CRIMES CIBERNÉTICOS E A SENSAÇÃO DE IMPUNIDADE

Cyber crimes and the feeling of impunity

Guilherme Microni Naziazeno[1]
Carlos Henrique Passos Mairink[2]

Resumo: Roubo de dados e de identidade, calúnia, difamação, bullying, crimes financeiros, pornografia e pedofilia infantil, verbos estes que constituem os crime cibernético praticadono Brasil, de modo que o presente artigo aborda classificação e características daspráticas 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 umapossível solução para a não ocorrência dos cybercrimes ou a diminuição deste

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

Abstract: Data and identity robbery, slander, defamation, bullying, financial crimes, 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 regardingthe growing number of cybercrime in all of Brazil, in a way that try to clarify the fact who cause the feeling of impunity and a possible solution to the non-occurrence of cybercrimes or its ddecrease.

Keywords: Crimes, Cybercrimes, Virtual Crimes, Evolution, Globalization,

[1] Discente do curso de direito da FAMIG – Faculdade Minas Gerais: guilhermenaziazeno20@gmail.com
[2] Professor orientador no curso de Direito da FAMIG – Faculdade Minas Gerais: passosmairink@gmail.com

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 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 todosos 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. Tambémserá 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.

Também é abordado neste artigo a inexistência da culpabilidade pelos crimes cibernéticos que é preocupante, pois a mesma consiste na condição regular

necessária para fundamentar juridicamente uma responsabilidade, sendo constituída por livre arbítrio e juízos sobre a realidade, criando um sistema de subjetividade individual de aferição da culpabilidade do agente. Não é apenas a percepção cultural, mas a percepção da realidade em si, o que alteraria a capacidade de entender o caráter ilícito da conduta e de se adequar perante tal entendimento. Assim, na ausência de uma legislação específica, aquele que praticou algum ato ilícito cibernético, deverá ser julgado dentro do próprio Código Penal, mantendo-se as devidas diferenças. No Direito Brasileiro existe o instituto da analogia, consistindo forma que se torna aplicável ao caso omisso, uma lei que prejudique o réu e que regulamente a prática de um ato ilícito semelhante.

A princípio, seria uma ótima alternativa para tipificar ações ilícitas praticadas no âmbito virtual, porém, a maioria da doutrina do Direito Penal Brasileiro, como Rogério Sanches Cunha, Guilherme de Souza Nucci e Cleber Masson, em outras áreas do Direito esse instituto pode ser aplicado com eficiência, mas no ordenamento penal, a sua aplicação necessita ser cuidadosamente avaliada, pelo fato desta possibilidade poder ferir o princípio constitucional da legalidade.

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 sãodisponibilizadas 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 queos 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, p. 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;

> CURIOSOS – agem por curiosidade e para aprender novas técnicas. Não causam danos materiais à vítima. Lêem os dados armazenados, mas não modificam nem apagamnada. Muitos seguem códigos de ética próprios ou de um grupo ao qual são filiados.
> 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.
> 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.
> 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.
> 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).
> 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
> 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. (VIANA, 2001, p. 64)

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 comque 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 meioda 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. (TAKEOKI[3], Apud. 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. (TAKEOKI, Apud. 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

---

[3] TATEOKI, CAVALCANTI, Ana Elizabeth Lapa Wanderley. Proteção de
TATEOKI, CAVALCANTI, Ana Elizabeth Lapa Wanderley. Proteção de dados pessoais na sociedade da informação: uma visão sob o aspecto dos direitos da
personalidade no Brasil e na União Europeia. Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI/ UNISINOS Coordenadores: José Renato Gaziero Cella; Salete Oro Boff; Júlia Francieli Neves de Oliveira. – Florianópolis: CONPEDI, 2012. p. 47-62

próprios, delitos informáticos mistos e delitos informáticos mediatos ou indiretos.

Na linha de pensamento de Vianna “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” (VIANA, 2001 p. 38) podendo neste caso utilizar como exemplo o crime de ameaça, ainda, “delitos Informáticos Próprios são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)” (VIANA, 2001 p. 42), 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” (VIANA, 2001, p. 49), assim se têm 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, p. 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 preambulonão 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;

I - 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 defavorecimentos sexuais, se a parte contraria sentir-se ofendida poderá prestar queixa na polícia por injúria ou difamação.

II - Discriminação, regulamenta pela Lei nº 7.716/89 de 1989, combinado (c/c) com o artigo140 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.
>
> 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.

III - 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. 3

> 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.

IV - 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.

V - 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 trêsa seis meses, ou multa. Em virtude deste artigo, a divulgação de vídeos, comentários, compartilhamentos que apoiam a violência enquadra-se na apologia ao crime.

VI - 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 vigorar 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.

VII - 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 eo 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 quem:
> I – 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.

VIII - 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.

IX - Roubo De Identidade, o roubo de identidade ocorre pela utilização de malwares que retiram informações de sistemas, possibilitando a utilização dos dados pessoais roubadospara 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 mesesa 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 amaioria da população pensa.

2.3 Leis 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 arespeito 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 clamavapor “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 políciajudiciária 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 janeirode 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 informático Art. 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 depermitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a umterço 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;

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.”

“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. OS PROBLAMAS ENFRENTADOS 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.

Observa-se uma grande dificuldade em investigar e punir esses crimes, devido ao fato de muitos delituosos agirem de modo a deixarem o mínimo de suspeitas possíveis, utilizando o mundo tecnológico a seu favor que permite agirem de forma

anônima e silenciosamente. Dessa forma, aumenta o grau de dificuldade de identifica-los, tendo em vista que esses delituosos fazem uso de dispositivos tecnológicos em locais públicos disponibilizando facilmente o acesso, tendo esses agentes artifícios para agir de forma anônima.

O anonimato está ligado principalmente a Deep Web. A Deep Web é a parcela da internet utilizada para comunicações e trocas de arquivos de forma anônima, ou seja, não é indexada por mecanismos de busca comuns. Pode ser acessada através de aplicativos da rede TOR (The Orion Rout), que elimina os rastros de acesso, embora tenha toda esta segurança, alguns sites ao serem acessados na rede podem exigir que para acessa-lo o usuário faça um login usando navegador da internet conhecida, comum.

Não se pode deixar de citar a Dark Web, que é uma pequena parcela da Deep Web, em que os sites e redes também não são indexados por mecanismos de busca. Porém ela se difere da primeira, pois os domínios nela são voltados para as práticas criminosas, devido a isso se mantém escorada na dificuldade de rastreio nas redes. A principal diferença entre é a supracitada, sendo que a Dark Web é voltada para a prática de crimes, quanto a Deep Web contém domínios necessários para a operação da web.

Segundo o advogado criminalista, especialista em cibercrimes, D'URSO (2019), em entrevista ao Jornal Estadão, a maior dificuldade com relação ao combate desses crimes está relacionada à dificuldade de se fazer prova e investigar a origem do delito, a materialidade e a autoria, bem como a falta de conhecimento técnico dos usuários, as supostas vítimas, tornando alvos fáceis do cibercriminoso e a variedade de delitos, que é quase ilimitada.

Não somente essas são as dificuldades no combate a esses crimes, fazemos a seguir a análise de alguns motivos que dificultam, ainda mais, o combate, com as possíveis hipóteses de solução.

Começamos pelo despreparo dos profissionais competentes dessa problemática, acerca da ineficiência de seus trabalhos, especificadamente a respeito do domínio da tecnologia. Bem como, a deficiência de ferramentas para investigação, devendo ressaltar o fato de que os profissionais precisam de meios, que devem ser fornecidos pela instituição em que trabalha para melhorar o desempenho de suas tarefas.

Constata-se outro obstáculo que é relacionado com a prova criminal através da perícia, onde para realização do exame é necessário que o perito tenha acesso ao dispositivo eletrônico do agente, porém só pode realizar o exame indireto, que é feito com outro aparelho semelhante, que necessita de uma autorização da autoridade competente.

Outro motivo que leva a dificuldade de obter provas e/ou a punição dos delitos virtuais é a ausência de capacitação dos profissionais especializados para combater esses crimes, por isso é necessário que os profissionais responsáveis se atualizem para realizar o trabalho da melhor maneira.

O Brasil enfrenta outra grande dificuldade que é o atraso de leis específicas a respeito do tema, que são criadas à medida que a sociedade evolui. São algumas dificuldades enfrentadas pela problemática.

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

3 FROTA, Jessica Olívia Dias; PAIVA, Maria de Fátima Sampaio. Crimes virtuais e as dificuldades para combatê-los. 2017. Disponível em: <https://flucianofeijao.com.br/novoo/wp-content/uploads/2018/11/ARTIGOS_CRIMES_VIRTUAIS\nDIFICULDADE.... Acessado em 24 de maio de 2020.

Artigo 92 da Constituição Federal de 1988 determina que;

> Art. 92. São órgãos do Poder Judiciário:
>
> I - 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;
>
> V - os Tribunais e Juízes Eleitorais;
>
> 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 oSupremo 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).

3.2 Problemas na Investigação dos Crimes Cibernéticos

A grande dificuldade encontrada para punir os infratores dos crimes praticados na internetconforme já foi mencionada não ocorre pela falta de norma que caracteriza os crimes e osclassifica 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" (Canuto, apud. 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 setorde investigação da polícia entra em contato com a empresa que disponibiliza o número narede, e só assim identificar o criminoso.

No momento de entrar em contato com aempresa 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. CONVENÇÃO DE BUDAPESTE

Essa referida convenção consiste em um ordenamento desenvolvido pelo Conselho da Europa em 2002, em que seu objetivo girava em torno da proteção da sociedade contra a criminalidade no ciberespaço. A princípio, a Convenção de Budapeste promovia a escolha de uma legislação comum que objetivasse uma maior cooperação entre os Estados da União Europeia, mas atualmente encontra-se aberta à assinatura por todos os países que a desejarem, tendo em vista que os crimes cibernéticos atingem todos os territórios do mundo (FERNANDES, 2013)16 . Desde o

planejamento até a elaboração da Convenção de Budapeste, transcorreram aproximadamente cinco anos, enquanto isso, no território brasileiro os julgadores pouco estão se importando para a aprovação de projetos de lei com a temática em questão, levando à instabilidade no meio social e à insegurança no âmbito jurídico (FERNANDES, 2013). No Direito Internacional, existe o Direito Internacional Uniforme, utiliza por quase todos os países do mundo, que ocorre quando coincidem os direitos primários entre ordenamentos, seja porque têm a mesma origem, ou por sofrerem influências idênticas, ou, ainda, quando países adotam sistemas jurídicos clássicos total ou parcialmente, de outros Estados (FERNANDES, 2013). Uma hipótese a favor da segurança jurídica do Direito Brasileiro em vista da tipificação dos crimes cibernéticos, configura-se no fato do Brasil adotar a Convenção de Budapeste, tendo em vista que, o conteúdo dos projetos de leis, que se encontram há anos sob o julgamento do Congresso Nacional, é similar aos tratados pela referida Convenção (FERNANDES, 2013).

[4] FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013, 2013.62: 139-178.

5. CONCLUSÃO

Durante a realização do artigo, 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 globalizaçãoe a evolução eletrônica. Muito comentado diariamente, diante de escândalos de espionagem, materiais pornográficos envolvendo pessoas de fama e informações privadas de agentes governamentais.

Os delitos cometidos através da internet são presentes em todo o mundo, entretanto, o Brasil encontra-se atrasado por não dispor de uma legislação específica e adequada à regulamentação e punição àqueles que cometem as condutas delituosas em questão A falta de tipificação adequada para os delitos praticados no ambiente cibernético, promove insegurança tanto para a sociedade quanto para o âmbito jurídico brasileiro. As tentativas fracassadas de projetos de lei ou mesmo a publicação apressada de legislações, como é o caso da Lei nº 12.737/2012, geraram inúmeras consequências em desfavor da adequada classificação e regulamentação dos crimes em questão. É necessária cautela na instauração de um ordenamento sob o referido tema, tendo em vista que o ambiente virtual está em constante evolução, devendo ser estudado de forma adequada.

Com a existência de condutas atípicas que não podem ser punidas em decorrência do princípio da legalidade ou da reserva legal, é essencial a elaboração de um ordenamento específico além da adoção do Brasil a tratados internacionais que disciplinam sobre o conteúdo em questão para adequação da legislação interna, como é o caso da Convenção de Budapeste. Diante a expansão do espaço cibernético em todo o mundo, a adoção à Convenção consistiria no dever preventivo do Estado, tendo em vista que promoveria a utilização de normas claras e eficientes, de modo que

promova segurança à sociedade e punição àqueles que se utilizam de meios escusos para provocar danos matérias e morais a terceiros.

REFERÊNCIAS

BRASIL. **Código Penal DECRETO-LEI No 2.848**: promulgada em 07 de dezembro de 1940

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

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 desetembro 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.

BURROWES, Frederick B. **A Proteção Constitucional das Comunicações de Dados: Internet, Celulares e Outras Tecnologias**. Disponível em REVISTA CIENTÍFICA ELETRÔNICA DO CURSO DE DIREITO – ISSN: 2358-8551 13ª Edição – Janeiro de 2018 – Periódicos Semestral https://revistajuridica.presidencia.gov.br/index.php/saj/article/viewFile/278/267. acesso em 05 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.

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.

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.

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.

DUDH, **A Declaração Universal dos Direitos Humanos**. Disponível em http://www.dudh.org.br/declaracao/. Acesso em 11 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

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.

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

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.

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.

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 -

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.

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.

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 de2016. REVISTA CIENTÍFICA ELETRÔNICA DO CURSO DE DIREITO – ISSN: 2358-8551 13ª Edição – Janeiro de 2018 – Periódicos Semestral

FERNANDES, David Augusto. Crimes cibernéticos: o descompasso do estado e a realidade. REVISTA DA FACULDADE DE DIREITO DA UFMG, 2013, 2013.62: 139-178.