHISTA – funcionário ou ex-funcionário de uma empresa que decide sabotá-la com objetivo claro de vingança. Geralmente trabalharam no setor de informática da empresa, o que facilita enormemente a sua ação, já que estão bem informados das fragilidades do sistema.
> 4-VÂNDALOS – agem pelo simples prazer de causar danos à vítima. Este dano pode consistir na simples queda do servidor (deixando a máquina momentaneamente desconectada da Internet) ou até mesmo a destruição total dos dados armazenados.
> 5- ESPIÕES – agem para adquirirem informações confidenciais armazenadas no computador da vítima. Os dados podem ter conteúdo comercial (uma fórmula de um produto químico), político (emails entre consulados) ou militar (programas militares).
> 6- CIBERTERRORISTAS – são terroristas digitais. Suas motivações são em geral políticas e suas armas são muitas, desde o furto de informações confidenciais até a queda do sistema telefônico local ou outras ações do gênero
> 7- LADRÕES – têm objetivos financeiros claros e em regra atacam bancos com a finalidade de desviar dinheiro para suas contas.8- ESTELIONATÁRIOS – também com objetivos financeiros; em geral, procuram adquirir números de cartões de créditos armazenados em grandes sites comerciais. (2001, pag. 64/65)

Ainda que não abordado por Vianna em sua tese, entra-se na classificação subjetiva os; PEDOFILOS – que na psicologia, são tratados como transtornos psicológicos, que adultos ou adolescentes, em que atração de cunho sexual por crianças na puberdade faz com que haja à procura na internet e INTIMIDADORES – que através de sites, redes sociais, constrangem ou ainda causam intimidação, podendo chegar até a perseguição e ameaça.

Passado a classificação dos sujeitos, diante diversas correntes doutrinárias tem-se a classificação dos crimes cibernéticos. De modo que;

> Para Higor Vinicius Nogueira Jorge (2012) e Emerson Wendt (2012), existem as ações prejudicias atípicas e os crimes cibernéticos. As ações prejudiciais atípicas, são aquelas condutas que causam prejuízo ou transtorno para vítima através da rede mundial de computadores, mas não são tipificados em lei. Por sua vez os crimes cibernéticos se dividem em "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos". Os "crimes exclusivamente cibernéticos" são aqueles que necessariamente precisam do meio da informática para cometer tal crime (como é o caso do crime de invasão de dispositivo informático, artigos 154-A e154-B do código penal, introduzido pela Lei 12.735/2012, conhecido como Lei Carolina Dieckmann). Portanto os crimes cibernéticos abertos são aqueles que podem ou não ser praticados pelo meio informático, como é o caso de estudo os crimes de violação de direito do autor, pode ser praticado tanto no ambiente virtual como no analógico. (Apud. Tateoki, Victor Augusto 2016).

Havendo ainda outras definições quanto a classificação dos crimes cibernéticos, no qual subdivide-se em três tipos, os puros, mistos e comuns. De modo que explica Teixeira (2014);

> O primeiro são aqueles em que o sujeito visa especialmente o sistema de informática; as ações materializam, por exemplo, por atos de vandalismo contra a integridade do sistema ou pelo acesso desautorizado ao computador. Crime de informática misto se consubstancia nas ações em que o agente visa o bem juridicamente protegido diverso da informática, porém o sistema de informática é ferramenta imprescindível. E os crimes de informática comum são condutas em que agentes utilizam o sistema de informática como mera ferramenta, não essencial à consumação do delito. (Apud. Tateoki, Victor Augusto 2016).

Além das duas correntes apontadas acima, existe uma terceira de Tulio Vianna, 2001 que traz que os delitos informáticos, ou seja, os crimes cibernéticos, possuem quatro modalidades, sendo delitos informáticos impróprios, delitos informáticos próprios, delitos informáticos mistos e delitos informáticos mediato ou indireto.

Na linha de pensamento de Vianna, 2001 pg. 38, "delitos informáticos impróprios são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico da informatização automatizada" podendo neste caso utilizar como exemplo o crime de ameaça, ainda pg. 42 "delitos Informáticos Próprios são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas

(dados) ” ou seja se tem a ofensa dos dados, a exemplo invasão de dispositivo de informática. Já os crimes informáticos mistos “em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa” pg. 49, assim se tem a título de exemplo os praticados em âmbito eleitora. Por fim delito informático mediato ou indireto “é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação” (Vianna, 2001, pg. 52). Através da análise das classificações dos crimes cibernéticos, percebe-se uma amplitude de crimes que podem ser praticados na rede, bem como a complexidade das ações cometidas, até a consumação dos crimes.

2.2 TIPICIDADE PENAL DOS CRIMES CIBERNÉTICOS FRENTE A LEGISLAÇÃO BRASILEIRA

O artigo 1º do Código Penal Brasileiro traz “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal”. O referido artigo é bem claro em que tange o conceito de crime apresentado no primeiro capítulo, o qual crime é a violação de normas estabelecidas em lei e que ocorrendo a falta de norma, não se pode falar de crimes.

Ao contrário do que as pessoas creem os crimes praticados através na internet possuem tipificação e quando identificado os infratores se tem a sanção penal. O que faz as pessoas acharem que há sempre a impunidade nos cybercrimes é o fato das previsões legais não trazerem no preambulo o verbo “internet”. Ainda que no preambulo não traga “internet”, o fato dos sujeitos utilizarem a rede como meio de praticar o ilícito, a consumação possui tipificação de modo que podem ser aplicadas as sanções. Por conseguinte, segue abaixo os crimes mais praticados na internet, com as devidas medidas;

1- Assédio Sexual, destarte o artigo 216-A do Código Penal Brasileiro (CPB);

> Art. 216-A. Constranger alguém com o intuito de obter vantagem ou favorecimento sexual, prevalecendo-se o agente da sua condição de superior hierárquico ou ascendência inerentes ao exercício de emprego, cargo ou função. Pena detenção, de 1 (um) a 2 (dois) anos.

O assédio sexual com base no artigo supracitado diz respeito a superior hierárquico ou ascendência inerentes do emprego exercido constrange a parte mais fraca com o interesse de obter vantagens sexual. Sendo assim é compreendido que para constituir assédio sexual na rede é necessário que o agente infrator seja superior hierárquico que é que o mesmo constranja ou chantageie funcionário com intenção de obter favorecimentos sexuais. Não se tratando de

superior, o ato de constranger ou tentativas de favorecimentos sexuais, se a parte contraria sentir-se ofendida poderá prestar queixa na polícia por injúria ou difamação.

2- Discriminação, regulamenta pela Lei nº 7.716/89 de 1989, combinado (c/c) com o artigo 140 do CPB, que trata dos crimes de raça ou de cor, em seu art. 20;

> Art. 20. Praticar, induzir ou incitar, pelos meios de comunicação social ou por publicação de qualquer natureza, a discriminação ou preconceito de raça, por religião, etnia ou procedência nacional. c/c Art. 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro. (...) § 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência

Através da análise do artigo compreende-se, que mesmo que a discriminação ocorra na internet, o fato da ofensa causa o mesmo dano, assim notasse que não é necessário a criação de leis que incorpore o verbo "internet" para gerar punições.

3- MERCADO NEGRO, acerca do mercado negro na internet, não há uma lei em especifica que traga sanções para o mercado negro, porém o fato de ocorrer a venda de materiais ilícitos, a título de exemplo drogas em que a lei de drogas nº 11.343, de 23 de agosto de 2006 traz no Art. 33;

> Art. 33. Importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar.

Percebe-se deste modo, que já existem normas que proíbem que proíbem a comercialização de produtos ilícitos, e que praticamente todos os crimes realizados na internet possuem tipificação no ordenamento jurídico brasileiro.

4- Calúnia/ Difamação/ Injúria, crimes estes relacionados a honra da pessoa tipificados nos artigos 138, 139 e 140 do CPB: "Art. 138 – Caluniar alguém, imputando-lhe falsamente fato definido como crime: (...)Art. 139 – Difamar alguém, imputando-lhe fato ofensivo à sua reputação: (...)Art. 140 – Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: (...).

Mesmo ocorrendo via internet a calúnia, difamação e injúria possuem os mesmos requisitos, de que se ocorresse presencial, dependendo da vítima para levar o fato a autoridades competentes.

5- Apologia Ao Crime, a pratica da publicação, compartilhamento de fatos criminosos como se fossem certos, tem tipificação legal no artigo 287 do CPB: "Art. 287 – Fazer, publicamente, apologia de fato criminoso ou de autor de crime: Pena – detenção, de três a seis meses, ou multa. Em virtude deste artigo, a divulgação de vídeos, comentários, compartilhamentos que apoiam a violência enquadra-se na apologia ao crime.

6- Pornografia Infantil, O estatuto da criança e do adolescente (Lei 8.069/90) estabeleceu em seu artigo 241-A;

> 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 envolvendo criança ou adolescente; Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

Este artigo passou a ser vigorado em 25 de novembro de 2008, através da Lei nº 11.829, que "altera a Lei no 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet". De modo que neste caso havia a falta de regulamentação e a necessidade da criação da Lei em virtude do aumento de casos de distribuição de conteúdo pornográficos na rede.

7- Espionagem, a espionagem ganhou força no Brasil ano de 2013 em que através de uma publicação feita por um ex funcionário americano, que o Estados Unidos, através da rede de computadores, estava obtendo informações de vários países, inclusive o Brasil e o qual foram vazadas essas informações na internet. Quanto os crimes de espionagem estão estabelecidos na Lei. Nº 7.170 de 14 de dezembro de 1983, que define os crimes contra a segurança nacional, ordem política e social. Sendo a espionagem tipificada no Art. 13 e seus incisos, conforme segue;

> Art. 13 – Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos. Pena: reclusão, de 3 a 15 anos.Parágrafo único – Incorre na mesma pena quemI – Com o objetivo de realizar os atos previstos neste artigo, mantém serviço de espionagem ou dele participa; II –Com o mesmo objetivo, realiza atividade aerofotográfica ou de 8ensoriamento remoto, em qualquer

> parte do território nacional; III – oculta ou presta auxílio a espião, sabendo-o tal, para subtraí-lo à ação da autoridade pública; IV – obtém ou revela, para fim de espionagem, desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo.

8- Estelionato, o estelionato na internet está se tornando muito frequente, a exemplo indivíduos maliciosos estão produzindo sites de vendas com informações falsas de modo que induzem as pessoas a pagar por produtos que não existem. Acerca do estelionato o Artigo 171 do CPB aborda;

> Art. 171 – Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de um a cinco anos, e multa.

9- Roubo De Identidade, o roubo de identidade ocorre pela utilização de malwares que retiram informações de sistemas, possibilitando a utilização dos dados pessoais roubados para a extração de dinheiro em contas bancárias, utilização de CPF para compras, até mesmo ocorrendo com pessoas jurídicas, em que roubam informações das empresas para realização de negócios. O roubo de identidade no ordenamento jurídico brasileiro encontra-se no Art. 307 do Código Penal;

> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Além dos nove crimes elencados, existem vários outros que são praticados através da internet no Brasil e que possuem tipificação, à exemplo de exemplo terrorismo, bullying, pirataria e dentre outros. Vislumbrasse então que o Brasil não carece de leis que repitam os crimes praticados na internet, apenas acrescentando o verbo “internet” e ainda fica evidente que ao cometer os crimes tratados como virtuais há punições, diferente do que a maioria da população pensa.

2.3 LEIS ESPECIFICAS A RESPEITO DOS CRIMES CIBERNÉTICOS

A internet "chegou" ao Brasil em 1988 começando por São Paulo e Rio de Janeiro e foi ganhando espaço, até chegar em todos os Estados, e desde sua concepção tiveram algumas leis citadas no primeiro capitulo como a Constituição Federal de 1988 que trata a respeito das proteções dos dados e ainda anterior a constituição federal, como forma de prevenção a lei 7.232/84, que dispõe sobre a Política Nacional de Informática e outras providências. Fora estas leis protecionistas, até o ano de 2012 a respeito da internet não havia nenhuma outra lei. E mesmo na falta de lei os crimes praticados através da rede, eram punidos com base no efeito da ação.

As leis que surgiram a partir de 2012, teve causa a pressão da mídia sobre o legislativo, a razão da lei ter sido promulgada ainda gera discussões, por ter sido subsequente a fotos intimas da atriz Carolina Dieckmann, que por diversas vezes clamava por "justiça" quando suas fotos foram divulgadas na internet. Na época os infratores que divulgaram as fotos foram localizados e indiciados por extorsão qualificada, furto e difamação.

Contudo tamanha foi a repercussão de que não havia leis que 6 (seis) meses após as fotos serem divulgadas, foram promulgadas na mesma data às Leis Nº 12.735/12 e 12.737/12 em que a primeira altera o Código Penal, Código Penal Militar e a Lei de Preconceitos, tipificando condutas mediante uso de sistemas eletrônicos e digital, contra sistemas informatizados;

> LEI Nº 12.735 - Art. 1 º Esta Lei altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.(...)Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.Art. 5 º O inciso II do § 3o do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:(...)II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

E a segunda lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação de delitos informáticos e altera o Código Penal, lei conhecida informalmente como "Lei Carolina Dieckmann"

> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.Art. 2º O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:"Invasão de dispositivo informáticoArt. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar 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: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. § 5 º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal." (Grifo nosso)"Ação penal Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Percebe-se pela lei promulgada que o legislador não se preocupou com os cybercrimes em espécie, mas sim com o momento, o qual uma pessoa com fama pública teve suas imagens intimas divulgadas e visando uma proteção própria, conforme destacado em negrito em que o artigo teve um parágrafo inteiro destinado ao alto escalão do legislativo, executivo e judiciário.

Já os demais crimes praticados na internet continuam a ser julgados tendo como base o efeito danoso, causado pelos infratores. A real problemática dos crimes cibernéticos não se encontra na falta de uma lei que classifica e pune, mas sim em questões técnicas de como chegar no infrator e de quem é a competência para julgar. De modo que o capítulo seguinte abordara estes aspectos, para que se entenda o que causa a sensação de impunidade e o clamor por justiça.

3. A PROBLEMÁTICA ENFRENTADA PELO JUDICIARIO DIANTE AOS CRIMES VIRTUAIS

São muitas as dificuldades que o Ministério Público, a Polícia e o Judiciário brasileiro encontram para punir os agentes que praticam o cybercrime, são estas dificuldades que as pessoas sentem que há impunidade aos que praticam os crimes virtuais, e acabam relacionando a "impunidade" com a inexistência de leis especificas para os crimes cibernéticos.

Este capítulo tem por objetivo apresentar as problemáticas encontradas para que se tenha a devida punição dos infratores, de modo que em primeiro momento é necessário o conhecimento de como se constitui o poder judiciário, as fases do processo penal e ainda a competência para julgar os crimes virtuais.

Pois após a ocorrência do crime as sanções não competem a sociedade aplicar, mas sim a lei, representada pelo poder judiciário.

3.1 COMPOSIÇÃO DO PODER JUDICIÁRIO, SE TRATANDO DE CRIMES

O poder judiciário conforme a Constituição Federal de 1988 é separado por órgãos que tem como função a garantia dos direitos fundamentais, individuais, coletivos e sociais, bem como resolver os conflitos entre os cidadãos entidades e o Estado. O Artigo 92 da Constituição Federal de 1988 determina que;

> Art. 92. São órgãos do Poder Judiciário- O Supremo Tribunal Federal;I-A O Conselho Nacional de Justiça;II - O Superior Tribunal de Justiça;II-A - o Tribunal Superior do Trabalho;III - Os Tribunais Regionais Federais e Juízes Federais;IV - Os Tribunais e Juízes do Trabalho; VI - Os Tribunais e Juízes Militares;VII - Os Tribunais e Juízes dos Estados e do Distrito Federal e Territórios.

Os órgãos funcionam como uma pirâmide, e os que julgam causas criminais são o Supremo Tribunal Federal (STF) órgão máximo e tem como prerrogativa de zelar pelo cumprimento da Constituição Federal e Julgar de forma conclusiva questões que envolvam normas constitucionais. Abaixo do STF encontrasse o Superior Tribunal de Justiça (STJ) o qual sua prerrogativa é fazer a interpretação análoga da Constituição; Justiça Federal comum que julga causas que envolvam a união, autarquias ou empresas públicas federais; Tribunal de Justiça Militar e Justiça Militar, que julgam casos de crimes militares e a Justiça Comum, em

que cada estado possui e se divide entre Juizados Especiais e Varas, a exemplo; varas da execução, varas criminais que se localizam no Fórum (praça pública, tribunal).

3.2PROBLEMÁTICA DA INVESTIGAÇÃO NOS CRIMES CIBERNÉTICOS

A grande dificuldade encontrada para punir os infratores dos crimes praticados na internet conforme já foi mencionada não ocorre pela falta de norma que caracteriza os crimes e os classifica em uma ordem.

O real problema se presencia em detalhes como a falta de tecnologia e de mão de obra especializada para o combate aos cybercrimes. Desde 1988, quando a rede mundial de computadores passou a ser implementada no Brasil, não houve preparos e investimentos para combater os crimes que já vinham sendo praticados nos países que originaram a internet, de modo que ficou mais fácil a pratica de crimes na rede.

Pois o volume de crimes que ocorrem no país, supera a o número de capacitados para realizar as investigações, conforme afirmou Carlos Eduardo Sobral, chefe da unidade de Repressão a Crimes Cibernéticos da Policia Federal na CPI dos Crimes Cibernéticos, realizada no dia 20/08/2014 "O volume de investigação vem crescendo, e o efetivo tem que crescer na mesma proporção. Hoje o nosso efetivo acaba sendo menor do que o volume que necessita para que seja dado um rápido andamento às investigações" (apud. Canuto, Luiz Cláudio, 2015).

Outro problema encontrado para as investigações serem mais precisas é que o nosso ordenamento jurídico a sanção penal só pode ser aplicada, quando houver a certeza da prática do crime, sendo fundamentais a comprovação da autoria e da materialidade, ou a existência de fortes indícios de que o sujeito praticou o crime. Caso não consiga ser comprovada a materialidade e autoria o juiz poderá absolver o réu, conforme traz o artigo 386 do Código de Processo Penal (CPP);

> Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça: I - Estar provada a inexistência do fato; II - Não haver prova da existência do fato; III - Não constituir o fato infração penal;IV - Estar provado que o réu não concorreu para a infração (...) V - Não existir prova de ter o réu concorrido para a infração penal;

Além de fundamental a existência de provas e autoria, as provas obtidas para a comprovação do crime devem ser adquiridas de forma licita, ou seja, em cumprimento da lei. Fato que dificulta a investigação dos crimes cibernéticos, em razão que a polícia ao realizar as

investigações criminais em primeiro momento identifica, a forma que o crime aconteceu, o local que ocorreu, em segundo momento busca localizar o endereço de IP (número que identifica o dispositivo na rede), após a identificação do IP do infrator, o setor de investigação da polícia entra em contato com a empresa que disponibiliza o número na rede, e só assim identificar o criminoso. No momento de entrar em contato com a empresa e na identificação do IP a Policia encontra a primeira dificuldade que é o artigo 5º, inciso X e inciso XXII da Constituição Federal, que protege a privacidade e os dados, acarretando uma maior demora para a obtenção de provas. Pois necessita de autorização do Juiz para realizar as investigações e comunicações com as empresas que armazenam informações da localização dos criminosos.

Além do tramite demorado, evidenciasse um outro problema que é as empresas de informação, se recusarem a prestar auxílio a polícia e ao judiciário, a título de exemplo o whatsapp, que mesmo com a autorização da justiça se recusou prestar informações quanto a usuários investigados, que gerou decisão de bloqueio da referida rede social, por tempo limitado.

Há a falta de pessoas especializadas para agilizar nas investigações, empresas como o whatsapp que não colaboram com o judiciário, leis fundamentais que atrasam as investigações e o pior com a globalização, aumenta o número de crimes praticados por estrangeiros no Brasil, e a facilidade de compra de hospedagens de IP localizada fora do País, causando um conflito de competência acerca de que órgão deve julgar os crimes cibernéticos.

4. CONCLUSÃO

Durante a realização da Monografia, foi assumido o desafio de buscar informações seguras, precisas e confiáveis sobre o tema tão polêmico quanto os crimes cibernéticos, virtuais, cybercrime que vem ganhando destaque, junto a globalização e a evolução eletrônica. Muito comentado diariamente, diante de escândalos de espionagem, materiais pornográficos envolvendo pessoas de fama e informações privadas de agentes governamentais.

Contudo muito se fala dos crimes praticados na Internet e pouco se conhece, de modo que no primeiro capítulo foi abordado a origem da palavra internet, como o contexto histórico até o surgimento da primeira ação, que desencadeou a prática dos crimes, onde não se passava de uma brincadeira entre os desenvolvedores e peças entre os estudantes de tecnologia.

Brincadeira que consistia na derrubada do sistema do companheiro de um computador para o outro, e a iniciativa dos estudantes de deixar uma mensagem “assustadora” aparecer na tela dos computadores da universidade. O que deu início à uma brincadeira desencadeou uma

pratica cruel muito utilizada, a título de exemplo a invasão do site do Tribunal de Justiça do Rio de Janeiro, que em decisão judicial efetuou o bloqueio da rede social WhatsApp, por não contribuir em investigações criminais. A invasão consistiu na inatividade do site, com ameaças de só voltar com o retorno do aplicativo social. O segundo capítulo tratou demonstrar o não intervencionismo do Estado diante a proteções fundamentais como a proteção de dados e a privacidade, em que a violação desses direitos somente é permitida com autorização judicial em razão a investigações criminais.

Tamanha proteção as pessoas, que também possibilita uma maior demora nas investigações da polícia, que antes de tudo para investigações dos crimes cibernéticos necessitam de autorização do judiciário, e na espera da autorização, muitas vezes acabam acarretando o desaparecimento de provas essenciais para a constituição do crime. Identificado a origem dos crimes cibernéticos e a proteção constitucional o terceiro capítulo tratou de especificar os crimes cibernéticos em espécie, os sujeitos e a legislação vigente no Brasil que puni os crimes. Quando falado dos crimes cibernéticos as pessoas associam com a falta de leis como causa da impunidade, e os alguns criminosos virtuais que aprendem meios de adquirir vantagem de forma ilegal na internet, acreditam na falta de legislação especifica e do crime perfeito por ser realizado a longa distância.

Contudo o ordenamento jurídico brasileiro mesmo não vinculando a palavra “internet” aos crimes não deixou de punir, pois independente do meio utilizado para a pratica do delito o fim é o mesmo. E o que não falta no Brasil é a quantidade de crimes, pois é considerado um dos países com o maior número de tipos penais. Ou seja, o que realmente causa a sensação de impunidade nas pessoas não é a falta de leis, mas sim a dificuldade do judiciário de punir, começando pela proteção constitucional dos direitos fundamentais a investigação para identificar a materialidade e a autoria. Tamanha a problemática encontrada pelo judiciário a chegar a punição que foi o tema decorrido no capitulo quarto. Conforme já mencionado acima a “impunidade” não ocorre por falta de lei, mas sim da dificuldade de investigação da polícia que falta equipamentos e pessoas especializadas e um contato mais direto com o judiciário para a concessão rápida das autorizações investigatórias, como quebra de dados, para que assim o ministério público encontre a materialidade e a autoria para dar início ao procedimento penal e assim chegar a uma sanção para os indivíduos que comentem o cybercrime.

Desta forma conclui-se que a sensação de impunidade das pessoas referente aos crimes cibernéticos não se dá pela falta de lei especifica, mas sim pela dificuldade que a polícia e o judiciário encontram para localizar o infrator, identificando a autoria e a materialidade dos crimes e assim aplicar a devida sanção.

A internet é a maior tecnologia desenvolvida e não possui fronteiras, permite de uma forma sofisticada, permite o desenvolvimento de conhecimentos aprofundado sobre todas as áreas, porém a liberdade tem um custo o qual não pode ser muito agradável, que é a perda da privacidade. Perda decorrente da falta de segurança que a rede possui para os usuários de todo o mundo, o crime cibernético não é um problema que o Brasil enfrenta de forma isolada, o mundo inteiro sofre com os crimes, até mesmo os países de primeiro mundo, a segurança da rede é instável e tudo que é digitado nos computadores e celulares podem estar comprometidas, de modo que nenhum pais até hoje encontrou uma solução para este problema. Nesta era global até mesmo crianças em seu desenvolvimento já conseguem utilizar a internet e crescem em virtude da rede, sendo assim a única solução atualmente para evitar ser vítima dos crimes virtuais, pode ser considerada careta é a utilização dos velhos modos, que é compras em lojas físicas, consulta de créditos de bancos, diretamente nas agências e o que vem se tornando a forma mais difícil, desvinculação da privacidade com as tecnologias.

5. REFERÊNCIAS

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A Trajetória da Internet no Brasil: do Surgimento das Redes de Computadores à Instituição dos Mecanismos de Governança.** Disponível em http://www.nethistory.info/Resources/Internet-BR-Dissertacao-Mestrado-MSavio-v1.2.pdf. Acesso em 10 de setembro de 2016.

KUROSE, Ross. **Redes de Computadores e A Internet - Uma Abordagem Top-Down** – 5 ª Ed. 2012.

NUCCI, Guilherme de Souza. **Manual de Direito Penal** 11ª Ed. 2015 -

HOLANDA, Aurélio Buarque de. **Novo dicionário da língua portuguesa**. 2. ed. Rio de Janeiro: Nova Fronteira, 1986.

BRASIL. **Constituição Federal da República Federativa do Brasil de 1988**. Promulgada em 05 de outubro de 1988.

BURROWES, Frederick B. **A Proteção Constitucional das Comunicações de Dados: Internet, Celulares e Outras Tecnologias**. Disponível em

https://revistajuridica.presidencia.gov.br/index.php/saj/article/viewFile/278/267. Acesso em 05 de setembro de 2016.

JUSBRASIL, **Direito à Privacidade: Intimidade, Vida Privada e Imagem**. Disponível em http://quentasol.jusbrasil.com.br/artigos/214374415/direito-a-privacidade-intimidade-vida-privada-e-imagem. Acesso em 08 de setembro de 2016.

DUDH, **A Declaração Universal dos Direitos Humanos**. Disponível em http://www.dudh.org.br/declaracao/. Acesso em 11 de setembro de 2016.
Celso Ribeiro Bastos; Curso de Direito Constitucional, 1999

OLIVEIRA, Rogerio Campos de, **Direito a Intimidade e Sua Proteção Baseada nos Direitos Humanos no Mundo**. Disponível em http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=14826. Acesso em 12 de setembro de 2016.

OFICINADANET, **Quais São os Crimes Virtuais Mais Comuns?** Disponível em https://www.oficinadanet.com.br/post/14450-quais-os-crimes-virtuais-mais-comuns. Acesso em 13 de setembro de 2016.

OFICINADANET, **Diferença Entre: Vírus, Spam, Spyware, Worm, Phishing, Botnet, Rootkit**. Disponível em https://www.oficinadanet.com.br/post/12991-diferenca-entre-virus-spam-spyware-worm-phishing-botnet-rootkit. Acesso em 13 de setembro de 2016.

JUSBRASIL, **Classificação dos Crimes Digitais**. Disponível em http://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais. Acesso em 14 de setembro de 2016.

VIANNA, Túlio Lima. **Do Acesso Não Autorizado a Sistemas Computacionais: Fundamentos de Direito Penal Informático**. Disponível em http://www.bibliotecadigital.ufmg.br/dspace/bitstream/handle/1843/BUOS-96MPWG/disserta_o_t_lio_lima_vianna.pdf?sequence=1. Acesso em 14 de setembro de 2016.

BRASIL, LEI 12.735 de 30 de novembro de 2012**. Condutas do Uso do Sistema Eletrônico.** Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em 14 de setembro de 2016.

BRASIL, LEI 12. 965 de 23 de abril de 2015. **Princípios, Garantias, Direitos e Deveres Para o Uso da Internet no Brasil**. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 15 de setembro de 2016.

CASTRO, Luiz Augusto Sartori de. **"Lei Carolina Dieckmann" Seria a Salvação da Internet?** Disponível em http://www.migalhas.com.br/dePeso/16,MI167980,81042-Lei+Carolina+Dieckmann+seria+a+salvacao+da+internet. Acesso em 15 de setembro de 2016.

CAMARA. **CPI Constata Dificuldade Em Rastrear e Punir Crimes de Internet**. Disponível em http://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/494363-CPI-CONSTATA-DIFICULDADE-EM-RASTREAR-E-PUNIR-CRIMES-DE-INTERNET.html. Acesso em 16 de setembro de 2016.

G1.GLOBO.COM. **WhatsApp: Justiça do RJ Manda Bloquear Aplicativo em Todo o Brasil.** Disponível em /http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-deve-ser-bloqueado-decide-justica-do-rio.html. Acesso em 18 de setembro de 2016.

BORRI, Luiz. **Competência nos Crimes Contra a Honra Cometidos Pela Internet**. Disponível em http://www.conjur.com.br/2012-out-09/luiz-borri-competencia-crimes-honra-cometidos-internet. Acesso em 18 de setembro de 2016.

ELEUTÉRIO, Fernando. **Análise do Conceito de Crime.** Disponível em http://www.uepg.br/rj/a1v1at09.htm. Acesso em 18 de setembro de 2016.