UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

TEYMISSO SEBASTIAN FERNANDES MAIA

ANÁLISE DOS MECANISMOS DE COMBATE AOS CRIMES CIBERNÉTICOS NO SISTEMA PENAL BRASILEIRO

FORTALEZA
2017

TEYMISSO SEBASTIAN FERNANDES MAIA

ANÁLISE DOS MECANISMOS DE COMBATE AOS CRIMES CIBERNÉTICOS NO SISTEMA PENAL BRASILEIRO

Monografia apresentada ao Curso de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de bacharel em Direito. Área de concentração: Direito Penal.

Orientador: Prof. Dr. Sidney Guerra Reginaldo

FORTALEZA
2017

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

M188a
Maia, Teymisso Sebastian Fernandes.
Análise dos Mecanismos de Combate aos Crimes Cibernéticos no Sistema Penal Brasileiro / Teymisso Sebastian Fernandes Maia. – 2017.
111 f. : il. color.
Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2017.
Orientação: Prof. Dr. Sidney Guerra Reginaldo.
1. Crimes Cibernéticos. 2. Legislação Brasileira. 3. Investigação Criminal. 4. Cooperação Internacional. I.
Título.
CDD 340

TEYMISSO SEBASTIAN FERNANDES MAIA

ANÁLISE DOS MECANISMOS DE COMBATE AOS CRIMES CIBERNÉTICOS NO SISTEMA PENAL BRASILEIRO

Monografia apresentada ao Programa de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de bacharel em Direito. Área de concentração: Direito Penal.

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

_____

Prof. Dr. Sidney Guerra Reginaldo (Orientador)

Universidade Federal do Ceará (UFC)

_____

Profa. Msc. Fernanda Cláudia Araújo da Silva

Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Daniel Maia

Universidade Federal do Ceará (UFC)

A Deus.

À minha família por todo o apoio na minha formação universitária e como ser humano.

AGRADECIMENTOS

A Deus, por sempre me dar sabedoria e força para enfrentar as dificuldades.

À minha esposa, Susy Anne, pelo amor, incentivo e apoio incondicional.

Aos meus filhos, Anthony Michael e Adriel Lucca, que me servem de inspiração para prosseguir nas lutas diárias.

Ao Prof. Dr. Sidney Guerra Reginaldo, pelo inestimável auxílio e acompanhamento na feitura desta obra monográfica.

À Profa. Msc. Fernanda Cláudia Araújo da Silva, pela sua dedicação à docência na Universidade Federal do Ceará, e devido à sua disponibilidade para participar dessa banca examinadora.

Ao Prof. Dr. Daniel Maia, pela inspiração na realização de partes dessa obra, e devido à sua disponibilidade para participar dessa banca examinadora.

Aos colegas da faculdade, especialmente Almino Pinheiro, Daniel Almeida, Tiago Cavalcante, Rômulo Braga, e Rodrigo Matos, pela amizade e pelos incentivos ao longo desse importante curso.

Aos colegas da Polícia Civil do Ceará, por todos os ensinamentos que me passaram durante o meu serviço como Inspetor de polícia.

Por fim, agradeço a todos que direta ou indiretamente fizeram parte da minha formação.

“Com grandes poderes vêm grandes responsabilidades.” (Stan Lee)

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ENIAC Electronic Numerical Integrator and Computer (Computador Integrado Numérico Eletrônico)

EUA Estados Unidos da América

ARPA *Advanced Research Projects Agency (Agência de Pesquisas e Projetos Avançados)*

NASA National Aeronautics and Space Administration (Administração Nacional da Aeronáutica e Espaço)

TCP/ IP *Transmission Control Protocol/Internet Protocol (Protocolo de Controle de Transmissão/Protocolo de Internet)*

WWW World Wide Web (Rede Mundial de Computadores)

HTML HyperText Markup Language (Linguagem de Marcação de Hipertexto)

IBGE Instituto Brasileiro de Geografia e Estatística

TI Tecnologia da Informação

CGI.br Comitê Gestor da Internet no Brasil

IP Internet Protocol (Protocolo de Internet)

RESUMO

No presente trabalho busca-se analisar os mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro, de tal modo a apresentar a tecnologia da *internet* relacionando-a com as ameaças computacionais provenientes do uso indiscriminado e da facilidade de anonimato idealizado pelos criminosos. Crimes Cibernéticos são tipos de crimes perpetrados pela utilização de dispositivos computacionais como meio decisivo para o cometimento das infrações penais. Essa nova tecnologia em mãos criminosas requer uma evolução nos métodos investigativos de combate aos crimes virtuais devido à facilidade que a rede mundial de computadores oferece para aqueles que procuram utilizar o computador como instrumento para o cometimento de delitos, em busca da dificuldade de rastreamento proporcionado por esse meio. O histórico da *internet* e das ameaças computacionais revelam um rápido crescimento em poucos anos. A necessidade de uma interação cooperativa entre os países do mundo através de Tratados, Convenções e outros mecanismos menos burocráticos por meio de uma legislação que permita uma celeridade e ao mesmo tempo garanta os direitos humanos, é um desafio que precisa ser superado para um efetivo combate a esse tipo de delito que não reconhece distâncias.

Palavras-chave: *internet*. Crimes Cibernéticos. Legislação

ABSTRACT

The present work we seek to analyze the mechanisms to combat Cybercrimes in the Brazilian penal system, in such a way as to present the technology of the Internet relating it to the computational threats arising from the indiscriminate use and the anonymity of criminals.. Cybercrimes are a type of crime where the criminal uses the computer like an important instrument to delinquency. This new technology in bad hands creates a urgency in the development of investigators methods to fight cybercrimes because the web offer a mask for the criminals can doing their crimes with a little possibility of tracking. The history of the *internet* and the threats reveal a grown development in fast time. A better cooperation between the countries with the help of trades, conventions and others interactions can allow a better use of time respecting the human´s rights. This is the challenge to the world in the war against this kind of crime that doesn´t respect distances.

Keywords: *internet*. Cybercrimes. Legislation.

SUMÁRIO

1 INTRODUÇÃO

A tecnologia trouxe um nível de vida jamais imaginado pelas pessoas de épocas anteriores. Os jovens de hoje em dia podem inclusive serem considerados nativos digitais, por já nascerem em um ambiente rodeado de desenvolvimento tecnológico. Um dos avanços mais impressionantes vivenciados pela humanidade foi a invenção da *internet*. Hoje é possível realizar através da rede mundial de computadores as mais diversas atividades, além de as barreiras temporais e espaciais terem sido relativizadas.

Infelizmente, todas as facilidades que a tecnologia da informática oferece também está vindo acompanhada de sérios riscos para as pessoas. A oportunidade de ocultar a sua identidade através da Internet atrai uma nova espécie de criminoso de difícil detecção. Deve-se observar que as pessoas tem desenvolvido uma personalidade virtual muitas vezes diversa da personalidade manifestada no mundo real. Através do ambiente informático alguns indivíduos mostram uma faceta desconhecida para muitos do seu círculo de relacionamentos em ambientes físicos.

A exemplo de importantes tecnologias como o avião, que teve seu uso desvirtuado para algo maligno como a guerra, há quem utilize a *internet* e outras tecnologias informáticas para realização de condutas atentatórias aos direitos de outras pessoas. Esses delitos cibernéticos são o objeto de estudo desse trabalho, que tem a intenção de entender a dinâmica do Brasil para o combate a essa espécie de conduta indesejada.

Neste trabalho procurou-se realizar uma pesquisa bibliográfica e "webiográfica" de forma a buscar subsídios teóricos para a análise de pontos cruciais dos delitos cibernéticos. Através da pesquisa realizada em obras e artigos científicos criou-se um embasamento teórico que justificasse a pesquisa e o ponto de vista acerca dos mecanismos de combate à criminalidade virtual.

Com essa abordagem procura-se entender a situação do crime virtual no cotidiano e como as tecnologias podem ser utilizadas para os fins mais lesivos possíveis. A importância da pesquisa bibliográfica vai no sentido de que a Ciência evolui através da colaboração, questionamento, e aperfeiçoamento de ideias ou estudos anteriores. Por mais que o estudo científico seja original, isso não significa que todo pesquisador deva "reinventar a roda",

podendo e devendo muitas vezes aproveitar as pesquisas desenvolvidas por outros estudiosos.

Essa pesquisa é feita a partir do levantamento de referências teóricas já analisadas e publicadas por meios escritos e eletrônicos como livros, ebooks, artigos científicos e web sites. Não deixa de ser um ponto curioso a utilização dos próprios meios virtuais como instrumento de obtenção de informações acerca de um fenômeno que ocorre nesse próprio ambiente.

O objetivo principal desse trabalho é analisar se o sistema penal brasileiro tem a estrutura e os mecanismos suficientes para o enfrentamento ao crescimento dos crimes cibernéticos no Brasil. Procura-se entender se a legislação penal é suficiente para lidar com tais delitos, e se o aparato de investigação e perícia tem condições de dar prosseguimento nas investigações. Além disso questiona-se o acesso à justiça e se as penas normalmente aplicadas aos crimes informáticos tem condições de desestimular a prática criminosa.

No primeiro capítulo houve uma descrição da evolução tecnológica das tecnologias computacionais, mais precisamente da *internet*. O entendimento do processo histórico é importante para que se tenha uma referência de como o desenvolvimento tecnológico foi surpreendentemente rápido, ainda mais se for considerado o tempo levado para que tecnologias passadas tivessem sido desenvolvidas. Foi destacado inclusive o histórico das ameaças virtuais para que se entendesse os prejuízos causados por tais softwares de conteúdo malicioso, e se entendesse a necessidade de medidas eficazes para se lidar com tais programas.

O relacionamento entre o Direito e a informática também teve sua abordagem, pois existe uma interdisciplinariedade atual entre as duas áreas, tendo os que defendem uma maior regulamentação da *internet*, e os que defendem a liberdade sem intervenções estatais nesse meio. O Direito como disciplina que interfere na realidade de modo a manter uma relação de equilíbrio não poderia deixar de questionar o quanto se faz necessária a regulamentação ou não dessa realidade virtual.

Durante o capítulo inicial houve uma análise dos crimes cibernéticos no cotidiano, de modo a entender a real necessidade de intervenção da esfera penal nesse tipo de conduta, considerando por óbvio o respeito ao princípio da intervenção mínima. Além disso, teve destaque algumas conceituações e classificações doutrinárias para esse tipo de delito, de modo a entender se há de fato uma nova espécie de crime, ou apenas crimes antigos com

uma nova “roupagem. Finalizando tal capítulo, foram estudadas as ameaças virtuais mais comuns no cotidiano, a exemplo dos vírus, *worms*, *trojans*, *spyware*, *keylogger*, etc.

Os crimes cibernéticos estão tendo um crescimento tão significativo na atualidade que se faz necessário responder o questionamento se os mecanismos de combate a esse tipo de criminalidade estão realmente adequados. No segundo capítulo desse estudo buscou-se analisar a situação da legislação acerca desse tipo de delito, além é claro da situação da polícia judiciária ou investigativa, e da perícia forense, instituição essa essencial para o combate a esse tipo de delito.

Na análise da legislação buscou-se fazer um paralelo com outros países que já se anteciparam em termos de normatização dos delitos cibernéticos, a exemplo dos Estados Unidos, Alemanha, Inglaterra, França, Chile, dentre outros. Esse direito comparado é uma referência importante que demonstra inclusive a preocupação a nível mundial quanto a esse fenômeno criminal.

Entre as leis objetos de estudo nesse capítulo destacamos as leis 12.735/2012, 12.737/2012 (Lei Carolina Dieckman), e 12.964/2014 (Marco Civil da Internet). Através de uma interpretação crítica teve-se a oportunidade da realização de alguns comentários essenciais sobre a importância e fragilidade dessas normas. O Marco Civil da Internet, por exemplo, foi vendido para a população como uma Constituição da Informática, algo que consideramos de certo modo supervalorizado. Tentou-se responder inclusive a necessidade de legislações específicas para esses crimes, a despeito da utilização de tipos penais já em uso.

Quanto ao aspecto investigativo houve uma análise da estrutura atual da polícia judiciária, e o quanto a mesma se encontra com condições tanto em termos de infraestrutura quanto em treinamentos e profissionais especializados, para o combate a esse tipo de delito. O trabalho procura entender o quanto a polícia investigativa está preparada, e quais os desafios da mesma na investigação dos crimes virtuais.

Como o delito informático apresenta uma faceta bem técnica foi estudada também a estrutura da perícia técnico-científica, sempre destacando a sua importância na busca da verdade real. Assim, procura-se responder a indagação do nível de desenvolvimento da área pericial no Brasil para a produção de provas técnicas que facilitem e subsidiem uma boa investigação e persecução criminal.

Os crimes virtuais têm a peculiaridade de irem além das fronteiras nacionais, sendo comum que um indivíduo de um país utilize recursos de outros países para atacar uma ou mais nações, o que acaba por tornar a investigação desse delito complexa, até mesmo pela sua abrangência transnacional.

Embora o crime seja algo que acompanha a humanidade durante toda a sua existência, atualmente ele assume um caráter globalizado, com organizações criminosas compartilhando informações e exercendo atividades coordenadas de diferentes partes do globo. Com isso fica o questionamento de como as relações internacionais estão sendo firmadas para o combate a essa modalidade criminal.

Com essa situação de constante desenvolvimento tecnológico cria-se o questionamento de quais providências tem sido tomadas pelo Brasil no intuito de firmar acordos que facilitem a cooperação dos outros países nas investigações envolvendo os crimes cibernéticos. O terceiro capítulo desse trabalho inicia com essa preocupação quanto à questão internacional na investigação e persecução criminal.

Há uma crítica em relação aos mecanismos de auxílio mais comuns como cartas rogatórias devido questões temporais, além do estudo da questão da extradição, instrumento esse necessário para julgamento e punição de infratores que costumam superar os limites geográficos nacionais. Esse tema é importante se considerarmos que além da punição de brasileiros, há a situação de como conseguir a punição de criminosos de outras nações, com respeito à soberania e a independência das mesmas.

Um dos objetivos fundamentais desse trabalho é salientar a importância da cooperação internacional para que se superem entraves na busca de informações relevantes para a investigação dos delitos informáticos, de modo que haja uma certa celeridade na troca de informações imprescindíveis para a persecução penal a nível mundial dessas condutas que podem causar danos morais e financeiros em proporções elevadas.

A questão das sanções aplicadas também foi considerada nesse estudo. Foi realizada uma pesquisa acerca da evolução da teoria da pena da fase de uma sanção que visava a agradar divindades até uma manifestação mais humanitária. Foi considerado também o direito que o Estado tem de punir os infratores com o intuito de manter a ordem social.

Quanto à questão da dosimetria da pena, foi estudado o aspecto que a dureza das sanções pode causar na inibição da criminalidade, onde teve-se a intenção de descobrir qual o efeito mais prático da pena na redução dos crimes cibernéticos.

Os países da Comunidade Europeia já se alertaram sobre a importância da cooperação para lidar com os crimes informáticos. A Convenção de Budapeste foi uma boa tentativa para uma integração internacional maior nesse cenário de crescimento do crime computacional.

As investigações muito tem a ganhar com uma redução das burocracias na troca de informações entre os países. Uma das esferas da atuação estatal no combate aos crimes cibernéticos é na fase de execução das penalidades aplicadas, e dai a importância em saber o quanto o juízo da execução pode contribuir para a minimização dos delitos virtuais. Para isso verificou-se o quanto o sistema penitenciário tem condições de fornecer uma resposta penal adequada para esse tipo de crime, mesmo com outras prioridades urgentes.

O acesso à justiça é um direito de todo cidadão, independentemente de sua situação financeira ou “status” social. Entretanto, questiona-se nessa pesquisa se realmente a justiça é acessível a todas as pessoas, inclusive em um dos seus aspectos essenciais, que é a celeridade e uma pronta resposta às demandas solicitadas.

Finalizando o terceiro capítulo houve o estudo de delitos, bastante noticiados na imprensa, relacionados com os crimes cibernéticos, a saber: estupro virtual, pornografia de vingança, estelionato virtual, furto virtual, racismo na Internet, pedofilia virtual, e invasão de dispositivo informático. Nessa parte procurou-se correlacionar tais condutas com situações reais observáveis tanto através de jurisprudência quanto de notícias policiais, onde é possível perceber o quanto tais crimes podem ser perigosos e necessitam ser inibidos com eficiência.

2. CRIMES CIBERNÉTICOS

O entendimento da evolução da tecnologia e das ameaças virtuais ajuda a compreender a necessidade de conhecimento acerca dos crimes cibernéticos, tanto a nível conceitual, quanto em relação às suas classificações. A relação entre o Direito e a informática é uma necessidade no mundo atual, e a regulamentação do ciberespaço é um desafio a ser superado.

2.1 Histórico da *internet* e das ameaças virtuais

A *internet* deve ser considerada como uma das principais invenções científicas e tecnológicas da humanidade. Ela oferece uma quantidade significativa de benefícios associados com a facilidade de troca de conhecimentos e informações, independentemente dos limites geográficos. Qualquer informação pode ser obtida, por exemplo, de qualquer parte do mundo e instantaneamente através da *internet*, o que faz com que haja uma alteração da cultura humana para uma cultura cibernética (LEVY, 1999, p. 222).

Mas como muitas das invenções engenhosas efetuadas pelo ser humano podem ser usadas para o bem ou para o mal, a internet não escapa dessa triste situação. Faz- se importante conhecer a história e evolução dessa tecnologia para se entender a evolução dos crimes que se utilizam desse poderoso meio de comunicação, para que observando o passado, possamos nos prevenir de problemas futuros.

A *internet*, embora atualmente não esteja restrita ao uso de computadores, sendo usada também por vários outros dispositivos como celulares, radares, videogames, entre outros, inegavelmente está bastante associada à invenção e desenvolvimento do computador.

Em 1946 foi criado o primeiro computador digital, o ENIAC, com o objetivo de realizar cálculos balísticos de trajetórias que exigissem um maior conhecimento em matemática, tendo portanto uma função bélica. Embora tenha sido um computador enorme e de difícil manutenção, se comparado aos computadores atuais, o ENIAC foi um importante marco na história da computação (FILHO, 2007, p. 104).

Apesar de a guerra e certos conflitos trazerem várias perspectivas de instabilidades e tristezas, eventos como a Segunda Guerra Mundial e a guerra fria trouxeram importantes incentivos ao desenvolvimento da tecnologia computadorizada.

Em 1957 a União Soviética, motivada pela constante disputa contra os EUA lança o seu primeiro satélite espacial. Devido a esse fato os Estados Unidos se comprometem a levar o homem à lua e buscam criar um sistema de defesa com maior proteção contra destruição. Devido a isso foi criada a Agência de Investigação de Projetos Avançados (*Advanced Research Project Agency* - ARPA), importante instituição para o desenvolvimento da computação (ABREU, 2009, p. 02).

A NASA (*National Aeronautics & Space Administration*), foi criada em 1958, tendo como foco a corrida espacial, o que levou a ARPA a dar prioridade para projetos cujos resultados somente poderiam ser avaliados a longo prazo. Além disso a ARPA passou a realizar parcerias com instituições de ensino, adquirindo com essa estratégia uma atuação mais técnica e científica, o que a levou a investir em pesquisas computacionais.

Com o tempo houve necessidade de uma rede capaz de integrar computadores que estivessem distantes de forma a ser permitida a comunicação de dados entre os mesmos, e assim surgiu em 1969 a ARPANET, rede essa que interligava a Universidade da Califórnia (Los Angeles e Santa Bárbara), a Universidade de *Stanford* (Santa Cruz) e a Universidade de Utah (*Salt Lake City*), realizando o prodígio de se permitir a interação entre essas entidades principalmente em casos de possíveis guerras (UMBATH, 1997, p. 05).

No final dos anos 70 é criado o *Transmission Control Protocol/Internet Protocol* (TCP/IP), considerado o principal protocolo de rede até hoje. Na década de 80 a rede se expandiu pelos Estados Unidos e permitiu a interligação entre universidades, órgãos militares e governo. Em 1986, a ARPANET passa a ser chamada de *internet*.

Para que ocorresse um avanço enorme no uso da internet foi essencial a criação do protocolo *World Wide Web* (WWW) e do *Hypertext Markup Language* (HTML), tornando popular o uso de páginas web e transformando a internet em uma rede mundial de computadores (KUROSE, ROSS, 2010, p. 48).

Qualquer país que queira acompanhar o desenvolvimento mundial não pode se isentar da realidade de evolução do uso da tecnologia nos mais diversos ramos da atividade humana. Com o Brasil não poderia ser diferente. Já no ano de 1961 o Instituto Brasileiro de Geografia e Estatística (IBGE) começou a utilizar um computador de modelo UNIVAC1105.

Em 1964 foi criado o Centro Eletrônico de Processamento de dados do Estado do Paraná, uma empresa pública com a finalidade de realizar diversas funções relacionadas com a informática como consultoria em TI, desenvolvimento e manutenção de sistemas, entre outras funções importantes para o crescimento da internet no Brasil (SILVA, 2016, online).

Em 1965 houve uma associação entre o recém-criado Serviço Federal de Processamento de Dados e o consórcio internacional de telecomunicações por satélites (INTELSAT), além de ter sido criada a Empresa Brasileira de Telecomunicações, como um instrumento do estado para intervir nos serviços de telecomunicações, mantendo o monopólio dessa função (OLIVEIRA, 2012, p. 02).

Todo este processo de introdução ao uso das telecomunicações e computadores culminou na criação do primeiro computador brasileiro pela Universidade de São Paulo (USP): O “patinho feio”. Em 1974 foi criada a Computadores Brasileiros S.A. (COBRA), que pode ser considerada a empresa pioneira no desenvolvimento, produção e comercialização de tecnologia nacional no ramo da informática. Em 1979 foi criada a Secretária Especial de Informática, com ideais protecionistas e como base de apoio a Lei de Informática.

Um passo essencial no uso da internet no Brasil se deu em 1988 com a conexão à Bitnet, que transportava mensagens de correio eletrônico do Laboratório Nacional de Computação Científica (LNCC), da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), e da Universidade Federal do Rio de Janeiro (UFRJ).

Em 1992 foi implementada no Brasil a primeira rede conectada à *internet* de forma a interligar as principais universidades brasileiras. Em 1995 foi criado o comitê gestor da internet no Brasil (CGI.br), com o interesse de coordenar e incentivar os esforços de desenvolvimento de uma *internet* com qualidade técnica, inovação e disseminação de serviços. Uma das tarefas essenciais do CGI.br é a divulgação de informações relativas ao uso da internet no país, o que é utilizado como parâmetros na determinação de políticas essenciais à integração digital dos brasileiros (ADACHI, 2009, p. 37).

Da mesma forma que a *internet* se desenvolvia, se desenvolviam também as ameaças aos recursos tecnológicos disponíveis em rede. Programas cujas informações se autoreplicassem já haviam sido previstos pelo matemático John Von Neumann, o que posteriormente seria a base de vários problemas que se apresentam hoje na forma de códigos maliciosos (LOVISON, 2012, p. 15).

Interessante observar a relação entre a diversão e a habilidade de se criar novidades. Na década de 60, por exemplo, foi desenvolvido por programadores o jogo *Core Wars*, que na verdade se tratava de um código malicioso que ao ser executado, sobrecarregava a memória da máquina do outro jogador. Os criadores desse jogo inventaram também o primeiro antivírus chamado *Reaper*, que operava de modo a apagar as cópias geradas pelo *Core Wars* (MEDEIROS, 2005, p. 09).

Em 1982, Richard Skrenta criou o *Elk Cloner*, considerado por muitos estudiosos como o primeiro vírus a infectar computadores. Esse código malicioso se difundia por cópias de disquete contaminado, uma das técnicas que viriam a causar uma ampla contaminação por vírus posteriores devido a facilidade de se trocar dados por disquetes. Em 1983, o pesquisador Fred Cohen nas suas análises denomina os programas de código nocivo com o nome de "Vírus de computador" (SPPAFORD, 1994, p. 03).

Em 1986, dois paquistaneses criam um vírus de computador denominado *Brain*. Esse vírus causava lentidão no sistema operacional. Esse vírus atingia o setor de inicialização do disco e se propagava através de discos flexíveis (os obsoletos disquetes), além de usar técnicas para dificultar a sua detecção.

Em 1988, foi criado o primeiro antivírus que tinha por finalidade imunizar os sistemas contra o vírus *Brain*. Esse ano foi um marco de uma batalha que dura até hoje, na qual os vírus estão sempre procurando maneiras de sobrepujar técnicas de antivírus, muitas vezes antes das mesmas serem criadas. Nessa mesma época o *internet worm* é liberado na internet infectando cerca de 6.000 computadores (OVERILL, 1998, p. 159).

Em 1989 o *Dark Avenger* contamina computadores de maneira rápida e como tática de ocultação retarda o seu estrago sobre as máquinas, de modo a ficar despercebido por mais tempo. Em 1992 surge o vírus Michelangelo como o primeiro vírus a causar a agitação da mídia. Esse vírus sobregravava partes do disco rígido das vítimas no dia 6 de março, data de nascimento do autor renascentista. Em 1994 ,o primeiro caso de punição de um autor de vírus é registrado pela polícia *Scotland Yard* da Inglaterra. Nesse caso o autor do vírus Pathogen é condenado a 18 meses de prisão (OVERILL, 1998, p. 159).

Em 1999, surge o vírus *Chernobill*, responsável por deixar a unidade de disco rígido e os dados do usuário inacessíveis, causando grandes prejuízos financeiros na China, Turquia e Coréia do Sul . No ano 2000, o vírus *Love Letter* varre a Europa e os EUA em seis dias, causando um prejuízo em torno de 9 milhões de dólares (SANTOS, CAMARGO, 2013, p.

44). Todos esses prejuízos financeiros trazem a crescente necessidade de se reavaliar as políticas de gestão de segurança computacional, criando um novo paradigma de prevenção e atualização constante das políticas de segurança.

Com o avançar da tecnologia, ao permitir o uso de novos dispositivos para acesso à Internet surgiram novos meios de difusão de ameaças. Em 2004, surgiu o primeiro vírus de celular denominado *Cabir*. Esse vírus se disseminava por Bluetooth e descarregava as baterias dos celulares infectados (LEAVITT, 2005, p. 21).

Com essa nova amplitude de meios de contaminação por códigos maliciosos, um desafio em relação ao acúmulo e atualização de conhecimentos e técnicas se tornam latentes para os órgãos policiais, que buscam proteger os bem jurídicos mais importantes para a sociedade, que também podem ser alvos de ataques criminosos através do uso da tecnologia com fins maldosos.

2.2 Direito e Informática

A estabilidade social é fator preponderante em uma sociedade, pois ela é que permite que possamos conviver uns com os outros de maneira pacífica. O Direito é quem favorece o relacionamento mais pleno entre as pessoas e os grupos da sociedade, o que é uma das bases do progresso da mesma (NADER, 2004, p. 25).

Estamos notando uma instabilidade frequente com o aumento da violência e a impunidade, o que acaba gerando uma insegurança jurídica. Essa situação na qual as pessoas deixam de acreditar no aparato do Estado é muito perigosa e pode gerar muitos conflitos. Tais fatos vêm levando a própria sociedade a se organizar, pleiteando direitos tão diferentes de alguns anos atrás, como os direitos informáticos.

Devemos colocar na balança a relação e influências recíprocas entre o direito e a sociedade, analisando uma diferença entre o fato social e o Direito. O fato social é dinâmico e o Direito, conservador, conseguindo abrigar somente parte das relações sociais. Deve haver um aperfeiçoamento do Direito frente a evolução da sociedade, se não por via legislativa, ao menos por via judicial jurisprudencial, pautando–se na democracia e no respeito à dignidade do ser humano.

Essa evolução do Direito deve estar em consonância com o modelo atual de sociedade da informação, modelo esse no qual vivemos muitas vezes sem nos darmos conta.

Atualmente podemos assistir televisão, falar ao telefone, realizar movimentações bancárias, verificar multas de trânsito, pesquisar e estudar pela Internet.

Essas facilidades estão tão em evidência no cotidiano que não há uma percepção clara de que se vive em uma sociedade informatizada, onde os dados fluem a velocidades inimagináveis há alguns anos, e tudo isso influi em nos valores sociais e econômicos (LISBOA, 2016, p. 10).

Vivemos em um período onde as fronteiras geográficas estão sendo superadas em termos de comunicação. As distâncias físicas deixaram de ser um entrave para o crescente mundo globalizado. O termo ciberespaço designa um espaço não físico que se compõem de uma rede de computadores ondes as informações circulam.

O ciberespaço é o novo meio de comunicação que surge da interligação mundial dos computadores. Tal designação, além de especificar a estrutura material de comunicação digital, caracteriza também o universo de informações abrigadas e também os seres humanos que navegam nesse sistema (LEVY, 1999, p. 16)

Como Direito é ao mesmo tempo causa e efeito das relações sociais, ele se configura em si um fenômeno social. Pois o Direito não determina a si próprio, sendo concebido a partir de normas e princípios superiores abstratos, tendo como referência a sociedade como fenômeno social que o produz.

O Direito é fonte instrumental de coexistência social, pois o Direito tem por função precípua auxiliar a manter um mínimo de ordem, direção, e solidariedade. Corresponde, portanto, ao antigo brocardo: *ubi societas, ibis jus* (onde está a sociedade, está o Direito), sendo a recíproca também verdadeira, de tal forma que não se concebe qualquer forma de convivência social sem regras, e nem sociedade sem Direito (REALE, 2002, p. 02).

Com o surgimento do fenômeno da informatização da sociedade, a partir da segunda metade do século XX, vimos surgir uma nova classe de bens ditos informáticos, que se revestem de caráter material, ou imaterial, e que de tal forma se inseriram no novo modelo social e econômico que campeia nas nações mais evoluídas do planeta, de modo a não se poder conceber a sociedade atual sem a figura do computador. As redes sociais estão fazendo parte do dia a dia de forma tão acelerada que muitas vezes os indivíduos não percebem o quanto estas ferramentas interferem positivamente ou negativamente nas suas vidas (SILVA, SILVA, MORAES, p. 05).

Desta maneira, percebemos que a Informática e o Direito são disciplinas relacionadas, mas que funcionam de maneira mais sintonizada quando o Direito, em sua aplicação, é auxiliado pela Informática e vice-versa. A Informática deve estar organizada de acordo com certas regras que assegurem o cumprimento e respeito aos protocolos tecnológicos.

O Direito Informático surge através do ponto de vista da cibernética, que trata da relação entre Direito e Informática até o ponto de vista do conjunto de normas, doutrina e jurisprudência, que venham a regular a complexidade de relações da Informática (PAIVA, 2011, p. 16).

O Direito Informático é uma disciplina que já é reconhecida pelos países mais desenvolvidos, e possui as características de um direito especializado e ao mesmo tempo interdisciplinar e universal. Esse novo ramo do Direito é uma disciplina jurídica que é delimitada pelos sistemas normativos contemporâneos, e que busca regulamentar as modernas tecnologias da informação (PIMENTEL, 2000, p. 153).

A humanidade criou uma civilização global em que elementos fundamentais como as comunicações, as relações comerciais, a educação e até a instituição democrática do voto dependem profundamente da ciência e da tecnologia (SAGAN, 1997, p. 31).

Nos últimos anos, com o crescimento do acesso à rede mundial de computadores – a *internet*, o fenômeno da informatização atinge um nível muito elevado, espalhando-se por todo o globo, passando a compor, de forma definitiva, o modelo de produção e circulação de riquezas.

Tal fenômeno tem influências no mundo jurídico, e vai demandar a existência de novos mecanismos de solução para os novos conflitos surgidos dessa revolução computacional. A *internet* é uma ferramenta de poder e a utilização em massa de novas tecnologias, e por isso requer uma normatização jurídica e reflexão ética (PICON, ANTUNES, DUARTE, 2013, p. 989).

O debate sobre a regulamentação da *internet* tem aumentado bastante na atualidade. Iniciativas governamentais vem sendo implantadas em países ao redor do mundo com o intuito de regulamentar o ciberespaço, o que acaba por gerar um debate social.

O tema é complexo se considerarmos a natureza fluídica do ciberespaço, que rompe fronteiras e redimensiona as questões sociais, econômicas, e políticas. O debate em relação à regulamentação do ciberespaço envolve a garantia das liberdades individuais e coletivas, o

direito à privacidade, e as possibilidades de censura às manifestações na *internet* (SEGURADO, 2011, p.46).

Há uma problemática quando se pensa em regulamentar o espaço virtual, pois há os que argumentam que isso seria censura, o que é vedada pela Constituição, sendo um ataque à liberdade de expressão e manifestação. Por outro lado há uma facilidade maior de ataque aos direitos individuais, além de instigação a crimes como racismo, calúnia, difamação, pornografia infantil, dentre outros. Tem-se, portanto, que a internet necessita de regras para proteção dos direitos fundamentais, apesar de a Internet ser uma rede aberta que proporciona o desenvolvimento de práticas colaborativas e não-proprietárias (SEGURADO, LIMA, AMENI, 2014, p.2).

Atualmente, com a globalização e as transformações que se operam no cenário mundial, afetando os campos econômico, social, político, e organizacional, as empresas e governos vem procurando estratégias para se manterem competitivas, sobrevivendo assim em um mercado de competição acirrada. Os sistemas de informação surgem como meio de otimizar os fluxos de informação e conhecimento entre as organizações (MARTINS, MELO, 2012, p. 02).

A informação assume um caráter vital em um mundo cada vez mais globalizado e interconectado. Os mecanismos de segurança devem procurar garantir autenticação, controle de acesso, confidencialidade de dados, e integralidade (STARLLINGS, 2008, p. 09).

Os prejuízos oriundos de um ataque a essa segurança computacional podem se manifestar tanto financeiramente como moralmente. O Direito Constitucional Brasileiro não exclui da apreciação do poder judiciário qualquer violação ou ameaça a um direito. Há, portanto, a necessidade de mecanismos legislativos que auxiliem na proteção dos direitos e garantias fundamentais das pessoas que utilizam a rede mundial de computadores.

O Direito da Informática, o Direito da Internet, ou o Direito do Ciberespaço nada mais seria que a introdução do elemento *internet*. O advento das tecnologias telemáticas, ou da *internet*, ainda que tenha causado uma revolução no mundo, ainda deve interagir com o mundo jurídico.

Importante salientar que os fenômenos da informática passaram a ser objetos do direito antes do aparecimento do Direito da Informática (CASTRO, 2014, p.4). Isso porque o Direito sempre deve dar resposta a situações de conflito, mesmo que não haja ainda nenhuma previsão legal sobre o assunto.

A vida social dos países vai se assentando no meio informático, de tal forma que o computador pode se tornar o calcanhar de aquiles da sociedade pós-industrial. Devido a esse risco recorre-se à proteção proporcionada pelo Direito Penal (ASCENSAO, 2002, p.255).

O sistema jurídico deve se adaptar à evolução da sociedade, uma vez que o Direito só tem utilidade quando ele consegue realmente normatizar o convívio social. Não se concebe nos dias atuais uma ordem jurídica que não apresente previsões legislativas acerca da interação com o mundo virtual, até mesmo porque a maioria das pessoas já estão de alguma forma inseridas tecnologicamente.

A rapidez da evolução, tanto quantitativa quanto quanto qualitativa, da tecnologia se mostrou incompatível com os conceitos e padrões, o que acabou culminando com o surgimento de conflitos entre as novas tecnologias e a sociedade. A presença cada vez mais forte dos aparelhos informáticos na vida das pessoas, o aumento da capacidade de coleta e análise de dados pelas empresas e instituições governamentais têm proporcionado benefícios, mas também malefícios.

Como a tecnologia digital hoje é uma realidade, e devido se estar diante do aparecimento de lacunas objetivas, o direito deve estudar e procurar preenchê-las. Com a popularização da Internet se evidencia a criação de novos conceitos sobre valores tradicionais como liberdade, privacidade, e crimes digitais (CORREA, 2000, p. 02).

Apesar de o Direito apresentar uma postura mais reativa e se mostrar de certo modo atrasado em relação às evoluções operadas na sociedade, ainda assim o mesmo tem que evoluir a ponto de não perder a sua eficácia social. Há, portanto, a necessidade de maiores estudos e regulamentações acerca de certos fatos computacionais como os delitos cibernéticos.

2.3 Crimes Cibernéticos no cotidiano

A tecnologia, sem sombra de dúvidas, trouxe um nível de vida jamais imaginado por pessoas de tempos mais antigos. Um dos avanços mais impressionantes vivenciados pela humanidade foi a criação da *internet*. Podemos dizer que vivemos em uma era digital que influencia os setores da sociedade, comércio, política, serviços, entretenimento, informação, e relacionamentos (KOHN, MORAES, 2007, p. 05). Com o advento da rede mundial de

computadores fronteiras foram vencidas, e podemos realizar negociações, obter informações e nos comunicarmos com pessoas de diferentes partes do mundo.

Infelizmente, o poder que a tecnologia da informática trouxe veio acompanhado de sérios riscos para as pessoas. A facilidade de ocultar a sua identidade através da Internet, atrai diversos tipos de criminosos, tanto tradicionais como ocasionais. Os criminosos que utilizam as redes sociais acabam assim sendo protegidos pelo anonimato (NETO, 2009, p. 11).

O gráfico abaixo ilustra o avanço do número de incidentes envolvendo dispositivos informáticos informados ao CERT.br. Dependendo do perfil do atacante, o mesmo pode ter motivações de invadir o sistema para adquirir conhecimentos e testar habilidades, ou mesmo progredir para outras atitudes ilícitas com vistas a conseguir vantagens econômicas.

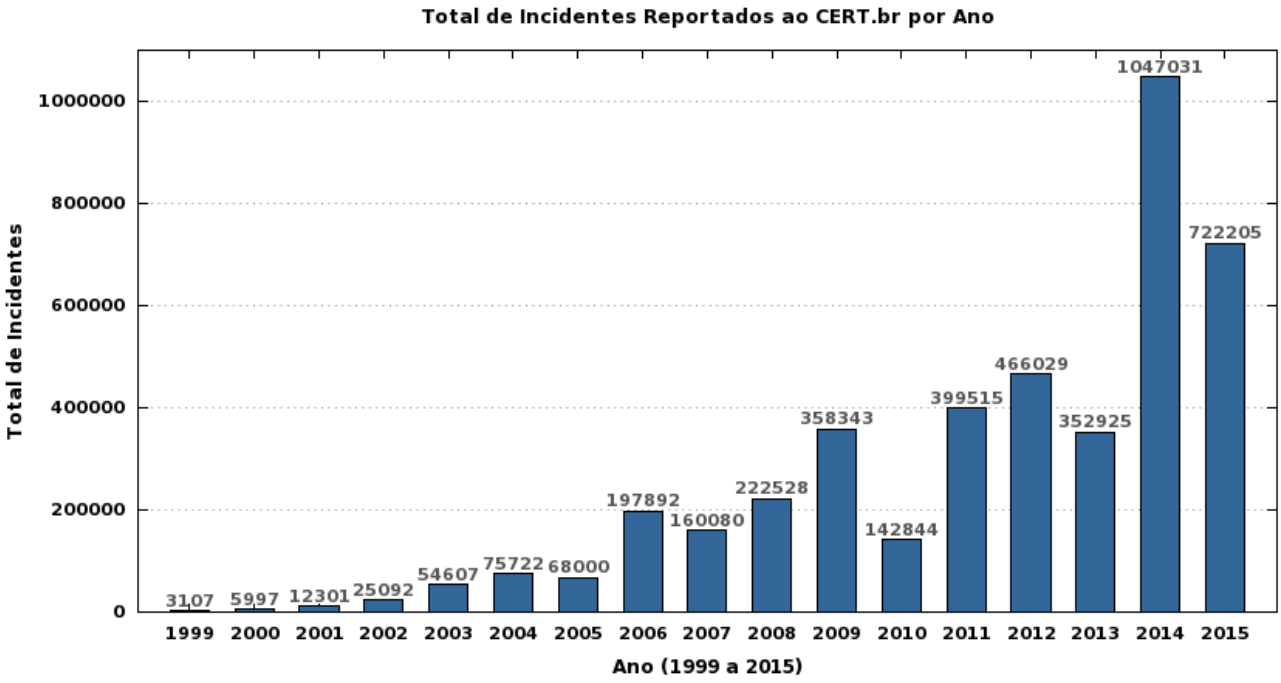


Figura 1: Fonte: Disponível em: <http://blog.diplan.com.br/estatisticas-do-cert-br-incidentes-2015/> Acesso em set. 2017.

A sensação de impunidade acaba sendo um atrativo muito forte para o crescimento desse tipo de delito. As ameaças podem ser tanto por meio de monitoramentos não autorizados do sistema, como através de ataques mais sofisticados realizados por hackers (PINHEIRO, 2007, p. 02).

Os crimes cibernéticos estão tão em evidência nos dias atuais que se faz necessário o aprimoramento dos mecanismos de investigação para que haja um combate realmente efetivo contra esse tipo de delito. Divisões de combate aos crimes computacionais é uma necessidade cada vez mais presente nos dias atuais.

A esfera penal com o avanço da tecnologia teve a necessidade de delegacias especializadas para o combate a esse tipo de crime (MENDES,VIEIRA, online). Entretanto, apesar da necessidade e do surgimento de algumas delegacias especiais, ainda falta muito para que a população tenha acesso ao aparato investigativo e judicial do Estado. A maioria dos crimes nem sequer são investigados até mesmo pelo descrédito que a população tem em relação à justiça do país.

Como os crimes cibernéticos não reconhecem fronteiras se faz necessária uma maior integração internacional entre os Estados para lidar com esses crimes que afetam ou apresentam riscos para todos os países, e esse risco fica ainda maior quando considerarmos o crescimento das organizações criminosas.

A prática criminal é tão antiga quanto à própria humanidade, mas a criminalidade a nível global, com a formação de poderosas organizações criminosas com atividades espalhadas em todas as partes do globo, é um fenômeno que afeta profundamente toda economia tanto a nível nacional quanto internacional, além de repercutir na política, na segurança, e na sociedade de forma geral (CASTELLS, 2000, p. 202). Incrivelmente, hoje temos grupos de especialistas em computação atuando de forma criminosa e causando as mais graves violações aos direitos das outras pessoas.

Esse fenômeno do crescimento das organizações criminais tem se tornado alarmante nos últimos tempos, e o pior, tem adquirido uma escala de ordem globalizada. A possibilidade de cometer um delito de um local muito distante tem sido um incentivo para que grupos de pessoas, às vezes de diversos países, se unam para o cometimento de delitos através de dispositivos computacionais.

Os países da Comunidade Europeia, por exemplo, já se alertaram sobre a importância da cooperação para lidar com os crimes informáticos. A Convenção de Budapeste foi uma boa tentativa para uma integração internacional maior nesse cenário de crescimento do crime computacional. As investigações muito tendem a ganhar com uma redução das burocracias na troca de informações entre os países. Importante destacar que o Brasil aparece na 33ª

posição do ranking do Global Security Map, formado por 219 países, em relação à segurança cibernética (CARDOSO, 2015, online).

Apesar de para muitos o atrativo da Internet ser o fato de a mesma ser como uma “terra sem lei”, uma ponderação acerca dos valores mais importantes vai ressaltar o quanto um tratamento especializado dos crimes nesse meio é crucial para uma utilização mais segura da Internet em atividades essenciais como comércio, serviços bancários, entre outros. Existe uma série de sistemas de informação onde a confiabilidade é um fator essencial. Uma prova disso é o crescimento do comércio eletrônico e das operações bancárias online.

O próprio sistema governamental precisa se atentar aos requisitos de segurança, ainda mais se considerarmos o número de informações sigilosas presentes em tais esferas. Entretanto, o que fazer quando a prevenção falha? Dai a necessidade de uma repressão a possíveis ataques através da evolução do direito, de tal forma que o ciberespaço não se transforme em um universo paralelo sem alcance penal (PINHEIRO, p. 12). Legislações mais eficazes e aparato investigativo atuante são requisitos essenciais para que todos possam lidar com esse novo cenário virtual.

Pode-se perceber que em um período relativamente curto de tempo houve uma evolução muito grande tanto das tecnologias quanto das ameaças virtuais, o que exige uma reação estatal. Procura-se dar uma noção sobre os procedimentos de investigação de crimes cibernéticos destacando as dificuldades decorrentes do anonimato proporcionado pelas facilidades de ocultação do criminoso.

Importante salientar a importância da cooperação internacional para que se superem entraves na busca de informações relevantes para a investigação desse tipo de crime que desconhece fronteiras, e que pode causar danos morais, financeiros, e outros em proporções elevadas (BUENO, 2013, p. 10).

Nesse novo cenário de desenfreado desenvolvimento tecnológico busca-se demonstrar que com uma correta ação organizada em nível internacional torna-se possível que os benefícios advindos da rede mundial de computadores não sejam diminuídos em face dos diferentes problemas advindos das ameaças cibernéticas.

Uma pergunta interessante a ser respondida seria o que justificaria a criação de uma legislação específica para o combate aos crimes cibernéticos, visto o princípio da intervenção mínima do Direito Penal. Por este princípio o direito penal só deveria ser aplicado em

situações nas quais haja extrema necessidade, de forma a manter-se como princípio subsidiário (*ultima ratio*) e fragmentário.

Assim o Estado só interveria através da esfera penal quando outros ramos do Direito não conseguissem prevenir a conduta ilícita. Já pelo princípio da fragmentariedade o Direito Penal só deve atuar quando houver relevante lesão ou perigo de dano a algum bem jurídico tutelado, protegendo fragmentos do universo jurídico (JESUS, 2012, p. 52).

Interessante observar que conforme a própria sociedade evoluiu, novos bens acabaram por necessitar de proteção jurídica, a exemplo da liberdade cibernética, do comércio eletrônico, vida privada, intimidade, e direitos autorais na internet. O Direito portanto deve acompanhar a evolução da sociedade, e já que a mesma está migrando para o ciberespaço, pra lá o direito também deve se voltar em respeito ao *Ubi Societas, ibi jus*. Assim, o Direito penal informático deve procurar proteger como bem jurídico as informações:

> Assim, está claro que a denominação mais precisa para os delitos ora em estudo é "crimes informáticos" ou "delitos informáticos", por basear-se no bem jurídico penalmente tutelado, que é a inviolabilidade das informações automatizadas (dados) (TULIO, 2001, p.33).

A informação surge no mundo de hoje como um bem de importância crucial a ser protegido pelo Direito, de tal modo que uma informação pode modificar a vida de várias pessoas, além de em um mundo globalizado e interligado como o atual, ser o diferencial em um mercado cada vez mais competitivo. A segurança e a confiabilidade dos dados são requisitos críticos a serem observados por todas as instituições, e dai a importância da regulamentação e da criação de tipos penais cibernéticos.

2.4 Conceito de Crimes Cibernéticos

A conceituação dessa espécie de crime não é algo simples, visto as várias facetas que as tecnologias podem apresentar atualmente. Devido ainda estarmos tratando de uma doutrina em formação, ainda não é pacífico o entendimento acerca do que poderia ser denominado crime cibernético.

Existem, por exemplo, muitos nomes para denominação dos crimes cibernéticos, de tal forma que não existe uma nomenclatura sedimentada acerca do seu conceito. De uma maneira ou de outra o que importa não é o nome atribuído a esses crimes, uma vez que o que deve ser observado é o uso de dispositivos informáticos e a rede de transmissão de dados com o intuito de delinquir, lesando um bem jurídico. Além disso a conduta deve ser típica, antijurídica, e culpável (DA SILVA, 2015, p.42).

Importante destacar que ainda existem muitos ilícitos praticados em meios virtuais que não estão tipificados, o que torna incorreta sua denominação a priori como crimes cibernéticos, pelo menos do ponto de vista da Constituição Federal do Brasil e do Código Penal Brasileiro.

Algo essencial para o conceito desse tipo de crime é que os crimes de informática são condutas descritas em tipos penais realizadas por computadores ou contra computadores, sistemas de informação, ou dados nele armazenados (CASTRO, 2003, p. 01).

Houve assim uma evolução do conceito de cibernéticos para algo mais abrangente, o que foi de acordo com a própria evolução tecnológica. É só observar que existe um deslocamento de foco em relação aos dispositivos computacionais isolados para sistemas de informações mais complexos.

A palavra cibercrime surgiu após uma reunião em *Lyon*, na França, de um grupo de nações denominada g8. Nessa reunião foram discutidos os crimes cometidos via aparelhos eletrônicos, ou pela disseminação de informações através da *internet*. Esse grupo havia se reunido para estudar os problemas da criminalidade surgidos e promovidos pela *internet* (PERRIN, 2006, p.1).

Uma definição bem completa para o crime de informática é a que o caracteriza como uma conduta atentatória ao estado natural dos dados e recursos oferecido pelos sistemas de processamento de dados, e pela compilação, armazenamento, e transmissão dos dados. O crime de informática, portanto, é aquele procedimento que ataca os dados armazenados, compilados, transmissíveis, ou em transmissão.

Tal crime pressupõe a utilização de software e hardware para perpetrá-lo. Toda conduta típica, antijurídica, e culpável dirigida contra ou pela utilização de processamento eletrônico ou transmissão de dados caracteriza tal crime. Assim utiliza-se um sistema de informática para prejudicar um bem jurídico que pertença à ordem econômica, à integridade

corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, entre outros (Fabrício Rosa 2002 *apud* SCHMIDT, 2014, online).

Nessa ampla definição o crime de informática tem como elemento essencial na sua caracterização a presença do dispositivo computacional para a prática das mais variadas condutas ilícitas. Considera-se cibercrime toda atividade onde um computador é utilizado como ferramenta, base de ataque, ou meio de crime (CASSANTI, 2014, p. 20).

Esse termo está sendo bastante utilizado atualmente, entretanto existem outras denominações para esse tipo de crime como “crimes digitais”, “crimes eletrônicos”, “crimes informáticos”, “e-crimes”, e “crimes virtuais”. Acredita-se para efeitos desse presente estudo que todas essas denominações são válidas e de fácil compreensão, e que todas elas remetem ao conceito de Crime Cibernético.

Crime Cibernético é o crime que ocorre no meio cibernético. Nesses delitos o computador é utilizado como uma ferramenta, um alvo, de modo incidental, ou associado. É uma atividade criminosa relacionada com a utilização ilegal do computador ou da rede, pelo acesso não-autorizado e roubo de dados online que podem ser utilizados de diversas formas contra as vítimas (AGARWALL, KASUHIK, 2014, p. 02).

Importante destacar essa faceta dos crimes cibernéticos da falta de autorização aos sistemas, de modo que as condutas de profissionais de “hacking” são consideradas lícitas, devido o fato de esses especialistas estarem autorizados a realizarem procedimentos e testes computacionais.

Uma definição simplificada considera cibercrime aquela conduta ilegal na qual o computador é utilizado como objeto, alvo, ou ambos (NAGPAL, 2008, p. 02). Essa definição tem um aspecto peculiar de fornecer uma generalização maior para essas condutas. Assim, o infrator que aciona um dispositivo computacional que acionasse uma “bomba”, por exemplo, estaria inserido no rol de delitos cibernéticos. Uma definição bem interessante sobre cibercrime que considera o ângulo das vítimas é a seguinte:

> ofensas cometidas contra indivíduos ou grupos de indivíduos com a motivação criminosa de intencionalmente prejudicar a reputação da vítima ou lhe causar sofrimento físico ou mental, direta ou indiretamente, usando redes modernas de telecomunicações como a internet (Salas de Chat, Grupos de notícias) e celulares (HALDER, JAISHANKAR, 2011, online).

O conceito acima tem a como peculiaridade o fato de observar a situação da vítima, a tornando ponto chave como alvo da conduta criminosa, além de ter o mérito de considerar o aparelho celular como um dos dispositivos que podem ser utilizados para ataque. Entretanto, essa definição ainda não parece completa suficiente.

Os crimes digitais são crimes perpetrados em ambientes que permitem a ausência física do sujeito ativo, e devido a isso ficaram usualmente conhecidos como delitos virtuais (TERCEIRO, 2009, p. 02). Nesse conceito fica mais evidente a questão do anonimato devido à ausência física dos autores do crime.

O delito informático englobaria a conduta típica e ilícita, que pode constituir crime ou contravenção, conduta dolosa ou culposa, comissiva ou omissiva, praticado por pessoa física ou jurídica, que utiliza dispositivo computacional, em rede ou offline, e que ofenda, de forma direta ou indireta, a segurança da informação, que tem como princípios a confidencialidade, disponibilidade, e integridade (ROSSINI, 2004, p. 110 apud GIMINEZ, 2013, p. 08).

Interessante observar que nesse último conceito não há a necessidade de que o dispositivo esteja conectado à Internet para que seja cometido algum delito informático. Tal conceito é bem completo e consegue oferecer uma ideia do que sejam todos os delitos virtuais.

A Organização para Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas (OCDE) definiu como crime informático qualquer conduta ilegal e antiética não autorizada, que envolva processamento automatizado de dados e/ou a transmissão de dados (REIS, 1997, p. 25). Percebe-se, portanto, a preocupação a nível internacional das organizações com a definição, o conhecimento, e o combate a esse tipo de crime que pode causar consequências econômicas catastróficas.

Importante se observar que por se tratar de uma modalidade de crime de certa forma recente, ainda mais se compararmos com os crimes mais comuns, há ainda uma dificuldade de consenso na definição do que é o crime cibernético. A evolução tecnológica também traz novos nuances para atualização desse conceito.

Hoje, por exemplo, podemos ver aparelhos celulares funcionando de forma bastante similar aos dispositivos computacionais, o que representa uma evolução tecnológica não imaginada por muitos na época. A tendência, portanto, é a atualização conceitual do crime cibernético de modo que o mesmo seja caracterizado como uma afronta a um sistema de informação, algo bem mais abrangente que apenas o computador.

O crime cibernético pode ser encarado como uma afronta a um sistema de informação. Os sistemas de informação pode ser definido como um conjunto de componentes interligados que coletam, processam, armazenam, e distribuem informações para apoiar a coordenação, o controle, e a tomada de decisões pelas organizações (LAUDON, 2010, p. 12).

Essa definição acaba sendo consequência dos riscos cada vez maiores que os ataque cibernéticos oferecem às grandes corporações e empresas. No mundo globalizado em que vivemos a segurança da informação pode ser o diferencial para sobrevivência das empresas no mercado. Parece bem acertada a utilização do termo sistemas de informação na definição de crimes cibernéticos, pois tais sistemas podem funcionar como um mero celular, até grandes redes de computadores.

Um conceito antigo, embora válido, temos a definição do Departamento de Justiça dos Estados Unidos, que define esses crimes como qualquer violação das leis criminais que envolvem a necessidade de conhecimentos computacionais para sua realização, investigação, e processo (DEPARTMENT OF JUSTICE, 1989, p. 02). Nessa definição entra em destaque a necessidade de conhecimentos especializados para a prática desse delito.

Como se pode perceber todos esses conceitos podem ser aplicados, embora alguns deles destaquem alguma faceta do delito. Para esse estudo adequado é a definição que considera esses crimes como condutas típicas, ilícitas, e culpáveis, que se utilizam de dispositivos computacionais para ataques a sistemas de informação, com o objetivo de obtenção de alguma vantagem ou acesso indevido.

2.5 Classificação de Crimes Cibernéticos

Há uma divisão que classifica os tipos de crimes informáticos em tipos caracterizados pelo uso de instrumentos informáticos, crimes caracterizados pela agressão ao meio informático, e pelo conteúdo da mensagem disponível em rede. Em todas essas modalidades, o bem ou meio informático deve aparecer como elemento típico ou determinante (ASCENSAO, 2002, p.256). Essa classificação ajuda a entender a motivação do criminoso, se o mesmo deseja atingir diretamente um determinado sistema informático, ou se o infrator visa um bem diverso do computacional, utilizando o elemento digital como instrumento para a prática de outro delito. Huebner et al (2003, p. 03) fornece uma interessante classificação,

até mesmo porque é muito utilizada pela doutrina, onde o mesmo divide os crimes cibernéticos da seguinte forma:

- Crimes centrados no computador: São os tipos de crime que apresentam como objetivo primordial o ataque a sistemas computacionais, redes, dispositivos de armazenamento, e outros dispositivos computacionais. Como exemplo desse tipo de ataque podemos citar o ataque de negação de serviço e o ataque *defacement* , que visa alterar uma página web.

- Crimes auxiliados por computador: Nesse tipo de crime o computador é utilizado como uma ferramenta para auxiliar na prática de um crime onde o uso do computador não é estritamente necessário. Esse tipo de crime pode ser considerado como uma forma alternativa de cometimento de infrações tradicionais. Pode-se mencionar como exemplo o crime de estelionato praticado com o auxílio de páginas falsas que simulam um site de instituição bancária, que faz com que alguns usuários se enganem e acessem o site falso fornecendo suas credenciais de acesso ao criminoso, o que pode utilizar tal acesso para obter alguma vantagem indevida, o que geraria um provável prejuízo econômico à vítima.

- Crimes incidentais por computador: Uma atividade criminosa onde a utilização do computador seja incidental ou eventual para a atividade em si. Como exemplo podemos citar a contabilidade do tráfico de drogas ou de qualquer outro crime, no qual o computador é apenas uma nova ferramenta utilizada em substituição a outras ferramentas tradicionais.

Na doutrina brasileira há uma classificação na qual os delitos informáticos podem ser classificados como próprios ou impróprios. Os crimes próprios seriam aqueles praticados com o objetivo de atingir o próprio sistema computacional, a exemplo dos serviços de negação de serviço, no qual o intuito do atacante é deixar um site indisponível, por exemplo.

Já os crimes impróprios são aqueles que utilizam a internet ou os meios tecnológicos apenas como uma ferramenta para realização do ilícito, a exemplo dos crimes de falsificação,

de documentos, furto, e estelionato (SOBRAL, BEZERRA, 2016, p. 17). No crime impróprio a intenção do agressor de lesar bem jurídico diverso do bem informático.

As ações prejudiciais podem ser atípicas ou configurar um crime cibernético. Quando a ação prejudicial é atípica, ela pode até causar prejuízo ou transtorno para vítima através da rede mundial de computadores, mas não são tipificados em lei, o que impossibilita a sua punição na esfera penal. Já os crimes cibernéticos podem ser divididos em crimes cibernéticos abertos e crimes exclusivamente cibernéticos.

Os crimes exclusivamente cibernéticos são aqueles que necessariamente precisam do meio computacional para cometer tal crime (como é o caso do crime de invasão de dispositivo informático, artigos 154-A e 154-B do Código Penal Brasileiro). Já os crimes cibernéticos abertos são aqueles que podem ou não ser praticados pelo dispositivo ou sistema informático, como é o caso de dos crimes de violação de direito do autor ou estelionato, que pode ser praticado tanto no ambiente virtual quanto fora do mesmo (WENDT, JORGE, 2012, p. 19).

Essa última classificação é muito boa por considerar tanto os crimes nos quais o elemento computacional é imprescindível, quanto outras condutas que não precisam necessariamente de tecnologia para serem perpetrados, apesar de o dispositivo informático facilitar bastante a concretização do delito.

Existe também uma classificação que divide os crimes digitais em quatro tipos, na qual o principal bem jurídico a ser protegido pela lei penal é a inviolabilidade da informação. Assim nos crimes informáticos próprios o computador é usado como meio para executar o crime, mas não existe a violação da informação automatizada, a exemplo dos crimes de ameaça e incitação ao crime.

Já nos crimes informáticos próprios há a proteção do bem jurídico inviolabilidade de dados, o que é o caso do delito de invasão de dispositivo informático e inserção de dados falsos em sistema de informações, por exemplo.

No caso dos crimes mistos, além de se proteger a inviolabilidade de dados, a legislação também procura proteger bem jurídico de natureza diversa a exemplo do crime eleitoral da Lei nº 9504/1997, do art 72. Por fim o crime informático mediato ou direto é aquele que é o delito fim não informático, que acaba herdando a característica do meio para consumar o crime. (VIANA, MACHADO, 2013, p.15).

Tal classificação tem a vantagem de categorizar bem os crimes, dando uma ideia ampla acerca das possibilidades de utilização dos meios informáticos para o ataque a diferentes bens jurídicos a serem protegidos pela legislação penal.

2.6. Principais Ameaças

Existem uma série de ameaças aos dispositivos computacionais, o que cria a necessidade de nos atualizarmos constantemente em relação aos mecanismos de segurança. Importante o conhecimento desses códigos maliciosos até mesmo para o trabalho no universo jurídico, seja na parte legislativa, investigativa, ou judicial. Um mínimo de conhecimento dessas ameaças é essencial para uma melhor definição e enquadramento no devido tipo penal.

Os vírus são programas ou partes de programas de um computador que se propagam inserindo cópias suas em arquivos ou outros programas. Eles são desenvolvidos para alterar nocivamente e clandestinamente softwares instalados em um computador (TAMEGA, 2003, p. 40).

O vírus de boot, por exemplo, vem causando vários problemas aos usuários de computador. Esse vírus tem como foco esse setor de inicialização ou de *boot*. Um exemplo desse tipo de infecção ocorre quando um usuário insere um pendrive contaminado em um computador, que ao ser infectado pelo vírus de *boot*, pode ser um foco transmissor de vírus para outros pendrives inseridos posteriormente, espalhando com isso o vírus em diversas máquinas.

Botnet é um código malicioso que permite a um intruso manipular a distância o computador da sua vítima como se fosse um robô. Ele explora vulnerabilidade dos sistemas operacionais e seus softwares. Normalmente a vítima não sabe que o seu computador está infectado com esse código malicioso e nem que está realizando ataques contra outros computadores.

O *Botnet* é muito utilizado nos ataques de negação de serviço distribuído, nos quais vários computadores enviam requisição a um servidor de modo a causar uma sobrecarga no mesmo, tornando seus serviços indisponíveis (CERT.br, 2012, p. 26).

Defacement é um tipo de ataque realizado com o intuito de alterar páginas de sites. Normalmente conhecidos como “pichadores” normalmente os *defaces* realizam seus ataques com o intuito de propagar ideias e convicções políticas, ambientais, religiosas etc.

Na busca de realizar as alterações nas páginas ou blogs os *defaces* costumam explorar erros do servidor Web e vulnerabilidades da linguagem de programação de modo a obter o acesso indevido para alterar o conteúdo do site remotamente (FERREIRA, 2015, online).

O cavalo de troia (trojan horse) é um tipo de código malicioso que permite que o computador do atacante acesse à distância o computador da vítima, permitindo desse modo acesso a dados confidenciais. Esse programa oculta seus objetivos sob a camuflagem de outro programa útil ou inofensivo. O ataque por trojan é realizado quando a vítima recebe esse código malicioso, que ao ser executado abre uma “porta dos fundos” para acesso remoto ao sistema da vítima, como se fosse um usuário legítimo. Esses programas oferecem grande risco para a máquina infectada pois o invasor tem total controle sobre a sua máquina (TAMEGA, 2003, p. 38).

Keylogger é um tipo de programa que permite monitorar tudo o que o usuário digita com o teclado do seu computador. Atualmente esses programas permitem não apenas captar as teclas digitadas, mas inclusive tirar fotos das telas do computador, mecanismo utilizado na captura de dados bancários em sistemas que usam teclado virtual, por exemplo. O *keylogger* normalmente é um software instalado no computador, mas pode inclusive ser um hardware colocado entre o teclado e a CPU (MACHADO, 2012, online).

O *Hijacker* é um tipo de código malicioso que “sequestra” o seu navegador web e lhe direciona a páginas não desejadas. Pode ser utilizado, inclusive, na exibição de propagandas, ou exibições de conteúdo pornográfico ou relacionados a sites fraudulentos (DUARTE, 2015, online).

Rootkits são programas que ficam ocultos no computador dos alvos, e que podem ser instalados pelo invasor com acesso físico ao computador, ou remotamente através de outra máquina (CERT.br, 2012, p. 29). O problema maior dos rootkits é que dificilmente eles são detectados por antivírus, o que leva o usuário a ficar com o seu computador infectado por bastante tempo sem desconfiar desse software.

Para manter essa “invisibilidade”, o *rootkit*, ao ser lido ou acessado usa um mecanismo de filtragem dos dados para que o sistema operacional ou antivírus não detecte o

código malicioso. Comumente, esse software é enviado por e-mail para usuários, que inocentemente copiam o arquivo e o executam na sua máquina. Através de técnicas de engenharia social, o atacante convence a vítima, muitas vezes se passando por uma instituição de credibilidade, a realizarem essas atividades que podem comprometer a segurança do sistema.

Sniffers são programas que monitoram o tráfego de rede, interceptando e analisando todos os dados que nela trafegam, podendo devido a isso fornecer informações sensíveis do usuário. Os *Sniffers* podem fornecer informações de login e senha, páginas acessadas, vulnerabilidades da rede, além de outras informações confidenciais como e-mails (MITISHASHI, 2011, p. 30).

Em redes corporativas o *sniffer* pode ser usado para monitorar o acesso dos funcionários, mas quando nas mãos de cibercriminosos pode ser uma base forte para os mais variados ataques e problemas. Como um forte representante desse tipo de programa temos o software *Wireshark*, que permite monitoramento de redes sem fio.

Backdoor é um tipo de programa que deixa uma “porta dos fundos”, ou seja uma brecha ou vulnerabilidade que permite que o invasor acesse as máquinas infectadas por esse programa (MORAES, 2010, p. 190). Já os Hoax são um conjunto de falsas histórias com conteúdo alarmante e falso (SCOTTI, 2005, p. 24).

Inventam mensagens como projetos de lei, desastres naturais, conspirações, lendas, pessoas doentes e mensagens religiosas que causam prejuízos para as vítimas. Através dos *hoaxs* pessoas de boa fé espalham essas falsas informações através de e-mail, sites ou redes sociais. É comum esses boatos virem acompanhados de solicitação para que o receptor encaminhe a mensagem para sua lista de contatos de e-mail através de promessas de prêmios ou de colaboração para uma boa causa como auxílio financeiro a alguma pessoa doente.

Phishing Scam consiste em uma técnica na qual o cibercriminoso envia um e-mail pelo qual convence a vítima a lhe fornecer informações confidenciais como senhas, dados bancários, ou outras informações pessoais. A vítima pode fornecer esses dados através de encaminhamento a páginas falsas, com possíveis códigos maliciosos, através de preenchimento de formulários, por exemplo.

Uma das táticas do atacante que utiliza *phishing scam* é convencer a vítima a clicar em um link, que direciona a uma página bastante semelhante a que o usuário espera, como por

exemplo a página de um banco (LAU, 2006, p. 66). Convencido da veracidade da página o usuário fica propenso a fornecer seus dados ou executar certos códigos maliciosos, que podem instalar um *spyware* em sua máquina e fornecer ao cibercriminoso dados que podem prejudicar a vítima.

O conhecimento acerca desses tipos de códigos maliciosos é necessário por oferecer uma direção para que o investigador e o perito criminal consigam apurar um delito cibernético. Isso pode beneficiar inclusive a cognição do juiz criminal que analisará o caso concreto que envolva aspectos tecnológicos. Conhecendo essas ameaças da para se ter uma ideia da amplitude dos danos que as mesmas podem causar,

3. LEGISLAÇÃO, INVESTIGAÇÃO, E PERÍCIA DE CRIMES CIBERNÉTICOS

Entre os mecanismos de combate aos crimes cibernéticos no Direito Penal a legislação, investigação, e perícia assumem posições essenciais para o bom andamento dos processos criminais, tendo como consequência a punição dos indivíduos que se aproveitam dos meios digitais para lesar bens jurídicos tutelados pela esfera penal. Esses mecanismos são aspectos chaves para inibição do crescimento dessas condutas inadequadas realizadas através da *internet*.

3.1 Legislação de Crimes Cibernéticos

As condutas ilícitas praticadas através do ambiente informático prejudicam a manutenção dos níveis adequados de segurança e credibilidade necessários a qualquer negócio jurídico. Fica realmente muito complicado a situação na qual precise-se realizar ações em um ambiente virtual que não ofereça o mínimo de segurança e de punição para os aproveitadores.

Além de tudo os delitos virtuais interferem no cotidiano de muitas pessoas, de modo que esse novo ambiente se torna inapto para a manutenção de relações sociais. A conquista da confiança nesses contextos se mostra essencial, de tal forma que deve-se buscar a redução dos riscos de fraude, erro, roubo, e uso indevido de informações (ABREU, 2011, p. 12).

Essas condutas, na sua maior parte, ainda se encontram sem a devida regulamentação, de tal forma que o mundo virtual acaba por se transformar em um “mundo sem leis”. Ainda se utiliza muito as leis convencionais existentes para situações ocorridas em contextos virtuais, embora muitas vezes tais condutas necessitem de um tratamento especializado. É crítica, portanto, a necessidade de uma nova regulamentação para que haja uma maior segurança na utilização das ferramentas virtuais, de modo que as transações realizadas em contexto eletrônico tenham validade.

Com o atual avanço tecnológico, é perceptível o atraso existente entre as normas do código penal e o momento histórico no qual estamos vivendo, restando aos operadores do direito a árdua missão de conciliar os institutos penais com as constantes mudanças na tecnologia (PACHECO, 2011, p. 06). Apesar do surgimento de novas legislações, ainda assim

há um conjunto reduzido de normas que tipificam as condutas ilícitas cometidas através da tecnologia.

Existe uma ineficácia na normatização dos crimes virtuais em frente aos desafios que a sociedade informatizada apresenta. As Leis 12.735/2012 (BRASIL, 2002), 12.737/2012 (BRASIL, 2012), e 12.965/2014 (BRASIL, 2014), ainda não foram suficientes para um combate efetivo contra esses delitos. Uma dificuldade encontrada, até mesmo pela natureza taxativa do Código Penal brasileiro, é a impossibilidade da aplicação da analogia aos crimes virtuais.

Quando se trata de contratos virtuais, por exemplo, o Código Civil Brasileiro (BRASIL, 2002) e o Código de Defesa do Consumidor Brasileiro (BRASIL, 1990) ainda podem ser utilizados em parte para sanar alguns conflitos, mesmo com a falta de norma específica sobre o tema. Já em relação ao Direito Penal, deve-se criar uma legislação específica para tipificação dos delitos, caso contrário, na aplicação da analogia, haveria uma afronta a um direito fundamental.

Devido a falta de legislação específica para os crimes virtuais, ainda se utilizam as seguintes normas já tipificadas na legislação penal convencional: Pedofilia[1] (art. 241-A da Lei nº 8.069/90-Estatuto da Criança e do Adolescente); Interceptação de comunicações de informática[2] (art. 10 da Lei nº 9.296/96); Crimes contra software - "Pirataria"[3] (art. 12 da Lei nº 9.609/98), Calúnia[4] (art. 138 do Código Penal Brasileiro), Difamação[5] (art. 139 do Código Penal Brasileiro), Injúria[6] (art. 140 do Código Penal Brasileiro), Ameaça[7] (art. 147 do Código

1 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

2 Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

3 Art. 12. Violar direitos de autor de programa de computador:

§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:

4 Art. 138 – Caluniar alguém, imputando-lhe falsamente fato definido como crime:

5 Art. 139 – Difamar alguém, imputando-lhe fato ofensivo à sua reputação

6 Art. 140 – Injuriar alguém, ofendendo-lhe a dignidade ou o decoro

Penal Brasileiro), Furto[8] (art. 155 do Código Penal Brasileiro), Dano[9] (art. 163 do Código Penal Brasileiro), Apropriação indébita[10] (art. 168 do Código Penal Brasileiro), Estelionato[11] (art. 171 do Código Penal Brasileiro), Violação ao direito autoral[12] (art. 184 do Código Penal Brasileiro) (CARNEIRO, 2012, p. 01). Isso foi feito como uma tentativa inadequada de tentar adaptar leis elaboradas tendo em vista uma situação peculiar, para um contexto bem diferente, o que é o caso do cenário tecnológico atual.

Importante destacar que além das condutas descritas como crime, ainda existem alguns ilícitos que não são considerados crimes, e que também não apresentam legislação específica, a exemplo dos danos praticados contra as informações, a propagação de ameaças virtuais, etc. Isso dificulta ainda mais a punição de condutas que deveriam ser consideradas ilícitas pelo potencial danoso que apresentam, e não são tipificadas pelo atraso do Direito Penal.

Existem também normas específicas que tratam do assunto, estando estas longe de englobar tantas condutas cometidas por criminosos virtuais. Como exemplo de crime virtual tipificado, temos a conduta de invadir dispositivo informático alheio com a intenção de obter, mudar, ou destruir dados ou informações. Tal conduta está prevista no Art. 154 da Lei Carolina Dieckman (BRASIL, 2012), legislação essa criada com inspiração em um fato ocorrido com a atriz que da nome a essa lei e teve fotos íntimas divulgadas. Entretanto, tal lei, apesar de ser a primeira a tipificar um delito estritamente virtual, ainda não é suficiente para englobar o número de ilícitos que podem ser cometidos em ambiente cibernético.

As soluções legais devem buscar garantir a circulação das informações, com um mínimo de privacidade para os usuários, isso sem acabar com o acesso às informações, o que é um desafio não tão simples de ser superado. Tudo isso deve ser feito de modo a compatibilizar as facilidades proporcionadas através da utilização da Internet com os mecanismos de privacidade e respeito à esfera individual dos cidadãos.

---

8 Art. 155 – Subtrair, para si ou para outrem, coisa alheia móvel

9 Art. 163 – Destruir, inutilizar ou deteriorar coisa alheia

10 Art. 168 – Apropriar-se de coisa alheia móvel, de que tem a posse ou a detenção

11 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

12 Art. 184. Violar direitos de autor e os que lhe são conexos

Há a necessidade de regulamentação da internet, e dai que se vislumbra a importância do Marco Civil da internet (BRASIL, 2014). Tal lei funciona como uma espécie de constituição da Internet que contém alguns princípios que orientam o uso da internet no Brasil, além de procurar mecanismos que promovam o desenvolvimento da rede mundial de computadores.

Acontece que a falta de regulamentação da Internet no Brasil tem transferido a regulamentação para as decisões judiciais em casos concretos, o que é perigoso se considerarmos que a demora na decisão do judiciário pode fazer com que não seja mais possível resolver o processo em tempo hábil.

A Internet apresenta uma grande utilização no país, mas apesar disso pouco se fez até o momento em termos de legislação para se definir os equilíbrios de interesses que permeiam a rede. Essa ausência de legislação traz como consequência a insegurança quanto à projetos de inovação, devido a incerteza do que seria ilegal e ilegal. Com essa falta de regras acaba-se por transferir a decisão do conflito de interesses ao judiciário, sem dotar o mesmo de regras claras, o que pode gerar mais incerteza (LEMOS, 2006, p. 93).

3.2 Direito Comparado de Delitos Virtuais

Interessante realizar um estudo de direito comparado para verificarmos como os outros países vem tratando o fenômeno dos crimes cibernéticos, e o quanto ainda temos que avançar em relação às normas de combate a esse tipo de delito. O Brasil apresenta de fato um atraso a ser superado em termos de legislação específica quanto a esse assunto.

Isso é ainda mais crítico se observarmos que o país é um dos que mais cometem crimes virtuais. Estamos vivendo em um período no qual a inclusão digital está cada vez maior, e o atraso na criação das leis podem acabar por tornar o Brasil um ambiente propício para indivíduos que utilizam a Internet de forma antiética.

O modelo americano se baseia em um sistema de precedentes judiciários conhecido como *Commom Law*. Além disso, devido o sistema dos Estados Unidos ser federalista, cada estado cria o seu sistema de leis, o que faz ter muitas vezes normas bem diferentes umas das outras.

Após um episódio em 1988, no qual um jovem estudante da computação criou um programa com a intenção de demostrar falhas de sistemas, o que acabou criando uma proliferação de vírus e *worms*, os Estados Unidos iniciaram um trabalho de combate aos crimes cibernéticos, tanto a nível federal quanto estadual. A nível federal foi criada a Lei de Proteção aos Sistemas Computacionais (*Federal Computer System Act of* 1981), que buscava incriminar condutas de fraude, furto, e apropriação indébita utilizando computadores.

Em 1982, foi criada a lei que trata das transferências eletrônicas de fundos –Eletronics Funds Transfer Acts - que serve para inibir as fraudes informáticas que atrapalhassem essas transferências. Como principal norma existe a Lei de Fraude e Abuso Computacional (Computer fraud and Act), de 1986, que protege os sistemas de defesa de invasões com o intuito de obtenção de vantagens econômicas (SILVA, 2015).

Após a Segunda Guerra Mundial houve na Alemanha uma preocupação em criminalizar certos delitos que atentassem contra a economia, surgindo dessa forma as primeiras manifestações legislativas quanto às fraudes eletrônicas e outras condutas criminosas realizadas por meio dos computadores.

Em 1986, através da segunda lei de informática, criminalizou-se na Alemanha os delitos de espionagem de dados, extorsão informática, falsificação de elementos probatórios, alteração de dados, sabotagem informática, utilização abusiva de cheques e cartões de créditos (TORRE, 2015, p. 121).

Na Espanha houve alterações das figuras típicas do código penal com o intuito de coibir condutas *hacking*, acessos ilegítimos, e disseminação de códigos maliciosos. Já a França previu bem as condutas criminosas praticadas por computadores, tendo previsões acerca de acesso fraudulento de acesso aos sistemas de dados, sabotagem informática, destruição de dados, e falsificação de documentos informatizados.

Na Itália, através do Decreto nº 518/1992, houve a tutela do direito do autor através da tipificação dos delitos de sabotagem informática, crimes de invasão de domicílio, intrusão de sistema informático , crimes com a violação de segredos, atentados contra a inviolabilidade informática, crimes contra o patrimônio, e danos de sistemas de informática que tragam prejuízos financeiros.

A Inglaterra elaborou a lei Computer Misuse (Lei de Abusos de Informática), com o objetivo de criminalizar as condutas de alterar dados informáticos, impedir as operações de computador, impedir a execução de programas de computador, etc.

Na Argentina surgiram regulamentações penais com o intuito de proteger o comércio eletrônico. Já o Chile, através da lei 19.233/1993 foi o primeiro país da América Latina a regulamentar tal assunto, prevendo crimes de destruição de software e hardware, acesso ilegítimo à informação, e divulgação indevida de dados confidenciais (TORRE, 2015, p. 121-132).

Todos esses exemplos demonstram que os países vem se alertando acerca da necessidade de se prever condutas que atentem contra a segurança informática, condenando e reprimindo os atos ilícitos que ataquem os bem informáticos.

O Brasil também tem se conscientizado em relação a essa onda de crimes computacionais, e iniciativas legislativas têm sido realizadas. Essas iniciativas legislativas, apesar de insuficientes, não deixam de ser um passo importante para o combate a esse delito, até porque, ainda mais se tratando da esfera penal, não existe como combater ilícitos sem a devida previsão legal.

3.3 Leis específicas para Crimes Digitais

Interessante observar que como uma maneira de facilitar e até mesmo possibilitar as investigações dos delitos digitais foram realizadas iniciativas de leis nos estados de São Paulo, Rio de Janeiro, Mato Grosso do Sul, e Santa Catarina.

Tratam- se das leis dos Cyber cafés, normas essas que determinam a guarda dos registros de acesso dos usuários pelos estabelecimentos que permitiam a conexão à Internet. Na época da criação dessas leis, por volta dos anos de 2005 e 2006, houve uma certa polêmica, devido o recorrente argumento de censura e vigilância indevida, algo que não se sustenta diante dos riscos de segurança a serem minimizados.

Teve que ser feita uma escolha entre a liberdade irrestrita de acesso com possibilidades praticamente ilimitadas de anonimato, e a garantia de um possível rastreamento

de criminosos que se aproveitam dos recursos tecnológicos para prejudicarem a vidas das pessoas de forma mais confortável. Felizmente, a primeira opção está sendo a escolhida, mesmo que de forma bastante tímida.

Já a Lei nº 12.735/12 teve alguns pontos motivos de polêmica, principalmente devido à obrigatoriedade de guarda de registros de acesso dos usuários pelos provedores de Internet. Devido a esse problema esse projeto de lei foi esvaziado em relação ao seu conteúdo inicial, se tornando uma lei com poucas disposições.

O texto aprovado trata acerca da necessidade de criação de delegacias especializadas no combate aos crimes digitais, o que requer investimento tanto em treinamentos quanto em equipamentos para as polícias. No Estado do Ceará, por exemplo, já se cogita há algum tempo a criação de delegacias especializadas nessa modalidade de crime, mas nada na prática ainda foi realizado.

Além disso, no art. 5º da Lei nº 12.735/12 houve uma determinação de que se alterasse o dispositivo do art. 20, §3º, II, que prevê a conduta de prática, indução, discriminação , ou preconceito de raça, cor, etnia, religião, ou procedência nacional, praticados por meio de comunicação social ou publicação de qualquer natureza, de tal forma que as respectivas transmissões radiofônicas, televisivas, eletrônicas sejam cessadas.

A lei quer com isso dar celeridade à retirada do conteúdo difamatório do acesso público. Interessante observar que tal lei já é uma clara demonstração da impossibilidade de proteção da nova classe de bens jurídicos através de uma legislação de 1940, o que é o caso do Código Penal Brasileiro.

A Lei 11.829/2008 (BRASIL, 2008) teve o mérito de alterar o Estatuto da Criança e Adolescente (BRASIL, 1990) e inserir normas que punissem crimes informáticos relacionados com a produção, venda, e distribuição da pornografia infantil, sendo mais abrangente ainda e criminalizando a posse desse material e outras condutas relacionadas à pedofilia.

Essa lei inclusive engloba as situações em que não há um ato sexual propriamente dito envolvendo criança e adolescente, mas uma mera simulação. Tudo isso é feito para proteger a imagem desses jovens, além de ser uma boa tipificação de crime propriamente virtual. Apesar de atualmente a sociedade passar por polêmicas envolvendo situações de pedofilia, a

tendência mundial continua sendo a de defender a criança e o adolescente desse tipo de abuso, o que é o procedimento mais acertado.

3.4 Lei Carolina Dieckmann

Em 2012 foi sancionada a Lei nº 12.735/12, popularmente conhecida como Lei Carolina Dieckmann. Essa norma recebeu essa denominação devido a um fato criminoso envolvendo essa famosa atriz através de uma violação de dados a nível computacional. Carolina teve o seu computador invadido por crackers, tipo de especialistas em sistemas de computação que apresentam profundas habilidades e conhecimentos em relação a tal ramo, se diferenciando dos demais hackers pelo seu uso direcionado de forma antiética.

Esses invasores divulgaram na Internet alguma imagens pessoais da mesma devido o fato da atriz não ter aceitado entregar a esses indivíduos a quantia de R$10.000,00 para que as imagens não fossem divulgadas. Tal fato, além da interceptação de e-mail, configurou o crime de extorsão.

Com essa lei foi incorporado ao art. 154 do código penal a previsão de crime de invasão de dispositivo alheio, sem motivo ou sem o consentimento do dono, com penalidade de 3 meses a um ano, e com causa de aumento, caso tal invasão cause prejuízos econômicos à vítima, ou caso se trate da administração pública no polo passivo.

Tal norma, apesar de dever ser considerado um avanço, ainda mais se considerarmos a inexistência de tal previsão acerca da invasão de dispositivo informático, ainda é muito modesta. Basta se verificar a potencialidade danosa de uma invasão de um dispositivo computacional que contenha dados íntimos de alguma pessoa.

Não é incomum o cometimento de suicídios motivados por uma divulgação indevida de dados pessoais, o que fragiliza a vítima de tal forma, que o dano possa ser considerado irreparável. Há uma certa limitação quanto à proteção da imagem e da honra das pessoas através do direito penal, e isso fica mais evidenciado, ainda hoje, com a potencialidade da calúnia e difamação através de meios informáticos.

Um ponto que merece críticas é o fato de a lei ter criminalizado apenas a invasão para obtenção de vantagem ilícita, não abrangendo dessa forma o caso de um criminoso que queira apenas ver informações da pessoa, mesmo sem o intuito de obtenção de nenhuma vantagem direta (TAVARES, 2013, p. 07). O que dizer então da conduta de um indivíduo que acessa a conta pessoal de alguma rede social de um indivíduo que esqueceu sua conta aberta? Como não houve a violação indevida do mecanismo de segurança, a conduta seria atípica, o que nos leva a criticar a generalidade de tal dispositivo.

Outro ponto importante a ser destacado é a força do "quarto poder" na determinação dos rumos do país. A influência midiática foi de certa forma tão decisiva para aprovação da lei Carolina Dieckmann, que nos deixa a sensação de que a vida particular de um indivíduo famoso seja mais importante que a segurança da informação contida em sites do governo, muitas vezes com informações críticas que afetem vários brasileiros. O Brasil tem a tendência de se mobilizar legalmente para criação de leis quando acontecem fatos de grande repercussão, a exemplo do caso do assassínio da atriz Daniela Perez, e não foi diferente em relação à lei inspirada em Carolina.

3.5 Marco Civil da Internet

O Marco Civil da Internet, Lei 12.965/2014, é um importante mecanismo para o combate aos crimes digitais, embora pela nomenclatura da norma tenha se destacado mais o seu aspecto cível. Essa norma é um auxílio para a investigação dos crimes virtuais, e procura através da previsão de princípios e garantias tornar a Internet um ambiente menos hostil. Tal lei busca manter o equilíbrio entre a liberdade de expressão e transmissão do conhecimento com previsões de segurança como a responsabilidade civil dos provedores e usuários.

O Marco civil se assenta em três pilares, a saber: a garantia da neutralidade da rede, a proteção à privacidade do usuário da Internet, e a garantia da liberdade de expressão. A neutralidade da Rede busca garantir que as operadoras não cobrem de forma diferenciada a depender do conteúdo que circula na rede, podendo a mesma cobrar apenas em relação às velocidades oferecidas. Tal mecanismo procura oferecer uma democratização do acesso à Internet.

Quanto à privacidade do usuário a lei procura proteger os dados dos usuário junto aos provedores, de modo que apenas em ocasiões especiais possa haver quebra do sigilo desses dados. Já a liberdade de expressão tem a intenção de impedir a censura (LISBOA, LOPES, p. 83). Lógico que devemos salientar que não existem direitos absolutos, e que em casos específicos um direito pode ser relativizado, tendo inclusive previsões constitucionais a esse respeito.

A regulamentação do marco civil foi vantajosa porque houve o estabelecimento de prazos mínimos para a guarda de registros de acesso e conexão, além da obrigatoriedade de observância da lei brasileira para atos realizados no território nacional.

Por outro lado, a impressão que fica é que o marco civil tenta defender as pessoas das ameaças às liberdades e à vida privada quando praticadas pelo Estado, o que justifica a necessidade de ordem judicial para obtenção de registros de acesso. É como se o Estado fosse o maior interessado em violar a privacidade das pessoas. Acontece que tal ordem judicial acaba por gerar mais burocracia e retardar uma investigação até por meses (BERGMANN, 2016, p. 47).

Deve-se observar que a obtenção de dados de registro é essencial até mesmo para a definição dos melhores rumos de uma investigação, e atrasos desnecessários são mais um fator que dificulta a identificação do criminoso, que normalmente já se encontra passos a frente das forças policiais.

O Brasil precisa urgentemente criar uma legislação específica para crimes cibernéticos, ainda mais se considerarmos que a internet hoje é indispensável para a sociedade. Assim, Se faz necessário no ordenamento jurídico brasileiro uma maior tipificação de condutas criminosas praticadas pela internet. O Estado brasileiro ainda está bastante atrasado no aspecto jurídico, e há a necessidade de uma legislação específica para os delitos virtuais, de modo a evitar que país seja um paraíso para esse tipo de criminoso.

3.6 – Investigação de Crimes Cibernéticos

Uma vez elaborada a legislação penal, há a necessidade de mecanismos para que a lei seja de fato cumprida pela sociedade, e dai a importância do trabalho da polícia, do

Ministério Público e do Judiciário. A investigação criminal é um dos processos mais importantes para apuração de denúncias ou queixas-crime:

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

Apesar de na doutrina o Inquérito policial ser considerado como mero procedimento administrativo prescindível, inegável é a sua utilização de forma a evitar julgamentos equivocados e ações desnecessárias. Embora muitas vezes o Ministério Público e o Judiciário afirmem que pode-se inclusive dispensar o inquérito, temos que observar que as provas necessárias para o bom andamento de uma ação penal não se encontram no fórum e sim no mundo real, tendo que haver portanto pessoas qualificadas para a busca dessas informações.

A polícia tem como função primordial, através de sua atividade delineada pelo Código de Processo Penal Brasileiro (BRASIL, 1941), realizar os trabalhos de apuração dos casos concretos, de modo a embasar as denúncias e as queixas a serem promovidas pelo Ministério Público ou demais querelantes.

Cabe à polícia, portanto, ao tomar conhecimento de algum fato criminoso, realizar diligências como: comparecer ao local do crime; realizar busca e apreensão de armas, instrumentos, e outros objetos relacionados ao crime; ouvir pessoas envolvidas e testemunhas; requisitar os exames periciais necessários ao entendimento da dinâmica criminal, e praticar todos os atos essenciais para o esclarecimento dos fatos e identificação do autor do crime (COBRA, 1969, p. 19).

O legislador brasileiro diferenciou o Inquérito Policial de qualquer outro procedimento administrativo, o normatizando no Código de Processo Penal Brasileiro, procurando delimitar o campo de atuação da polícia judiciária e do Ministério Público com o intuito de garantir ao cidadão a quem se acusa de alguma infração penal o direito de ser investigado por uma organização estatal predefinida. Isso é importante pois é um argumento de maior imparcialidade, visto que a autoridade policial não fará parte de uma futura ação penal (SOUZA, CABRAL, 2013, p. 29).

A Constituição Federal Brasileira (BRASIL, 1988) trata de atribuir as funções investigativas às policias civis dos Estados, e à Polícia Federal. Tais atribuições são essenciais pois a própria lei maior trata de reconhecer a necessidade de um tratamento especial às investigações criminais ao expor a necessidade de polícias especializadas em investigação criminal, a diferenciando das polícias ostensivas (Polícia Militar).

A Lei nº 10.446/02 (BRASIL, 2002) regulamentou o art. 144, parágrafo 1º, I, ao dispor que a Polícia Federal atuaria também como "polícia judiciária nacional", uma vez que os delitos citados abstratamente no referido diploma legal seriam primeiramente atribuição das polícias civis.

A nível federal, portanto, as investigações cabem à polícia federal, instituição essa que ainda consegue demonstrar o quanto de resultado pode ser alcançado com a valorização devida da função investigativa. Há uma melhor estrutura se comparada às polícias dos estados, e há um maior número de policiais especializados e com conhecimentos práticos na investigação de crimes cibernéticos, algo que se pode observar inclusive pelo número de publicações desses profissionais.

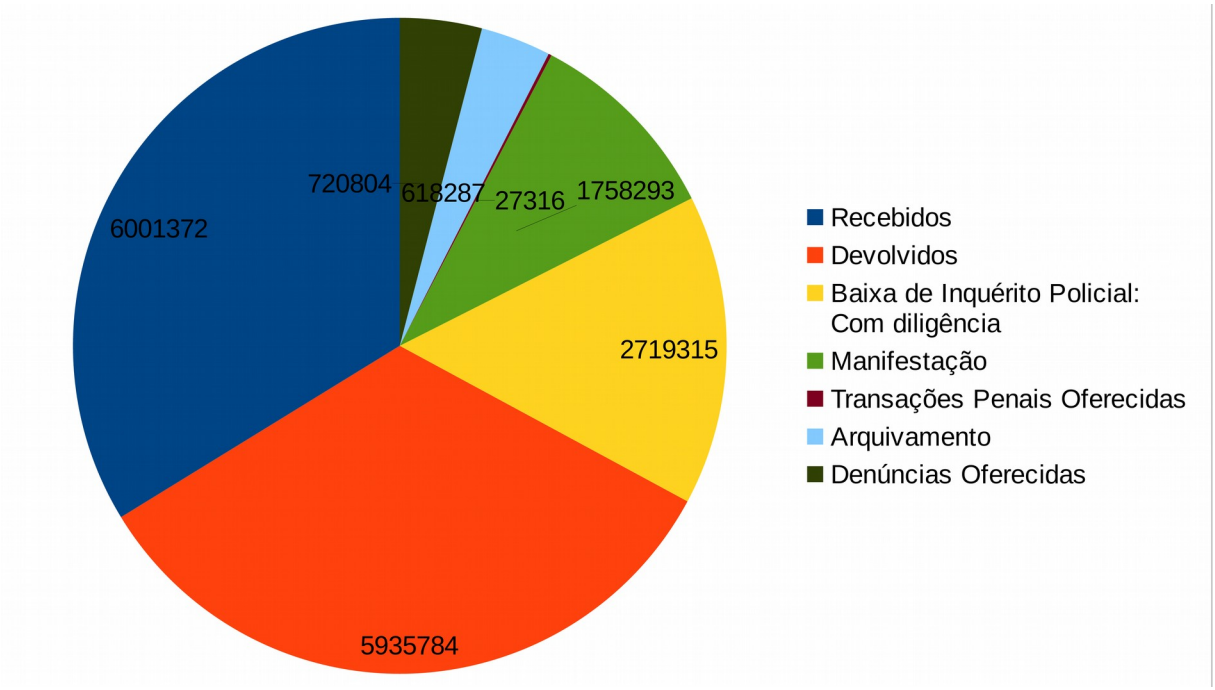
Verificado a quem incumbe precipuamente o andamento das investigações criminais, no caso às Polícias investigativas (Federal ou civis), temos a necessidade de responder a seguinte pergunta: Essas polícias realmente são estruturadas para responder a uma demanda de crescimento criminal cada vez mais diversificado? O quão atualizado é a atual estrutura policial para fazer frente a esse novo cenário de crimes cometidos por intermédio das mais avançadas tecnologias ?

A Polícia Federal apresenta maiores recursos financeiros que as policias civis dos estados, além de ser uma referência quanto à investigação de crimes virtuais. A Polícia civil apresenta a desvantagem de ter que disputar recursos com as polícias militares, o que dificulta o seu trabalho principal, visto a preferência dos governos em um modelo de polícia que além de oferecer uma maior visibilidade, pode ser controlado com mais facilidade.

Praticamente não há a possibilidade de melhores resultados na redução da criminalidade sem o investimento nas polícias investigativas, pois é a instituição que tem a condição de fornecer subsídios para que o judiciário faça uma sentença completa, de modo a eliminar situações de *in dubio pro reo*, que acabem por favorecer os delinquentes.

Como podemos observar no gráfico a seguir o número de inquéritos que são transformados em processos penais representam uma porcentagem bastante pequena. Isso se

explica na maioria dos casos pela falta de aparato da polícia judiciária para resolução dos crimes, o que acaba fazendo que boa parte dos inquéritos sejam arquivados pela inexistência de autoria.



Desenho 1: Fonte: Conselho Nacional do Ministério Público

Desenho : Gráfico CNMP

A falência da polícia judiciária é consequência de uma política que valoriza mais a polícia ostensiva do que a investigativa. Percebe-se que as policias civis de todos os estados do país enfrentam problemas com a falta de estrutura, o que é lamentável visto a investigação ser a chave para o combate ao crime organizado.

Ao que tudo indica não é muito interessante para os governos investirem em uma polícia de inteligência, preferindo muitas vezes apostar em um marketing proporcionado pela imagem das polícias ostensivas. Falha-se em não dar maiores recursos a uma polícia que realmente ofereça resultados práticos na redução da criminalidade. Conforme palavras do ilustre professor Cândido de Albuquerque (2014):

> Ao que parece, sem ação efetiva e competente da Polícia Civil, que é a que investiga e que incomoda o criminoso, tornando sua vida um tormento e coletando provas para fundamentar as condenações judiciais, não se faz segurança pública. No Ceará, de fato, a Polícia Civil, até pelo contingente inexpressivo, e pelo mau gerenciamento e péssimas condições de trabalho, representa carta de alforria para os assaltantes,

> nosso maior temor. Com efeito, livrado o flagrante, o que quase sempre ocorre, basta ao ladrão, após meia hora, mudar de bairro ou de esquina e ficar livre para cometer novos crimes impunemente. Não se deseja negar a importância da PM – invenção brasileira, diga-se – mas sim combater o erro antigo e inaceitável da falta de priorização da reestruturação da Polícia Civil, como unidade responsável pelas investigações e, portanto, pela coleta das provas que permitirão o julgamento, pelas vias legais. Em todos os países o combate à violência urbana se deu com a atuação da Polícia Cívil (Judiciária).

As polícias civis brasileiras vêm enfrentando dificuldades para atuar no seu mister junto à população, e tudo isso tem uma razão histórica. Acontece que existe um certo trauma gerado pelo regime político ditatorial repressivo pelo qual o país passou há poucos anos.

Deve-se recordar que o regime democrático no Brasil ainda é muito recente, o que faz com que muitas pessoas ainda temam um novo golpe militar. Um dos fatores que ajudam a manter um governo no poder é a força das suas polícias militarizadas, e isso deve estar relacionado com os maiores investimentos nesse tipo de polícia.

Por outro lado, como se pode inferir do grande número de denúncias de corrupção recentes, não parece interessante para as grandes forças políticas investir em uma polícia que pode muito bem se voltar contra ela, utilizando inclusive instrumentos avançados de investigação. Seria como um “tiro no pé”. Existe tanto um abandono material quanto uma ingerência do poder executivo em relação à polícia civil, o que logicamente atrapalha o bom desempenho da instituição (CAVALCANTI, 2009, p. 109).

A falta de investimento e de verba na polícia investigativa vem mostrando as suas consequências com o baixo índice de resolução criminal. Há uma carência enorme de pessoal, pouca renovação do quadro, treinamentos obsoletos que geram práticas de atuação ineficazes. Percebe-se que há um processo no qual os requisitos para entrar na polícia civil de quase todos os estados seja o nível superior, embora tal exigência para ingresso não tenha repercussão em maiores salários, o que não faz sentido em uma função técnica e de risco como essa.

Há também um quadro no qual grande parte dos funcionários estão alocados em atividades que fogem das suas atribuições primordiais, exercendo papel de motoristas, digitadores, telefonistas, e vigias de delegacia. No estado do Ceará já virou moda o fenômeno de presos em delegacias, o que faz com que boa parte dos investigadores sejam forçados a exercer a atividade do agente penitenciário, Entra governo, sai governo, e a

situação não se altera. De acordo com o professor Daniel Maia (2017) a solução para o combate à criminalidade é a mudança desse paradigma:

> Nota-se que a velha política de segurança pública de tentar combater o crime com medidas clássicas, tais como o aumento do número de policiais militares, não funciona mais. O crime há muito tempo se organizou e, se o Estado não investir com inteligência na inteligência da polícia investigativa para que os criminosos sejam identificados e levados à justiça, de nada vai adiantar aumentar o efetivo da Polícia Militar nas ruas. Isso por uma razão muito simples: é impossível que tenhamos policiais em todos os lugares e também os criminosos não querem conflitos diretos com o aparato de segurança do Estado. Os criminosos atuam onde a polícia não está, pois sabem que, de fato, não serão investigados, ou seja, se não forem presos em flagrante, não serão depois. Isso gera para a população um sentimento de impunidade e desestímulo até em noticiar os crimes que sofre, pois do que vai adiantar perder horas em uma delegacia a espera da realização de um B.O. se aquele crime não será investigado? Gera ainda um efeito contrário para o criminoso, o qual passa a se sentir estimulado a cometer novos crimes.

Na estrutura da polícia civil faltam carros descaracterizados, para as investigações nas quais os policiais não querem e não devem chamar a atenção, faltam verbas para viagens e horas extras, muitas vezes necessárias, pois o crime não se compatibiliza sempre com o horário de trabalho da corporação.

Até mesmo o sistema de informação policial ainda é muito falho, não tendo a interligação necessária com outros sistemas importantes, além de não apresentar uma boa base de dados que facilite a investigação. Aqui, diferentemente de países com os Estados Unidos, percebe-se a pouca valorização da atividade policial, algo que pode ser percebido claramente pela relação da imprensa e da própria população em relação aos seus defensores.

Quando um policial morre em serviço nos EUA há realmente um clamor popular. Aqui, a morte de um policial, além de já ter virado rotina, não tem a mesma repercussão que a de um criminoso defendido pelos direitos humanos. Tudo isso tem um efeito na moral e na energia das polícias do país, que percebem o quanto são dispensáveis pela maioria da população. Dificilmente alguém sem o devido reconhecimento vai oferecer o seu melhor, e quem mais sai perdendo com tal situação é a própria população.

Nas investigações de crimes cibernéticos podemos identificar uma fase técnica e uma fase de campo (WENDT, JORGE, p. 52). Na fase técnica se enfatiza um conjunto de atividades e técnicas importantes para a identificação do computador do criminoso.

Ao iniciar a fase técnica um aspecto importante é a compreensão do fato ocorrido e análise das informações fornecidas pelas vítimas. Nessa abordagem inicial deve-se procurar

utilizar técnicas de interrogatório de modo a realizar uma filtragem de informações com o intuito de selecionar aquelas que sejam imprescindíveis para o bom andamento da investigação. Conhecimentos de psicologia e linguagem corporal podem ser bastante úteis para verificar até que ponto se pode confiar nas afirmações realizadas pela vítima.

Muitas vezes as vítimas, devido a constrangimentos gerados pelo fato criminoso, tomam atitudes precipitadas de forma a colocar em risco o corpo de delito, que é todo objeto e software relacionado ao crime, tornando complicado o trabalho da perícia. A segurança virtual da vítima pode inclusive ser ainda mais ameaçada devido a atitudes descuidadas realizadas pela própria mesmo após o início das investigações. Faz-se essencial uma orientação à vítima acerca de procedimentos e cuidados a serem tomados com o intuito de colaborar com a investigação ou pelo menos não dificultá-la.

Sobre a investigação policial e a posterior confecção do laudo pericial, o sucesso das provas obtidas depende da capacitação do investigador e do perito, de tal modo que os mesmos tenham aptidão para manusear as tecnologias modernas para a busca dos indícios (MALAQUIAS, 2012, p. 55). Quanto antes for realizada a coleta de provas em ambiente cibernético, mais possibilidades de se encontrar vestígios que levem a busca da verdade acerca do fato a ser investigado, tornando o trabalho da perícia bastante confiável na apreciação das circunstâncias relacionadas ao fato criminoso e na indicação do provável autor do ilícito.

Algo que não pode ser esquecido é a formalização da denúncia através do registro de boletim de ocorrência. Algo que tem acontecido, não somente em relação aos crimes cibernéticos, mas em relação aos crimes em geral, é a falta de ciência e cobrança das vítimas, que muitas vezes por motivo de constrangimento, não relatam o fato ocorrido à polícia, o que acaba trazendo prejuízos a uma política criminal mais sofisticada.

A possibilidade de uma pressão para que se crie uma legislação mais abrangente em relação aos crimes cibernéticos seria muito grande caso houvesse uma maior exigência da população, formalizada através de boletins registrados nas delegacias.

Ao se realizar a investigação na internet acerca de prováveis autores, origem de e-mails, registros e hospedagens de domínios deve-se ficar atento às técnicas empregadas por criminosos experientes no uso de estratégias que dificultam sua detecção. Uso de mascaramento de endereços IP e ataques remotos são técnicas que podem levar a caminhos

errados na investigação. O investigador deve ter um certo conhecimento para entender as possibilidades de “camuflagem” oferecidas pelas tecnologias digitais.

Na hora de se confeccionar o relatório das provas apuradas deve-se ficar atento em não se esquecer de detalhes que podem ser aspectos chaves para o bom andamento das investigações. Esses detalhes servem para que através de metodologias dedutivas, indutivas ou de raciocínio analógico seja possível ter êxito nas buscas.

O modus operandi é a maneira ou o conjunto de procedimentos efetuados por um criminoso que funciona como uma espécie de assinatura. A análise desse *modus operandi* pode ser a chave para o sucesso de investigações que envolvem certos grupos de *hackers* que utilizam técnicas bastante sofisticadas, o que os tornam bastante difíceis de capturar.

A Constituição Federal brasileira oferece sigilo de dados, o qual só pode ser quebrado através de autorização judicial. Essa autorização é essencial, pois sem ela se correria o risco de contaminar as provas judiciais obtidas através de meio ilícito, dificultando o andamento da ação penal, gerando inclusive a possibilidade de punição por quebra desse sigilo. De posse dessa autorização, pode-se obter informações de provedores de conexão e de conteúdo de modo a obter indícios da provável localização do criminoso.

Basicamente a fase técnica pode ser dividida nos seguintes passos: Compreensão do fato ocorrido e análise das informações fornecidas pelas vítimas; Orientação à vítima com a finalidade de proteger o corpo de delito e sua segurança virtual; Coleta inicial das provas em ambiente cibernético; Formalização do crime através do registro de boletim de ocorrência; Investigação na internet acerca de prováveis autores, origem de e-mails, registros e hospedagem de domínios; Confecção de relatório das provas apuradas; Representação perante o poder judiciário para expedição de autorização judicial para quebra de dados; Análise das informações prestadas por provedores de conexão e provedores de conteúdo.

Na fase técnica pode ser necessário diversas interações junto aos provedores de dados ou mesmo várias solicitações judiciais de modo a obter maiores informações úteis ao deslinde do processo investigatório.

Os registros relativos às conexões aos servidores da internet contem dados que auxiliam na identificação da origem de qualquer transação na rede (BLATT, 2016, p. 83). Quando um computador ou outro dispositivo se conecta a internet a ele é atribuído um endereço IP exclusivo.

Desse modo evita-se a existência de dois usuários utilizando o mesmo IP durante a mesma navegação, de modo que no mesmo dia e hora e fuso horário, independentemente do IP ser estático ou dinâmico, não haja repetição de IP. Isso é o que vai permitir o rastreamento do criminoso, e dai a importância da guarda desses registros.

A partir da identificação e localização do computador que está sendo usado para a prática do ato delituoso, inicia-se a fase de campo, através da qual uma equipe de agentes policiais realiza diligências com o intuito de reconhecerem o local do crime, que deve ser preservado de modo a obedecer a uma cadeia de custódia, que é um conjunto de procedimentos que visam a garantir a confiabilidade das provas técnicas devido a procedimentos padronizados de coleta e guarda de vestígios.

Durante a fase de campo deve-se atentar acerca da necessidade de se pedir um mandado de busca e apreensão para a busca de materiais comprobatórios no local, de modo a agir com respeito a legalidade, evitando-se invalidar as provas obtidas por meios ilícitos. Há a possibilidade de haver um possível gargalo e atraso na obtenção desse mandado judicial, o que prejudica sobremaneira a investigação.

Em algumas situações pode ser necessária a solicitação ao poder judiciário, no caso de redes corporativas, para que haja uma determinação dirigida ao administrador da rede de um determinado local, de forma que o mesmo forneça informações técnicas que ajudem a identificar a máquina de onde partiu o acesso.

Essa determinação pode ser enviada diretamente ao administrador de rede, ou entregue pessoalmente pelo oficial de justiça ou por autoridade policial. Recomenda-se a participação de um perito computacional oficial no acompanhamento do processo, e na falta deste um profissional da área designado pela autoridade policial.

Existe uma cobrança enorme para a elucidação de crimes até mesmo pela forte sensação de impunidade. Apesar disso devemos levar em consideração que por mais difícil que seja a investigação de crimes virtuais o Estado não pode se privar de esgotar todas as possibilidades para elucidação desse tipo de delito.

No caso da investigação criminal exercido pelas polícias judiciárias afirma Ribeiro (2006), “O trabalho da polícia é como o do médico. Este não é obrigado a todo custo a salvar o paciente, mas dispensar-lhe o melhor atendimento médico possível. Isso também se aplica, com toda certeza, ao trabalho prestado pela polícia investigativa”.

Apesar de certo atraso, há uma tendência para que as polícias brasileiras criem divisões especializadas no combate aos crimes cibernéticos, de tal forma que reunindo especialistas no assunto seja possível inibir com maior eficiência a ocorrência desse tipo de delito.

Já existem delegacias no Sul e Sudeste do país focado na investigação de cibercrimes. Há um tempo que se fala da necessidade de criação de uma divisão de cibernéticos no estado do Ceará, entretanto ainda não houve movimentação mais concreta a esse respeito. Enquanto isso, a maioria da população continua sofrendo com a falta de aparato investigativo para o combate a tais crimes.

3.7 Perícia Computacional

Conforme foi discorrido durante esse trabalho, a evolução tecnológica e o advento da internet propiciou um ambiente repleto de facilidades às pessoas, como compra de mercadorias online, transações bancárias, envio e recebimento de mensagens eletrônicas, entre outras.

Entretanto a questão da segurança se mostrou fragilizada nesse ambiente, onde as mentes criminosas vislumbram um grande potencial para a prática dos crimes devido à sensação de impunidade. Na busca de combater esse cenário de crescimento de crimes cibernéticos, a investigação criminal vem se desenvolvendo em sintonia com a perícia criminal, o que não poderia acontecer de outra forma por estarmos tratando de um tipo de delito que para ser julgado necessita de provas obtidas por meios bastante específicos para o melhor convencimento da justiça.

No começo da fase técnico-científica da investigação criminal, a partir do século XIX, cabia à disciplina da Medicina Legal os exames de integridade física do corpo humano, além da pesquisa e demonstração de outros elementos relacionados com a materialidade do crime, como exame dos instrumentos e demais evidências exteriores ao corpo humano.

A perícia forense no Brasil, seguindo o exemplo dos países europeus, também teve início a partir da Medicina Legal. A nacionalização da perícia ocorreu em 1860 com o primeiro curso de prática tanatológica no Brasil, realizado no Rio de Janeiro, onde Raimundo Nina Rodrigues deu início a estudos de Medicina Legal a partir da ótica brasileira.

Em 1832, o Código Criminal do império estabeleceu a perícia oficial como responsável pela realização dos exames de corpo delito em todo Brasil, e dai a Medicina Legal passou a fazer parte do currículo da maioria das faculdades de Direito do país.

Com a regulamentação da atividade médico pericial em 1854, através do Decreto nº 1.740, foi criada a assessoria médico legal como auxiliar da secretária de polícia da corte, fazendo tal organização além do exame de corpo delito, outros exames necessários para o esclarecimento dos crimes.

Ocorreu o advento e desenvolvimento de outras disciplinas científicas como a Física, Química, Biologia, Matemática, entre outras, a polícia começou a utilizar cada vez mais tais conhecimentos para o desvendamento dos crimes. Assim, como uma Ciência de apoio à polícia e à justiça surgiu uma Ciência independente em sua ação, embora munida de conhecimentos obtidos por outras disciplinas científicas, denominada Criminalística.

Essa disciplina inclusive já apresentou as mais variadas denominações como: antropologia criminal, psicologia criminal, polícia técnica, policiologia, polícia criminal, técnica policial, polícia judiciária, criminalística, e polícia científica (MAIA, 2007 , p. 03). O termo criminalística foi criado pelo professor de Direito Penal e juiz de instrução Hans Gross, em 1893, na Alemanha ao escrever o livro sistema de criminalística, manual do juiz de instrução. Eraldo Rabelo define criminalística como:

> Disciplina autônoma, integrada pelos diferentes ramos do conhecimento técnico-científico, auxiliar e informativa das atividades policiais e judiciárias de investigação criminal, tendo por objeto de estudo dos vestígios materiais extrínsecos à pessoa física, no que tiver de útil à elucidação e à prova das infrações penais, e ainda, a identificação dos autores respectivos (RABELO, 1996, p. 20).

Não há como presidir um Inquérito Policial sem o conhecimento dos princípios da Criminalística. Não é possível que o responsável pelo Inquérito Policial, o delegado de polícia, possa dar andamento a uma investigação de forma produtiva sem conhecer os procedimentos desse campo de estudos no contexto em que trabalha. Há que se ter uma base. O delegado precisa saber, por exemplo, o que precisa ser feito, até mesmo para saber quais tipos de exames deve requisitar, além de ter uma boa noção de quais quesitos sejam essenciais.

Logicamente, o chefe do inquérito não precisa dominar os métodos e técnicas periciais, no entanto uma base mínima é importante para que o mesmo tenha uma noção da

dinâmica do fato, e possa inclusive enquadrar o indivíduo da forma mais completa no tipo penal correlato (REIS, 2013, online).

Há que se entender a relação entre as provas e as normas do código penal e de processo penal para que se tenha inclusive uma noção da importância dessa prova e o quanto ela pode influenciar na convicção do juiz. Embora a Código de processo penal propague o princípio da livre convicção do magistrado, logicamente que quanto mais uma prova indique um fato de tal modo a diminuir as resistências à sua contestação, mais óbvias e menos subjetivas são as conclusões do magistrado:

> Nesse sentido, a produção de provas passa ser requisito básico e insubstituível para a própria realização do direito material. E impõe-se que as provas sejam claras, seguras, e aptas a transmitir a necessária confiança ao julgador, de modo que, livre de qualquer dúvida, este possa firmar a convicção racional da existência do fato criminoso e de sua autoria, pois, em sentido inverso, restringindo-se o conjunto probatório aos limites da verdade provável, forçosamente inviabiliza-se a aplicação da pena, restando apenas a solução da ação penal com base no in dubio pro reo (BARROS, 2002, p. 113).

No início de sua estruturação, a Criminalística utilizava profissionais de formação genérica. Entretanto, em face da evolução tecnológica e devido alguns crimes terem passado a serem executados com uma maior complexidade e sofisticação, passou a ser necessário a colaboração de profissionais com especializações para fazer frente às necessidades de conhecimento importantes para o bom andamento das investigações criminais.

No caso da perícia envolvendo dispositivos computacionais, por exemplo, podemos verificar que a própria Ciência da Computação é uma área que abrange diversas disciplinas com uma gama vasta de conhecimentos como Banco de Dados, Sistemas Operacionais, Redes, Segurança da Informação, etc.

O termo Criminalística está relacionado ao meio policial, e até pouco tempo as ciências computacionais não tinham relação com tal ciência, a exemplo da balística forense, toxicologia forense, medicina legal, documentoscopia, química forense, entre outras.

Devido ao aumento do uso do computador e da Internet, houve o surgimento de uma nova espécie de delitos que utilizam as facilidades da informática o cometimento de crimes. Muitas vezes tais infratores são pessoas de conduta íntegra no mundo real, e se aproveitam do anonimato proporcionado pelo mundo virtual para o cometimento das mais variadas afrontas às outras pessoas. Com a evolução tecnológica e o surgimento dos primeiros casos

envolvendo o meios computacionais foi necessária a criação de uma nova disciplina forense: A Ciência Forense Computacional (OLIVEIRA, 2001, p. 02).

A Perícia Digital é um exame técnico realizado por especialista em dados armazenados em mídias no formato digital, tendo o perito que analisar questões relacionadas ao hardware e ao software de equipamentos digitais como computadores, aparelhos celulares, fax, tablets, entre outros:

> A Perícia Digital utiliza um conjunto de técnicas e procedimentos com embasamento científico para coletar, analisar, e apresentar as evidências encontradas. Tem o objetivo de buscar informações relativas a eventos passados em uma investigação (não apenas criminal ou cível, mas também em casos particulares nos quais não se deseja acionar a polícia ou a justiça, em um primeiro momento. A partir da análise dos eventos ocorridos é possível reconstruir as ações executados nos diversos equipamentos e mídias questionados (VECCHIA, 2014, p. 77).

Deve-se observar que na perícia digital os vestígios encontrados constituem-se na sua maioria de forma indireta, o que significa que no caso de um computador estiver como suspeito de ter sido utilizado para a prática de algum delito, qualquer programa ou arquivo irá dar uma indicação de tal fato indiretamente, ao contrário de um crime fora do sistema computacional, onde um vestígio precisa apenas ser interpretado, como um restante de pêlo encontrado sob a unha de uma vítima de homicídio que leva a supor uma luta anterior com um agressor.

Devido a isso, exige-se além do conhecimento técnico dos profissionais que trabalham na área computacional, um raciocínio lógico coerente, pois a análise pericial em um computador é algo muitas vezes de difícil execução, a depender da complexidade do sistema operacional sob análise. Uma vez verificada a necessidade da perícia para a investigação desse tipo de crime, resta a pergunta de o quanto as estruturas do país estão preparadas para lidar com essa crescente onda de criminalidade virtual?

Em quase todos os ordenamentos jurídicos existe um consenso de que quando ocorre um fato criminoso, deve haver a presença no local da ocorrência de uma equipe contendo perito, investigadores, e polícia ostensiva. O que ocorre na realidade é a ausência desses profissionais em um primeiro momento, fato esse causado pelo baixíssimo efetivo desses profissionais.

Espanta verificar o número de laudos atrasados presente em nas organizações periciais, algo que atrapalha e muito o andamento de qualquer investigação criminal. Some-

se a isso a constante violação dos locais de crime, fato esse causado pela falta de conhecimento e técnicas das forças de segurança pública, e de cultura da população quanto à importância de tal preservação, algo que muitas vezes coloca em xeque a credibilidade dos procedimentos periciais realizados (AYRES, 2015, p. 40).

Há no país um movimento de autonomia das polícias em relação às forças policiais. Isso ocorre com a justificativa de se afastar os órgãos periciais de uma imagem estritamente policial. Alegam como vantagem o afastamento da noção de suspeição da população em relação aos serviços periciais. Além disso, a questão da autonomia orçamentária e técnica é decisiva para essa desvinculação. A Perícia Forense do estado do Ceará, por exemplo, é desvinculada da polícia civil, embora ainda seja vinculada à Secretária de Segurança Pública e Defesa Social do Ceará.

De fato observa-se que as atividades de polícia judiciária são diversas das da perícia criminal. Enquanto o trabalho da polícia investigativa apresentam uma organização mais rígida, com especial atenção às provas testemunhais e subjetivas, a perícia criminal deve recorrer a uma metodologia científica aplicada à análise dos vestígios encontrados, ainda que existam discrepâncias entre essas provas e as do inquérito policial.

O art. 2º da Lei 12.030 (BRASIL, 2009) procura garantir ao perito criminal uma autonomia para o exercício de suas atividades com liberdade científica, para que não se corra o risco de seu trabalho ser afetado negativamente pela relação com as instituições policiais, principalmente pela desconfiança de que a prova pericial possa ter sido manipulada para estar de acordo com a acusação (SILVEIRA, 2015, p. 23).

Por outro lado, há quem acredite que tal desvinculação possa atrasar ainda mais as investigações policiais, e consequentemente a persecução criminal. Infelizmente essa é uma escolha difícil que deve ocorrer, pois um passado antidemocrático ainda assusta e influi nas decisões políticas do país.

A perícia em crimes digitais necessita de procedimentos profissionais e bem técnicos. No processo de perícia computacional toda informação relevante deve ser coletada para análise, extraída, restaurada (caso esteja danificada), documentada, e preservada, respeitando a todo momento a cadeia de custódia para que não haja questionamentos acerca da isenção da prova, obedecendo com isso um dos princípios mais importante da criminalística, o da documentação:

> Este princípio , baseado na cadeia de custódia da prova material, visa proteger, seguramente, a fidelidade da prova material, evitando a consideração de provas forjadas, incluídas no conjunto das demais, para provocar a incriminação ou a inocência de alguém. Todo o caminho do vestígio deve ser sempre documentado em cada passo, com documentos que o oficializem, de modo a não pairarem dúvidas sobre tais elementos probatórios. A documentação correspondente a cada vestígio pode ser realizada por anotação ou despacho do próprio perito que o considerou (STUMVOLL, 2014, p.10).

O local de crime é o local onde provavelmente se encontrarão os vestígios relacionados à prática de uma infração penal. Essas evidências são de extrema importância para que possamos definir a autoria (Quem cometeu o crime), a dinâmica (como ocorreu o delito), e a materialidade do delito. Inclusive isso é muito mostrado nas mídias, séries, e filmes policiais, a exemplo do “CSI Investigation”.

O local de crime de informática é um tipo específico de local que apresenta como característica marcante a presença de dispositivos computacionais. Para operações envolvendo locais de crime deve-se realizar um planejamento que contemple o isolamento, a análise, a documentação minuciosa do local onde foram encontradas as evidências, e sua coleta de modo a respeitar a cadeia de evidência:

> cuidados especiais devem ser tomados durante a coleta dos vestígios digitais, pois assim como alguns vestígios convencionais, são muito sensíveis, uma vez que podem ser facilmente perdidos e/destruídos. O impacto, a umidade, a imersão em água, o calor excessivo, o atrito e o eletromagnetismo são apenas alguns exemplos de possíveis causas de perdas de informações digitais. Após a coleta, precauções também devem ser tomadas durante o transporte e armazenamento do material apreendido (ELEUTERIO, MACHADO, 2010, p. 26).

Entre as etapas básicas da perícia temos a identificação, a apresentação, a análise, e a apresentação. Na identificação se utiliza o mandado de busca e apreensão para se realizar uma busca legalizada no suposto local de crime identificando, documentando e apreendendo as evidências identificadas.

Com a preservação se realiza a manipulação das evidências através da coleta e documentação da custódia, embalagem, e transporte das evidências. Na análise fazem-se os exames propriamente ditos. Na apresentação busca-se materializar as provas através da confecção dos laudos periciais (COSTA, 2011, p. 48).

Os peritos dos locais de crime informáticos devem seguir um protocolo específico de modo a obedecer um profissionalismo e técnica necessária à credibilidade de determinada

perícia. O perito portanto, ao cumprir mandados de busca e apreensão em casas, empresas e demais locais de crime, deve com o auxílio de seus conhecimentos fornecer uma boa orientação à equipe quanto à seleção, preservação e coleta dos dispositivos computacionais imprescindíveis a uma posterior perícia em laboratório.

A fase de identificação das evidências envolve o levantamento de dados como nome das pessoas envolvidas, datas, locais, e circunstâncias dos fatos. De posse desses fatos o perito terá uma noção maior do que deverá procurar no local do crime. Um detalhamento dos vestígios é essencial para a sua posterior análise e convencimento da sua relação com o fato delituoso investigado.

Essa fase é muito importante e nela é preciso que haja uma boa interação entre a investigação e a perícia de modo que ambos atuem de maneira sinérgica, beneficiando ambas atuações, e conseguindo alcançar os resultados de forma objetiva e eficiente. Por isso a integração entre a polícia e a perícia são primordiais para o andamento célere da investigação criminal.

Recomenda-se entrevistar as pessoas do local do crime de modo a obter-se informações de como os computadores são utilizados, para que de posse desse conhecimento prévio seja possível ter uma ideia do que deve ser buscado no local.

Na fase de preservação das evidências inicia-se a coleta dos dados necessários a investigação. É uma fase crítica na análise forense, onde o profissional da computação deve seguir critérios necessários para evitar a perda de dados relevantes, bem como de garantir a sua integridade.

Precauções devem ser tomadas porque uma operação simples pode causar a perca de informações armazenadas (ALMEIDA, 2011, p. 18). Uma das principais providências em qualquer local de crime é o cuidado de impedir a entrada de pessoas estranhas à equipe, de modo que somente aquelas pessoas que tenham a autorização do chefe de equipe possam adentrar no local do crime.

Especificamente em relação aos locais de crimes informáticos deve-se evitar ligar os equipamentos computacionais que estejam desligados, pois tal atitude pode levar à perca de informações valiosas. Muitas vezes deve-se atentar à necessidade de desconexão de equipamentos ligados à rede ou a retirada das fontes de energia, pois há inclusive um risco de que um acesso remoto apague arquivos importantes à investigação.

Existe inclusive a possibilidade de que a memória RAM do computador, memória essa de característica volátil, apresente dados cruciais para a informações, requerendo assim um tratamento profissional para que os seus dados não sejam perdidos com o desligamento do aparelho (SILVA, LORENS, 2009, p. 21).

Um dos pontos que não se pode descuidar é em relação à utilização dos objetos encontrados no local do crime, o que não pode ser feito por pessoas sem a habilidade para verificá-los, o que pode ocasionar a perca das informações por descuido. Importante recordar também que o Perito é uma pessoa investida oficialmente em um cargo público através de concurso público, ou um profissional de notório saber técnico designado por autoridade judiciária, conforme Código de Processo Penal Brasileiro.

O trabalho de busca e apreensão requer certas ações a depender do caso concreto. Esse tipo de utilização específica requer na maioria das vezes a utilização de softwares apropriados para essa tarefa. Existe inclusive um procedimento operacional recomendado para a Secretária Nacional de Segurança pública com o intuito de padronizar os exames periciais de equipamentos computacionais (BRASIL, MINISTÉRIO DA JUSTIÇA, 2013, p. 87).

O perito deve levar em consideração os seguintes questionamentos ao realizar um perícia em um local de crime: O que apreender? Como apreender? Como descrever o material apreendido? Como acondicionar e transportar o material apreendido? A depender do tipo de investigação e delito a ser apurado, os dispositivos a serem apreendidos podem ser bem diferentes.

Quando se busca arquivos e dados contidos em computador, a apreensão de dispositivos de armazenamento como discos rígidos, pendrives, cartões de memória, CDs, DVDs, etc, podem ser suficientes. Já ao se investigar falsificação de documentos devem se apreender impressoras e aparelhos *scanner*.

Ao se investigar crimes de posse e transmissão de pornografia infanto juvenil deve-se atentar se o dispositivo computacional se encontra ligado e se o mesmo está transmitindo o material pornográfico. Busca-se apreender também câmeras fotográficas e filmadoras que possam estar relacionadas com a gravação desse tipo de material (U.S. DEPARTMENT OF JUSTICE , 2008, p. 36).

Ao se investigar crimes de “pirataria” ou cópia ilegal de CDs e DVDs, deve-se apreender os equipamentos gravadores de mídias ópticas, além das próprias mídias e impressoras utilizadas para confecção dos encartes. Devemos lembrar que em qualquer

procedimento de busca e apreensão, os agentes da lei devem buscar incessantemente a prova do crime. Essa “prova digital” pode ser armazenada ou transmitida, a exemplo de arquivos, fotos, vídeos,, históricos armazenados em um disco rígido do computador, vídeo digital, áudio digital, etc.

Feitas essas condições técnicas percebe-se que a etapa da perícia forense deve ser realizada de forma bem criteriosa, e que para isso é necessário o trabalho de pessoas qualificadas tanto no nível técnico como a nível de relacionamento, pois o perito vai ter que interagir com os investigadores para a busca da verdade real.

As estruturas de perícia estão em constante evolução, mas ainda há muito para se desenvolver para que o combate aos crimes cibernéticos possa ser efetivado de fato. O número de peritos computacionais ainda é muito escasso, o que inviabiliza o andamento das investigações para essa espécie de crime que cresce mais a cada dia.

4. QUESTÃO INTERNACIONAL E EFETIVIDADE PENAL

Como os crimes cibernéticos são delitos que ultrapassam as fronteiras geográficas dos países, uma ação internacional é essencial para uma atuação efetiva na persecução criminal, que tem como objetivo aplicar a pena devida ao infrator que se utiliza de meios virtuais. O acesso das pessoas a uma investigação completa e um processo judicial célere são características fundamentais para a inibição dos crimes envolvendo tecnologias digitais.

4.1 Cooperação Internacional no combate aos Crimes Informáticos

Um dos pontos mais significativos para a disseminação dos crimes virtuais diz respeito à sensação de anonimato que os criminosos que cometem esse tipo de delito apresentam. De fato um criminoso pode cometer um crime de qualquer parte do mundo, além de poder utilizar mecanismos tecnológicos que dificultem o seu rastreamento.

Em um cenário de forte crescimento do crime organizado e perigo de atos terroristas a investigação computacional muito pode auxiliar na manutenção da paz mundial. Não podemos mais tentar viver como uma ilha e esquecer que o Brasil é um país com milhares de relações com outros países, e logicamente que isso gera muitas consequências. O fenômeno da globalização flexibiliza de certa forma o conceito de soberania:

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

Uma situação que deve ser destacada é o fato de o Direito Internacional ter evoluído de uma concepção clássica, onde as normas eram dirigidas aos Estados como sujeitos de Direito Internacional para um cenário contemporâneo no qual organizações internacionais, empresas transnacionais, e indivíduos podem assumir também papeis importantes na construção dos rumos da política mundial.

Isso está ligado também à enorme evolução tecnológica, onde as barreiras da comunicação foram superadas. Hoje em dia um indivíduo pode muito bem fazer uma doação

ou prestar palavras de solidariedade a um país estrangeiro, bem como acionar mecanismos de destruição contra esse país à distância e de um âmbito confortável.

O Direito enfrenta mais um desafio com a necessidade de convergência dos ordenamentos jurídicos diversos. Não há como negar a crescente ligação entre as nações do planeta, a para isso basta só verificar o quanto uma crise mundial afeta a economia em todos os países.

A nova ordem mundial requer habilidades na busca de relacionamentos estáveis e benéficos entre os países, até mesmo porque existem assuntos que afetam a todos, o que gera a necessidade de acordos de cooperação entre os mesmos. Nesse contexto, o direito brasileiro por si mesmo não basta, havendo a necessidade de um Direito Internacional desenvolvido:

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

Em relação aos Crimes Cibernéticos não podia ser diferente. *hackers* de diferentes países se unem para realização de invasões de dispositivos. Grupos de especialistas computacionais realizam os mais ousados ataques a sistemas de segurança ao redor do globo.

Se não fosse suficiente a dificuldade em investigar delitos virtuais devido a toda uma questão de tecnologia informática, ainda há o diferencial entre os ordenamentos jurídicos, o que pode fazer com que os criminosos obtenham vantagens tanto na dificuldade em serem rastreados, como pela impunidade oriunda da falta de legislação criminalizadora.

Uma das maiores dificuldades na investigação de crimes cibernéticos em âmbito internacional diz respeito à demora em se obter informações dos provedores de serviços de internet, informações estas por vezes essenciais ao desenvolvimento da investigação criminal. Há que se respeitar as regras de relacionamento internacional como Tratados e Convenções para o sucesso dessa empreitada.

Infelizmente pode ocorrer uma certa burocratização do processo, o que pode dificultar o desvendamento do crime. O Tratado é um acordo formal internacional celebrado por escrito entre Estados ou organizações internacionais, regido pelo Direito Internacional, que conste de

um instrumento único ou mais de um instrumento conexo, que produza efeitos jurídicos independentemente de nomenclatura particular (GUTIER, 2009, p. 14). A realização de Tratados é de extrema importância para que o país consiga investigar os delitos computacionais.

A Constituição brasileira protege as comunicações privadas através do princípio da inviolabilidade do sigilo das comunicações, conforme art. 5º, XII [13]. Ao solicitar informações cadastrais ao provedor de um determinado serviço utilizado por um suspeito, muitas vezes se necessita de uma autorização judicial para tanto.

Esses serviços podem ser tanto uma conta de e-mail quanto uma página da Internet, ou mesmo um perfil de rede social que o autor do delito utilizou para manter contato com a vítima. No caso de uma investigação no qual o tempo não pode ser considerado um amigo, esse tipo de burocracia pode gerar um atraso significativo.

Já existiram situações polêmicas envolvendo redes sociais como o Whatsapp, dentre outras, a exemplo do Facebook, Instagram, etc. No caso específico do Whatsapp, houve um impasse entre o judiciário e os administradores dessa aplicativo, pelo simples fato de não atenderem a requisição da justiça para quebrar o sigilo de algumas mensagens criptografadas.

Tanto a justiça de São Paulo quanto a do Rio de Janeiro pediram o bloqueio do aplicativo de comunicação devido a não colaboração com as investigações, o que acabou gerando uma certa polêmica no país. Isso acabou por fazer com que tal aplicativo tenha uma predileção como meio de comunicação entre grupos criminosos, visto a jurisdição brasileira não conseguir a interceptação e decodificação dos dados envolvendo essa tecnologia.

No caso da Internet, o endereço IP é um importante dado para investigação pois embora o criminoso oculte seus dados cadastrais de um determinado provedor de serviço, seu endereço IP utilizado para acesso a esse serviço pode ficar registrado nesse provedor. Esse endereço IP pode nos auxiliar a rastrear o local e a máquina de onde partiu determinado ataque criminoso.

Interessante observar que a delimitação do local de crime fica complicada devido ao fato de o criminoso poder estar em qualquer lugar do mundo. Assim algumas vezes, para se

13 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

determinar a circunscrição ou jurisdição de um determinado crime deve-se procurar todos os locais associados a atos relacionados com o delito, e assim talvez seja necessário a troca de informações referentes a essa investigação com vários países, o que por si só já torna a investigação mais complexa.

Através de uma legislação adequada, do comprometimento de todos os países do globo, e da eficiência dos órgãos de combate aos crimes cibernéticos, é que se consegue coibir a ação dos criminosos na Rede Mundial de computadores (BLATT, 2016, p. 83). O primeiro passo é reconhecer que esse tipo de crime vai além das fronteiras nacionais, e que todo acordo de cooperação que possa ser realizado é importante para a celeridade das investigações, pois o tempo nesse tipo de crime é um fator bastante crítico, sendo que em certas situações deve-se investigar o fato simultaneamente à sua ocorrência.

A Interpol enfatiza a necessidade de profissionais especializados para lidarem com esses delitos, sendo que tal organização possui um sistema de comunicação mundial para troca de informações, o I-24/7. A Polícia Federal, por exemplo, tem acesso à esse sistema, até mesmo porque fazem parte da Organização Internacional de Polícia Criminal (OIPC/Interpol).

Entretanto, a maioria desses crimes devem serem investigados pelas polícias civis dos estados, que em sua grande maioria, não sabem nem ao menos como lidar com esse tipo de delito, e muito menos como solicitar uma cooperação internacional, mesmo que seja por intermédio da polícia federal.

Em termos de Legislação de crimes cibernéticos no exterior, temos que destacar a legislação estadunidense devido ao amplo uso dos provedores desse país. Nesse país, cada estado apresenta uma legislação autônoma, sendo que a legislação federal também impõe obrigações aos seus provedores.

Nos Estados Unidos, a quebra do sigilo é obtida com maior facilidade pelas autoridades policiais, sem a necessidade de acionamento do poder judiciário, fato esse bastante destacado nas séries policiais, onde cria-se a impressão de que seja possível obter informações sobre a vida de qualquer pessoa com muita facilidade devido ao poderoso banco de dados que os EUA possuem.

Independentemente dos exageros da ficção, fato é que nos Estados Unidos há uma maior confiabilidade em relação às instituições policiais, o que torna mais simples o processo de obtenção de dados imprescindíveis para as investigações policiais, que também são bem

valorizadas, o que ajuda a explicar os melhores índices de combate à criminalidade nessa nação.

Quando uma equipe de investigação do brasileira necessitar de informações de provedores estadunidenses uma certa dificuldade pode ser encontrada pelo fato de poucos deles terem representantes no Brasil e não costumarem se sujeitar à legislação brasileira. Por esse motivo deve-se utilizar o procedimento padrão de solicitar ao juízo local através de carta rogatória as informações dos provedores. Infelizmente esse é um procedimento que pode levar anos.

Em respeito aos princípios da independência nacional, da autodeterminação dos povos, da não -intervenção, e da igualdade entre os Estados, toda relação internacional deve respeitar a soberania de cada nação envolvida. Devido a isso uma empresa estrangeira sem representação no Brasil não tem a obrigação formal de respeitar a legislação brasileira e de fornecer informações que não encontrem amparo na legislação do seu país (VERSIANNI, 2016, p. 153).

Há portanto a necessidade de um trabalho internacional de modo a superar essas dificuldades pois do contrário fica praticamente impossível a investigação de delitos que envolvam alguns países, o que pode acabar criando paraísos informáticos criminosos, onde fica praticamente impossível a obtenção de “pistas” necessárias para as investigações digitais.

Grande parte dos provedores de serviços mantém as suas cópias com os registros de acessos por um prazo máximo de noventa dias, e às vezes, por menos tempo, devido a falta de leis que os obriguem a preservarem tais dados por mais tempo. Devido à morosidade dos procedimentos envolvendo cartas rogatórias, pode acontecer de os dados necessários para a investigação já terem sido liberados pelo provedor, tornado assim os vestígios perdidos (SILVA, 2006, p. 10).

A Rede 24x7 apesar de ainda ser limitada quanto à questão da cooperação, ainda possibilita que os dados dos provedores sejam ao menos preservados por tempo suficiente para que o processo da carta rogatória não perca o seu objeto, o que a torna um instrumento essencial para o trabalho investigativo internacional.

O fato é que a Internet criou um cenário que exige uma cooperação internacional mais acentuada para o combate aos crimes cibernéticos. Não podemos esquecer que no combate aos crimes transnacionais, não podem existir mecanismos que contrariem as constituições de cada Estado.

Há caso em que inclusive provedores estrangeiros situados no Brasil negaram quebra de sigilo devido a alegação de que tal pedido deveria ser direcionado ao poder judiciário do país de origem, o que mostra o quanto essa questão internacional é delicada. Logicamente deve haver uma ligação entre a Cooperação jurídico penal e o garantismo penal de modo a sempre observar os princípios da segurança jurídica e respeito à dignidade da pessoa humana.

> Nesse ínterim, se adentraria numa sociedade em que todos são, a priori, suspeitos, e não presumidamente inocentes, em evidente desrespeito ao princípio do estado de inocência, estabelecido, segundo Damásio, a partir do art. 5º, LVII da Carta Magna. Romperia-se, ainda, com os direitos constitucionais de todos à privacidade e intimidade, de uma forma sem precedentes ou proporcionalidade, pois, no paradoxo entre monitoramento e privacidade, de que trata Assis Medeiros (MEDEIROS, 2002, p. 153), se supervalorizaria o primeiro em detrimento da segunda. Enfim, claramente se adotaria um posicionamento antidemocrático através desse policiamento cibernético indiscriminado, ao se privar a democratização da informação pela proibição do compartilhamento de arquivos entre usuários. (SOUZA, PEREIRA, 2009, p.10)

Existem duas formas de cooperação internacional: as que podem serem feitas através da colaboração entre as polícias, e a cooperação jurídica que deve ser realizada entre juízes e membros do ministério público. Logicamente, a cooperação via judiciário é mais morosa ainda, a exemplo das buscas dependentes de mandado judicial.

A Comunidade europeia foi pioneira na criação da Convenção de Budapeste que visa combater a cibercriminalidade através de auxílios mútuos, trazendo procedimentos para o recolhimento de provas virtuais e na aplicação de medidas que facilitem a persecução de tais crimes. Essa convenção foi firmada pelo conselho da Europa em 23 de novembro de 2001, entrando em vigor no ano de 2004, onde formalizou a intenção de uniformizar legislações, terminologias, definições, e mecanismos de cooperação internacional (, BEZERRA, AGNOLETTO, 2016, p. 182)

A Convenção de Budapeste recomenda critérios de resolução de conflitos jurisdicionais para que todos os países possam ter competência sobre as práticas de crimes cibernéticos. Procura inclusive ampliar a cooperação entre os países membros nas investigações dos delitos envolvendo computadores com previsões referentes à assistência, extradição e cooperação mútua, mesmo naqueles casos que não haja tratado ou reciprocidade entre os Estados. Infelizmente o Brasil ainda não aderiu a essa importante Convenção , o que não se explica frente ao crescimento do número de vítimas desses crimes no país.

Para o combate dos crimes cibernéticos, na busca de provas o investigador deve saber uma série de requisitos que podem variar a depender do país ao qual se deva encaminhar os pedidos. Até mesmo para punição do infrator deve-se observar os critérios e tratados de extradição firmados entre os países para que o *jus puniendi* possa ser exercido.

Como o Brasil adota o princípio da territorialidade quando os crimes cibernéticos são cometidos no território nacional ou onde o Brasil exerça a sua soberania, independentemente da nacionalidade do autor ou da vítima, a jurisdição será brasileira, conforme art. 5º do Código Penal brasileiro. Deve-se é claro levar em consideração os acordos e tratados nacionais como os que dizem respeito às embaixadas e representações estrangeiras.

Entretanto, como já comentado, os crimes virtuais costumam irem além das fronteiras nacionais. Existem situações em que o Brasil pune crimes cometidos em outros países, casos nos quais os autores devem serem processados e julgados no Brasil. Esses são os casos de Extraterritorialidade previstos no Art. 7º do CPB (GRECO, 2014, p. 135).

A Extraterritorialidade pode ser incondicionada ou condicionada. No caso da Incondicionada a jurisdição brasileira se aplica de forma absoluta, sem depender de nenhum requisito. É o caso de crimes contra o presidente da República, Fé Pública, Administração Pública, etc. Nos casos da Extraterritorialidade condicionada existem alguns requisitos para que o crime possa ser punido no Brasil. De toda forma é necessária uma política e diplomacia para que um criminoso estrangeiro possa ser extraditado para o Brasil.

Para que a situação não acabe se tornando um incidente diplomático grave acaba sendo necessário o estudo dos tratados e convenções assinados entre o Brasil e o país do qual se necessita a extradição de um criminoso. Há alguns casos que praticamente não há a possibilidade de punição dos autores dos crimes, a exemplo do caso *Wikileaks*, no qual a presidente da época (Dilma Roussef) e membros importantes do governo estavam sendo espionados pelos Estados Unidos. Quem punir nesse caso e como punir sem gerar um grave problema diplomático?

Como muitos brasileiros também cometem cibercrimes, pode ocorrer de um país estrangeiro solicitar a extradição de alguma pessoa brasileira. A regra é que brasileiros natos não podem serem extraditados de forma alguma. Até mesmo os naturalizados não podem serem extraditados por crimes cometidos após sua naturalização, nem tampouco por crimes políticos.

Nem sequer os estrangeiros podem serem extraditados para países que almejem a aplicação de penas de caráter cruéis devido ao principio da dignidade da pessoa humana. Ao negar a extradição de alguém, entretanto o Brasil tem o compromisso de julgar e punir de acordo com suas leis os crimes objetos do pedido de extradição, o que não deixa de ser mais uma inquietação visto o país não ter condições de cuidar apropriadamente nem dos crimes nacionais.

Como a maioria dos provedores que os brasileiros utilizam são provenientes dos Estados Unidos, é importante se ter alguma noção sobre os tratados que existem entre os dois países. Há um Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América – Decreto n º 3.810, de 2 de maio de 2001 (WENDT, JORGE, 2013, p.132). Há também a Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo), a Convenção das Nações Unidas Contra a Corrupção (Convenção de Mérida), a Convenção contra o Tráfico Ilícito de Entorpecente e Substâncias Psicotrópicas (Convenção de Viena) e a Convenção Interamericana sobre Assistência Mútua em Matéria Penal (Convenção de Nassau, OEA).

Esse conjunto de legislações possibilitam solicitações de oitiva de testemunhas, oitiva por meio de depositions (oitiva de testemunhas fora do tribunal competente), obtenção de bloqueio de ativos, preservação de dados de computador armazenados, obtenção de dados de computador armazenados, como logins, informações de assinantes de informações de conteúdo mais antigo, cumprimento de mandado de busca para obter conteúdo de e-mail mais recente e interceptação de telecomunicações ou de dados de computador em tempo real.

Cada uma dessas solicitações (depositions) apresentam determinadas particularidades para serem aceitas, mas em geral todas elas requerem um pedido bem fundamentado com base em provas que possam ensejar uma justificativa plausível para a quebra do sigilo de suspeitos submetidos a uma investigação.

Como O Brasil é signatário de um Tratado para Cooperação Judicial (MLAT), órgãos de investigação brasileiros podem representar pela concessão desse tipo de medida. Há casos em que os provedores podem viabilizar algumas informações sem tanta burocracia, mas em geral, existe todo um procedimento judicial para que países estrangeiros obtenham dados dessas empresas.

Nos casos de e-mail, site ou conexão de Internet de responsabilidade de provedores estrangeiros deve-se contatar o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça (VERSIANNI, 2016, p. 159).

O importante é que se estude com critério os requerimentos para que se obter as informações dos provedores, de tal modo que independente de que seja por Cooperação Jurídica, Cooperação Policial, ou mesmo diretamente com os provedores, não haja maiores atrasos no curso das investigações pois como afirma o criminalista Edmond Locard (LOCARD, 1939 apud FERRARESI, 2005, p. 63): “O tempo que se passa é proporcional à verdade que foge”. Isso não poderia ser mais claro quando se trata de delitos virtuais devido a facilidade que se tem em apagar os vestígios desse tipo de crime.

4.2 – Efetividade das Penas

Um dos efeitos mais gravosos do processo penal é a pena. Embora a mesma não deva ser encarada como um fim em si mesmo, fica difícil conceber um Direito Penal sem esse fator de coerção. A pena é, portanto um preceito secundário de uma norma penal que se constitui em uma sanção penal de caráter aflitivo, imposto pelo Estado em execução de uma sentença, ao culpado pela prática de uma infração penal, que se mostra como uma restrição ou privação de um bem jurídico (COIMBRA, 2010, p. 01).

Interessante uma compreensão do histórico das penas na humanidade, pois assim melhor se entende o atual caráter estatal e a busca constante de sanções humanitárias. A divisão em idade antiga, vingança privada, penas cruéis, e humanitarismo auxiliam o entendimento de como o Direito Penal e as sanções evoluíram ao longo da história da humanidade. A depender do período analisado espécies de penas bem diversas eram aceitas, em oposição à tendência atual na qual se busca um sistema que respeite os direitos fundamentais do homem.

Na Idade Antiga foi que se formaram os primeiros Estados organizados com certo grau de organização mais complexa. Nesse período a pena tinha a finalidade de eliminar o indivíduo que havia se tornado inimigo da comunidade e das forças divinas, e também evitar a punição dos seres sobrenaturais.

Os indivíduos acreditavam, por exemplo, que a ira dos deuses poderia vir em forma dos mais diversos fenômenos naturais como a seca e outros desastres naturais, de tal forma

que a punição de pessoas consideradas nocivas aos olhos divinos seria uma forma de se evitar um castigo a todo o grupo. Não havia, portanto uma racionalidade justificável para aplicação da penalidade, pelo menos do ponto de vista dos dias atuais, e a sanção tinha mais o caráter de aplacar a raiva divina.

Posteriormente tal postura defensiva evoluiu para o período da vingança privada (CALDEIRA, 2009, p. 07). Em tal fase procurava-se vingança acerca da agressão de um membro de um determinado grupo por um membro de outro grupo. Não se questionava bem o caráter do criminoso e o crime cometido, assumindo tal ato de vingança um caráter coletivo.

Em tal contexto de vingança privada é que se situa a lei de talião, que não deixa de ser um dos primeiros traços do princípio da proporcionalidade, o que pode ser percebido na máxima “olho por olho, dente por dente”. Não se pode dizer que tal postura de vingança tenha sido retirada por completo dos sistemas penalistas, tendo ocorrido de fato certa amenização a partir de preceitos legais. No entanto a filosofia de que um indivíduo deva pagar com certo rigor pelo dano causado a um particular nunca deixou de existir totalmente.

Com o desenvolvimento dos grupos sociais e o crescente apego à religião a prova dos fatos começou a ser realizada através das ordálias ou das provas divinas. Testes hoje considerados absurdos como fazer com que o indivíduo ande sobre o fogo eram utilizados para se verificar o grau de culpa de uma pessoa.

Caso tal pessoa sujeita a esse teste fosse culpada já teria dessa forma um castigo apto a aplacar a fúria divina. Havia inclusive uma supervalorização da prova da confissão, sendo que tal prova subjetiva poderia ser obtida mesmo através de tortura. Logicamente não havia sentido em se aceitar tal meio de prova, visto não haver o mínimo de autenticidade em um indivíduo que diria qualquer coisa para se livrar de intensos sofrimentos.

Um dos períodos nos quais houve maior evolução quanto à racionalidade das penas foi na época do iluminismo, através das ideias do estudioso Cesare Beccaria, que em sua obra Dos Delitos e das Penas começou a analisar os fundamentos da punição. Tal autor criticou o arbítrio judicial na aplicação das penalidades, as atrocidades das sanções, e a injustiça decorrente da falta de sistematização da legislação criminal na época. Para esse autor italiano a rapidez na aplicação da pena é o mais justo e útil:

> Quanto mais rápida for a aplicação da pena e mais de perto acompanhar o crime, tanto mais justa e útil ela será. Mais justa, porque evitará ao acusado os cruéis tormentos da dúvida, tormentos supérfluos, cujo horror aumenta para ele na razão da força da imaginação e do sentimento de debilidade. A rapidez do julgamento é justa também porque, sendo a perda da liberdade uma pena em si, esta somente deve preceder a condenação na exata medida em que a necessidade o exige (BECCARIA, 2001, p.57).

Beccaria não acreditava na ideia de que pena tivesse apenas um caráter retributivo. Para ele, o a pena deveria estar baseada nos princípios da utilidade e da máxima felicidade, de modo que a mesma visasse garantir a segurança e a boa convivência dos indivíduos em sociedade. O foco de uma boa legislação penal seria, portanto, a prevenção dos delitos e não a sua punição. As penas deveriam desviar os homens do crime e não atormentar o ser humano. Não existiria a possibilidade de se desfazer um delito já cometido, mas uma pena bem aplicada teria o condão de prevenir novos crimes e evitar danos sociais. Há a necessidade de uma proporção entre os delitos e as penas, de modo a evitar injustiças como a arbitrariedade na aplicação das sanções.

A aplicação das penas se justifica inclusive na necessidade que os homens tem de conviverem em sociedade. Existem diversas teorias que tentam explicar o motivo que levou os homens a conviverem em grupo, de modo a abdicarem de parte de sua liberdade em prol de um poder soberano.

Ao que tudo indica os seres humanos perceberam que não podiam ter as suas necessidades satisfeitas sem que houvesse o mínimo de colaboração entre os mesmos. Provavelmente foi por necessidade que os homens cederam parte da sua liberdade, e com a justificativa de manter essa sociedade o Estado possui o direito de punir. Entretanto tal direito deve estar em conformidade com a evolução atingida:

> A pena como instituição social torna transparente o nível de evolução moral e espiritual atingido por uma determinada sociedade. Atualmente, portanto, não é admissível qualquer postura semelhante àquela do chamado “direito penal do terror”, como o discurso do cadafalso, imposto ao condenado, que, momentos antes de morrer vitimado por seu carrasco, era obrigado a reconhecer sua culpa e abominar seu crime (SHECAIRA, JUNIOR, 2002, p.128).

Atualmente no ordenamento jurídico brasileiro existe uma limitação aos poderes do Estado, de modo que o mesmo deve atuar respeitando o princípio da Legalidade. Assim o Estado não deve atuar na esfera particular com desrespeito às leis, o que configura a base do

Estado Democrático de Direito. Há que se buscar garantir a Segurança jurídica, de modo a evitar que o Cidadão seja punido por um crime que nem sequer existia, e também não permitir que o mesmo seja apenado com sanções extremamente rigorosas e desumanas, o que contrariaria a racionalidade e os direitos humanos mais fundamentais.

O *jus puniendi*, ou o poder de punir do Estado é baseado, portanto em leis previamente elaboradas. Tanto os crimes e as penas devem ser previstos em leis penais, de modo a garantir que o cidadão tenha entendimento do seu erro e das consequências do mesmo. Torinho Filho acredita que o Jus Puniendi tem uma existência abstrata e concreta. Quando o Estado elabora por meio do legislativo leis penais cominando sanções para aqueles que desobedecerem ao mandamento proibitivo contido na norma penal, surge o Jus puniendi em abstrato. Já quando o Estado desce do nível abstrato para o plano concreto de modo a infligir a pena ao autor da conduta proibida e restringindo o seu *jus libertatis*, temos o Jus puniendi em concreto (FILHO, 2010, p.29).

Isso não deixa de ser uma conquista dos cidadãos, que acabam assim sendo de certa forma protegidos dos desmandos do Estado, tendo que haver regras preestabelecidas. Importante recordar que todas as leis devem estar em consonância com a Constituição Federal do Brasil, de modo que não se deve aceitar uma lei que permita uma prisão perpétua ou cruel, devido à afronta evidente à Constituição. Há uma característica de supermacia da Constituição, de modo que a mesma irradia seus preceitos a todo ordenamento jurídico:

> *A relação do direito penal com o direito constitucional deve ser sempre muito estreita, pois o estatuto político da Nação – que é a Constituição Federal – constitui a primeira manifestação legal da política penal, dentro de cujo âmbito deve enquadrar-se a legislação penal propriamente dita, em face do princípio da supremacia constitucional (ZAFFARONI, PIERANGELI, 2002 , p.135)*

Assim deve-se considerar a importância do *jus puniendi* como mecanismo que o Estado necessita utilizar para manutenção da sociedade, mas não devemos esquecer das suas limitações baseadas na legislação e na Constituição Federal Brasileira. Antigamente as penas eram tão cruéis que muitas vezes o sofrimento causado ao criminosos o tornava uma vitima devida tamanha desproporcionalidade.

Devido à gravidade das atrocidades cometidas durante o período da Segunda Guerra Mundial foi criada a Declaração dos Direitos do Homem e a Convenção de Viena,

instrumentos esses que defendiam os Direitos fundamentais e combatiam a aplicação de penas severas.

O art. 5º, inciso XLVII, da Constituição Federal brasileira veda as penas de morte, de caráter perpetuo, de banimento, e penas cruéis. A pena de morte só é admitida em casos extremos de guerra declarada. As de caráter perpétuo não são admitidas, existindo um limite temporal de 30 anos no qual uma pessoa possa ficar presa. As penas de banimento não são admitidas por não se permitir a deportação de brasileiro. As penas cruéis não são aceitas devido a própria Constituição reprovar a tortura. A pena de trabalhos forçados também não é aceita devido o fato de o preso que trabalhe ter direito à remuneração.

Quanto às penas admitidas no Direito Brasileiro temos: penas restritivas de liberdade, penas restritivas de direito, e penas de multa. As penas restritivas de liberdade retiram a liberdade do indivíduo que comete Crimes apenados com penalidades de reclusão ou detenção. A prisão simples é aplicada àqueles que cometem contravenções e outros crimes de menor potencial ofensivo.

A pena de multa pode ser aplicada única ou cumulativamente com outras penas nos Crimes ou Contravenções. As penas restritivas de direito visam substituir as penas de restrição de liberdade por outras penalidades menos rigorosas. Como exemplo de penas restritivas de direitos temos: limitação de fim de semana, prestação de serviços à comunidade, etc.

Entendido o histórico das penas e a tendência atual de flexibilização das sanções penais, fica a indagação de como o atual sistema de penas pode ajudar a inibir os crimes cibernéticos? Há certa hipocrisia em se defender penas mais brandas, pois não se tem mostrado estudos científicos aptos a justificar tal amenização.

No caso do atual crime de invasão de dispositivo informático, um dos poucos crimes cibernéticos próprios, fica o questionamento de se tal sanção com valor máximo de três anos realmente tem condições de inibir especialistas em computação de continuarem a realizar tais condutas criminosas, afinal o custo benefício de tal violação tende a ser um ponto bem favorável à prática do crime.

A punição, segundo a ótica da psicologia behaviorista, é um procedimento importante que envolve a entrega de uma resposta quando há um estímulo aversivo. Os dados das pesquisas tem demonstrado que a supressão do comportamento indesejado só é definitiva

quando a punição for realmente intensa, isso porque geralmente os motivos que estimularam a ação não são suprimidos com a punição (BOCK ET AL, 2001, p. 66).

Isso significa que a gravidade da sanção tem o seu fator inibitório em relação ao crime. Entretanto, parece que o Estado justifica a sua ineficiência em punir o infrator com eficiência utilizando a ideia de que estratégias como tornozeleiras eletrônicas sejam mais adequadas. Quem acaba perdendo com isso é a vítima e a própria população, visto que o infrator acaba não sendo nem punido e muito menos reinserido na sociedade.

Observa-se que uma minoria da população carcerária esteja relacionada com crimes cibernéticos, até mesmo porque não existe crime estritamente virtual que justifique uma pena privativa de liberdade. De toda forma, pode-se perceber que a maior parte dos presos está relacionada a crimes de danos mais visíveis à sociedade. Acontece que se nem os crimes mais gravosos tem sido tratados com o devido cuidado, o que dizer de crimes cibernéticos que nem sequer conseguem ser considerados algo perigoso a priori. Há de fato certa aceitação de alguns delitos virtuais, a exemplo de crimes de colarinho branco, o que faz com que dificilmente o infrator acabe preso.

Com um sistema penitenciário falido, que não consegue ressocializar ou punir adequadamente o criminoso, e com medidas alternativas aplicadas em desconformidade com a realidade do país, fica ainda mais evidente a impossibilidade do sistema brasileiro combater o delito cibernético sem uma reforma substancial no seu sistema penitenciário.

Em respeito ao princípio da intervenção mínima o direito penal só deve ser aplicado em último caso, entretanto, caso deva ser utilizado, não adianta flexibilizá-lo de tal forma a não satisfazer o pedido de justiça da vítima, o desestímulo ao delito, e a reinserção do infrator:

> A ressocialização (ou, em certos casos, a socialização substitutiva de outra deficiente) como fim da pena, especialmente a de prisão, não é mais que um mito, que não se sustenta empiricamente. Da mesma forma que a defesa da prevenção geral intimidatória se baseia em em uma sobrevalorização empiricamente insustentável da capacidade de influência das normas penais e das penas nas decisões cotidianas dos cidadãos, a prevenção geral sobreestimou a capacidade de influência positiva da pena nos condenados e, por isso, fracassou (SANCHEZ, 2015, p.54)

Essa flexibilização sem planejamento pode acabar por tornar a figura do direito penal mais desacreditada do que já é, além de tornar inepto esse importante instrumento de

controle social. Não parece acertada descartar o efeito da gravidade da pena na inibição do crime. O crime de tráfico de drogas na Indonésia, por exemplo, é punido com a pena capital, e isso tem o seu efeito na mentalidade das pessoas daquele país.

Logicamente que não se devem conceber penas desrespeitosas aos direitos fundamentais no sistema jurídico brasileiro, entretanto é importante reconhecer que um crime de invasão de um dispositivo informático pode evoluir para danos de proporções elevada, e que tal conduta deve ser bem desencorajada.

A sanção criminal não precisa necessariamente atacar a liberdade da vítima, sendo interessante inclusive, como acontece em países como os Estados Unidos, uma sanção com efeitos econômicos significativos no patrimônio do criminoso, sendo possível até que esse dinheiro seja utilizado para minimizar os danos as vítimas. Isso significa que sanções muito brandas não tem a persuasão necessária para evitar a prática de boa parte dos delitos virtuais. Há, portanto a necessidade de aplicação de penas maiores para esse tipo de crime, além de apurados critérios para concessão de outras benesses penais como a suspensão condicional do processo.

4.3 Acesso à justiça

Existe uma problemática na ligação entre os conceitos de direito e de justiça. O termo direito tem origem etimológica com o correto e adequado, do latim "*directum*". Já a palavra justiça, é proveniente do latim "*justitita*". A prova da ligação entre essas duas palavras é a quantidade de denominações do direito ligados à palavra justiça. A exemplo das palavras jurídico, juiz, jurisdição, etc. Entretanto nos estudos de introdução ao direito os alunos são levados a questionar a força de tal relação, assim como a relação do direito com outros ramos do conhecimento humano como a moral e a política.

O fato é que muitos dos legisladores, profissionais do direito, e população acreditam que a busca do direito consiste na aplicação da justiça. Entretanto, ao que parece nem sempre uma decisão embasada na lei parece ser a mais justa, até mesmo porque o conceito de justo é uma discussão filosófica tão profunda quanto o da verdade. Há quem acredite que exista um conceito de justiça imutável ao longo do tempo, e quem acredite que tal conceito evolui com a época, ou que possui uma certa relatividade. Portanto, há essa problemática nas relações entre o direito positivo e a justiça:

> O exame de vários aspectos da problemática da justiça em sua relação com o direito positivo conduziu-nos a resultados negativos. O conceito da justiça é extremamente controvertido e não parece possível dar uma definição que permita operacionalizá-la para avaliar o caráter justo ou injusto do direito em vigor. Diante dessa situação, a persistência da doutrina em reivindicar a vinculação do direito positivo com a justiça revela-se como tentativa para legitimar ou deslegitimar determinados regulamentos mediante o apelo emocional à justiça (DIMOULIS, 2011, p. 97).

Acontece que as palavras às vezes possuem uma multiplicidade de significados, e com o termo justiça não é diferente. Podemos aceitar o uso de tal palavra em seu sentido amplo ou estrito. No sentido amplo pode-se considerar justiça como o sentimento ou valor pelo qual as pessoas sentem que há certa reciprocidade e isonomia nas relações sociais.

As pessoas acreditam que há justiça quando pessoas que se adaptam ao ordenamento social são recompensadas, e pessoas que não se adaptam e prejudicam as demais sejam penalizadas. Tal ideia, por mais que tenha sido flexibilizada ao longo dos tempos, continua viva na mente da população, que espera que as leis garantam o equilíbrio na sociedade, não sendo à toa a representação da “balança” como parte do símbolo da justiça.

Já no sentido estrito, a palavra justiça estaria de acordo com o aparato do Estado que visa dirimir os conflitos sociais com a imposição das leis abstratas aos casos concretos. Fica o questionamento da capacidade dessa organização estatal na realização desse mister. Interessante observar que dentre as funções mais remuneradas do serviço público, as que envolvem as organizações judiciais se encontram dentre as mais bem pagas.

Existe portanto um investimento alto da sociedade, ficando assim o questionamento do real retorno obtido pela maioria dos cidadãos? Quais crimes são os mais julgados e quais pessoas conseguem obter uma prestação jurisdicional célere? Faz sentido pedir eficiência do poder judiciário considerando tanto a sua importância para o equilíbrio da sociedade, quanto em respeito à ideia de que a quem mais se dá , mais se exige em termos de resultados.

Pode-se inclusive mencionar o fato de que a diferenciação começa já na fase da investigação policial. Basta mencionar o caso do roubo cometido contra o Ministro Gilmar Mendes na cidade de Fortaleza em 2010, onde foi subtraído o seu cordão de ouro. Rapidamente o seu caso foi solucionado. Dai fica a indagação de quantas pessoas são assaltadas nesse mesmo local e tem o seu objeto recuperado?

E quanto aos sequestros que foram extintos do estado do Ceará? Devido ao número considerável desse tipo de crime foi criada uma divisão especializada no combate a esse tipo

de crime que praticamente não existe mais no estado. O poder aquisitivo dessas pessoas que geralmente são sequestradas tem influência na rápida solução desse crime? Porque não criar uma divisão de combate aos crimes virtuais, visto boa parte da população já estar sendo vítima desses delitos? Ao que tudo indica as diferenças de acesso à justiça já começam na fase policial.

O Direito existente em uma determinada sociedade ajuda a definir o quanto podemos considerá-la isonômica. Os componentes da igualdade indicam os aspectos em relação aos quais as diferenças se tornaram inaceitáveis em um Estado dito democrático de direito. Assim, foi realizada a passagem de uma sociedade baseada em privilégios e prerrogativas, para uma sociedade aberta e sem distinções, de acordo com a onda de constitucionalismo social:

> O constitucionalismo social não renega os elementos positivos do liberalismo – a sua preocupação com os direitos individuais e com a limitação do poder – mas antes pugna por conciliá-los com a busca da justiça social e do bem-estar coletivo. Ele implica a adoção de perspectiva que enriquece o ideário constitucionalista, tornando-o mais inclusivo e sensível às condições concretas de vida do ser humano, no afã de levar as suas promessas de liberdade e de dignidade também para os setores desprivilegiados da sociedade (NETO, SARMENTO, 2013, p.82).

O conceito de igualdade define e dá conteúdo ao de cidadania. Ser um igual e ser cidadão são conceitos que sofreram profundas alterações do mundo antigo até os dias atuais. Ser um igual em séculos passados não é a mesma coisa do que ser igual nos dias de hoje. Há portanto uma igualdade variável no tempo e no espaço, formada por componentes diversificados a depender do local, por exemplo.

Ser igual no Brasil é diferente de ser igual nos países islâmicos, e ser igual no Brasil de hoje é diferente da igualdade em tempos coloniais. A meta igualitária se mostra como uma ampliação do rol de direitos e em uma maior inclusão social. Houve, por exemplo, uma evolução em torno das conceitualmente consideradas gerações de direitos, nos quais os direitos de segunda geração contemplavam mais as questões sociais.

Buscou-se ir além de proteger os indivíduos contra as arbitrariedades do Estado, pois o cenário mais crítico era de uma diferenciação social enorme e perniciosa, de modo que não adiantava apenas dizer que os seres humanos eram livres, se os mesmos não tinham nem sequer o básico para viver dignamente. Para cada momento histórico e para cada país

determinadas desigualdades passam a ser consideradas inaceitáveis, havendo consequentemente evolução desse conceito ao longo dos anos.

No Brasil, por exemplo, já houve época na qual pessoas negras, pobres, ou do sexo feminino, não tinham sequer direito ao voto. Existe, portanto uma evolução da questão da igualdade na nação brasileira, consubstanciada nas leis que cada vez mais procuram garantir o preceito constitucional de que todos são iguais perante a lei.

O reconhecimento formal de direitos, entretanto, não significa que haja realmente uma real efetivação, o que pode fazer com que a crítica de Fernand Lassale acerca da Constituição não refletir as forças sociais que constituem o poder, não passando apenas de uma simples “folha de papel” sem o mínimo de efetividade e legitimidade (LENZA, 2014, p. 85).

Daí a tão criticada distância entre a legalidade e a realidade. O fato das relações reais não respeitarem a igualdade prevista em lei, não significa que tal ideal deixe de ser perseguido, o que indica um desafio a ser enfrentado por toda a sociedade . Deve-se verificar o quanto os mecanismos legais e estatais estão comprometidos com essa questão, de modo a tornar a igualdade formal algo possível de ser concretizado na prática:

> A absoluta igualdade jurídica não pode, contudo, eliminar a desigualdade econômica; por isso, do primitivo conceito de igualdade, formal e negativa (a lei não deve estabelecer qualquer diferença entre os indivíduos), clamou-se pela passagem à igualdade substancial. E hoje, na conceituação positiva da isonomia (iguais oportunidades para todos, a serem propiciadas pelo Estado), realça-se o conceito realista, que pugna pela igualdade proporcional, a qual significa, em síntese, tratamento igual aos substancialmente iguais. A aparente quebra do princípio da isonomia, dentro e fora do processo, obedece exatamente ao princípio da igualdade real e proporcional, que impõe tratamento desigual aos desiguais, justamente para que supridas as diferenças, se atinja a igualdade substancial (CINTRA, GRINOVER, DINAMARCO, 2014, p.72).

Dentre os direitos a serem garantidos ao cidadão brasileiro se encontra o direito de acesso à justiça, conforme Art. 5º, inciso XXXV, da Carta Magna. Assim, a garantia de acesso ao sistema de justiça é uma das condições de transformação da igualdade formal em igualdade material. No caso dos crimes que estão sendo analisados no presente trabalho, crimes cibernéticos, fica a indagação se a justiça apresenta condições de na prática dar uma resposta satisfatória às vítimas desse tipo de violação.

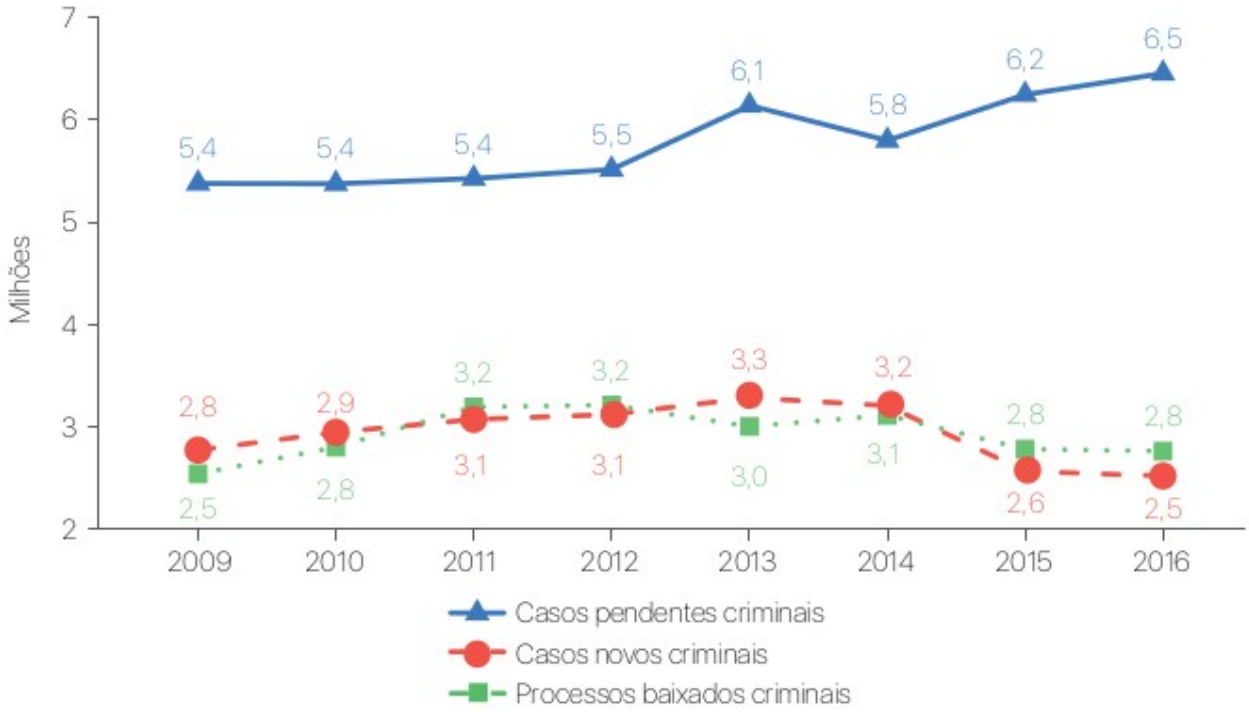


Figura 2: Estatística dos processos judiciários

O gráfico acima, extraído do site do Conselho Nacional de Justiça, demonstra que as estatísticas judiciárias não são das mais promissoras. Conforme se pode extrair das informações do gráfico, o número de casos criminais pendentes tem aumentado bastante, já somando a quantidade de 6,5 milhões no ano de 2016. Em outras palavras, o judiciário não vem tendo condições de dar vazão à quantidade enorme de processos criminais que vem surgindo, o que acaba gerando um certo descrédito em relação à justiça.

Isso porque ainda não foi analisada a percentagem de acordo com o tipo de crime, pois se verificaria que a maioria desses crimes estão ligados a crimes comuns como homicídios, tráfico, roubos, etc. No caso dos crimes virtuais essa estatística tende a ser ainda pior. Realmente de nada adianta a polícia ter sucesso nas investigações se o aparelho judiciário não tem a mínima condição de dar celeridade aos processos criminais envolvendo tais crimes.

O direito ao acesso à justiça é um tema muito discutido pelos no mundo jurídico desde que o Estado tomou para si o poder de resolver conflitos. Um dos maiores indagações sempre foi como garantir que todos, ou pelo menos o maior número possível de pessoas, a

oportunidade efetiva de posicionar-se diante do Poder Judiciário solicitando a tutela de seus interesses.

No Brasil, a inserção de direitos como o acesso à justiça e a razoável duração do processo como direitos fundamentais da Constituição foi um fator chave da importância da promoção dessa garantia básica. Entretanto, o Poder Judiciário brasileiro está em uma grande crise de efetividade, de tal modo que está muito difícil fornecer aos jurisdicionados a tutela adequada de seus interesses, o que acaba acarretando uma violação substancial do direito ao acesso à justiça.

Dentre os aspectos primordiais do acesso à justiça, temos a questão do tempo de duração do processo, pois o Estado, além de possibilitar que o assistido ingresse na justiça, deve preocupar-se também com a saída da jurisdição, devido às dificuldades de obtenção de respostas judiciais em tempo hábil.

A possibilidade de se obter a tutela jurisdicional em tempo razoável identifica-se na maior parte com a efetividade do processo. A demora judicial é uma das principais causas de descrédito do Judiciário. As pessoas que buscam a tutela da justiça se sentem desprestigiados e com uma sensação de injustiça (BARCELLOS, 2008, p. 02).

Fica o questionamento se a justiça é realmente direito de todos, ou se apenas uma parcela privilegiada da sociedade pode de fato ter acesso a mesma, independentemente de poder aquisitivo ou possibilidade de formação de opinião. A maioria das pessoas não tem a sorte do ator Bruno Gagliasso e da atriz Thaís Araújo em terem rápidas respostas em relação aos seus processos criminais.

Essa dificuldade que as pessoas tem em relação ao acesso à justiça acaba sendo a causa de outro fenômeno chamado cifra negra ou criminalidade oculta. O conceito de criminalidade oculta foi elaborado pelo estudioso belga Lambert Adolphe Jacques Quételet, que em seu trabalho, estabeleceu o conceito de “homem médio” como um tipo ideal e abstrato de sujeito.

Quételet acreditava que a criminalidade poderia ser representada por uma função matemática relacionada com os estados econômicos e sociais, tendo tal autor alertado inclusive para a questão dos crimes não comunicados ao Poder Público. Interessante observar a tendência positivista desses estudos, procurando regras exatas em fenômenos sociais.

Embora a criminalidade possa ter influências e poder ser explicada até certo ângulo de vista por essa teoria, ainda assim é algo mais complexo e difícil de mensurar. Já a questão da cifra oculta representa algo que gera reflexão acerca da diferença entre a criminalidade real e a criminalidade aparente. Existe de fato uma distância entre os crimes cometidos no dia a dia, e os crimes que chegam a ser noticiados às autoridades competentes.

Normalmente são lembrados de três métodos para se verificar a grandeza da delinquência oculta. O primeiro é o da autoconfissão, que consiste na realização de pesquisas anônimas para se conhecer quantas pessoas realizaram atos delituosos em um determinado período de tempo. O segundo método é o da vitimização, na qual se busca analisar o número de pessoas que foram vítimas em um certo período de tempo. Já no terceiro método há um estudo da relação de entrada e saída de processos nos sistemas de controle formal, ou seja nos tribunais e na polícia (SHECAIRA, 2014, p. 72). Apesar de esses métodos não serem exatos, já são um bom passo para a busca de dados mais seguros que ofereçam uma noção da criminalidade oculta.

No caso dos crimes cibernéticos tal estatística oculta tende a ser bem maior devido o fato de a vítima desse tipo de crime passar por três processos de vitimização. O primeiro ocorre pelos prejuízos diretos advindos da prática do delito, a exemplo de perdas financeiras. O segundo processo de vitimização ocorre quando a vítima não é bem tratada nas instituições formais ou quando o seu processo não tem o devido prosseguimento nas instituições oficiais. Por último, a vítima ainda sofre com a reprovação da sociedade que consistem em julgamentos por ter facilitado a ação do criminoso. Tudo isso acaba por facilitar ainda mais a vida do criminoso pela sensação de impunidade, além de que dados estatísticos irreais acabam por camuflar a necessidade urgente de o Estado investir no combate a esses tipos de delitos.

4.4 Crimes mais Comuns e Jurisprudência

A seguir será analisada algumas jurisprudências dos crimes mais comuns relacionados com os dispositivos informáticos. Analisaremos a figura do estupro virtual, pornografia de vingança, estelionato, furto virtual, racismo, e pedofilia. Por último será destacado o crime de invasão de dispositivo informático, delito esse configurado como crime cibernético próprio. Algumas jurisprudências servirão para destacar a necessidade de tipificação de delitos

virtuais, além da tentativa de utilização da legislação penal atual, por mais inadequada que ainda seja.

4.4.1 - Estupro Virtual

Não é necessário para a configuração do crime de estupro que o autor e a vítima mantenham contato físico. Há inclusive uma decisão judicial nesse sentido do Superior Tribunal de Justiça, no Habeas Corpus RHC 70976/MS, em que uma criança foi levada por cafetinas a um motel, onde a despiram e a expuseram nua a um homem que havia pago pelo encontro para contemplar com lascívia a criança sem roupas. O homem foi denunciado pelo crime de estupro de vulnerável – art. 217-A do Código Penal- onde a defesa alegou a possibilidade do crime pela inexistência de contato físico.

O relator Joel Ilan Paciornik negou seguimento a esse recurso por desconsiderar a necessidade desse contato físico com o agressor, pois para ele a dignidade não se ofende apenas com lesões de natureza física, e que a maior ou menor gravidade do fato deveria afetar a questão da dosimetria da pena. Essa desnecessidade de contato físico é o que justifica a possibilidade de prática desse crime pela internet.

De acordo com o artigo 213 do CPB o crime de estupro se concretiza quando o autor constrange a vítima mediante violência ou grave ameaça, a ter conjunção carnal, ou praticar ato libidinoso diverso da conjunção carnal, ou permitir que com ela seja praticado outro ato libidinoso. Assim, na situação em que o autor ameaça divulgar vídeo íntimo da vítima, e a constrange via internet, a se masturbar ou introduzir objetos em seus órgãos genitais, mediante grave ameaça, se configuraria o ato libidinoso diverso da conjunção carnal, e consequentemente o estupro virtual.

Há quem questione se realmente tal situação configuraria uma grave ameaça? Existem parâmetros para se entender a existência dessa grave ameaça. No Recurso Especial REsp 1.299.021-SP, o STJ considerou que a ameaça de causar um “mal espiritual” contra a vítima pode ser considerada como “grave ameaça” para fins de configuração do crime de extorsão.

Também no REsp 1.207.155, o STJ decidiu que a promessa de destruir bem da vítima

configura “grave ameaça” para fins de extorsão. Nesse último caso o ministro Nelson Hungria considerou que todo bem ou interesse cujo sacrifício represente, para o respectivo titular, um mal maior que o prejuízo patrimonial, correspondente à vantagem exigida pelo criminoso que comete extorsão. Tais situações levam a conclusão de que a ameaça de difusão de vídeos que causem constrangimento à vítima podem configurar a grave ameaça.

Há inclusive precedente de 2005, no Habeas Corpus HC 85.674-8, em que o Supremo Tribunal Federal apreciou o caso de um homem que, de posse de uma fita de vídeo que mostrava uma jovem de 16 anos tendo relação sexual com o namorado, a estuprou sob a ameaça de divulgação da gravação . Nesse caso, o relator ministro Joaquim Barbosa considerou que houve o emprego da grave ameaça.

Houve um caso no Piauí de um homem que teve um relacionamento de cinco anos com a vítima, ter realizado algumas imagens com ela nua. Após o fim do namoro o mesmo passou a ameaçá-la afirmando que enviaria tais fotos caso ela não enviasse novas imagens. Após algumas investigações houve a decretação da prisão preventiva desse indivíduo por trinta dias, sendo esse o primeiro caso de prisão no país. Nessa situação, o juiz Luiz de Moura entendeu existir o crime de estupro virtual, cometido em autoria mediata ou indireta, pois a ofendida, mediante coação moral irresistível, foi obrigada a realizar tal ato libidinoso.

4.4.2 Pornografia de Vingança

A sensação de anonimato proporcionado pela internet pode funcionar muito bem como um incentivo para certos tipos de condutas, o que é um argumento para que as leis realmente tenham um alcance para certos atos como a pornografia de vingança. Essa espécie de afronta pode ser considerada uma lacuna jurídica a ser preenchida, pois atualmente não há previsão legal para esse delito. A estratégia utilizada atualmente pelos juízes é a utilização da punição prevista no capítulo V do código penal brasileiro para os crimes contra a honra.

Hoje devemos levar em conta que a Internet não esquece certos fatos publicados. Ao contrário de mídias impressas de antigamente, cujas edições se perdiam sujeitas ao desgaste dos suportes físicos, as informações publicadas na rede mundial de computadores circulam indefinidamente, sendo muito difícil controlar a sua disseminação. Muito complicada a

situação de uma pessoa que acaba por ser perseguida pelo resto de sua vida pela prática de atos pretéritos.

Nos crimes de divulgação de conteúdo sexual sem a autorização da vítima fica a dúvida se os atuais tipos penais com injúria e difamação realmente são eficazes para o combate a esse tipo de delito. Devido ao crescimento dos relacionamentos em redes sociais, comumente tem surgido casos de fotos e vídeos íntimos em redes sociais e aplicativos como Whatsapp e Facebook. Ao que parece as penas previstas para o autor dessas condutas são relativamente brandas para o causador do dano, isso porque o prejuízo causado à vítima é imensurável.

Há a necessidade de um tipo penal específico para punir de forma mais severa tais condutas quando comparadas ao grave prejuízo sofrido pela vítima, e talvez, por assim ser, não inibem a prática do delito, até mesmo porque nem mesmo a indenização cível tem inibido esses tipos de crimes.

Há o caso da jovem de 12 anos Saori Teixeira, que se deparou com fotos íntimas nas paredes da sua escola quando chegava na mesma para estudar. Essas imagens tinham sido enviadas a um garoto que possuía 17 anos, com o qual havia se envolvido. Devido esse fato a criança teve que aguentar as fofocas dos colegas, além de ter sido expulsa do colégio e apanhado dos pais. O garoto ainda ameaçou disseminar mais ainda tais fotos íntimas caso a mesma se recusasse a fazer sexo com ele. Com a repercussão do caso a vida do jovem se tornou muito difícil, tendo a mesma se afastado dos estudos por dois anos, tendo não saído mais de casa, o que ocasionou depressão e uma tentativa de suicídio. Suas fotos foram para no Facebook e em outros sites de pornografia, sendo que mesmo após a solicitação de retirada do material, ainda é possível encontrar fotos compartilhadas. O garoto que realizou tal conduta permanece sem punição.

Esse caso é mais um exemplo de o quanto os crimes de informática podem ser prejudiciais, e o quanto os crimes contra a honra previstos no código penal são insuficientes para a repressão de tais crimes, ainda mais ao se tratar de menores infratores. Dessa forma, a vítima de tal tipo de conduta acaba se tornando mais uma das pessoas que não encontram apoio na legislação, sendo vitimizadas também pela própria sociedade.

4.4.3 Estelionato e Furto Virtual

O crime de estelionato praticado na Internet encontra amparo no artigo 171 do Código Penal Brasileiro. Tal delito, também conhecido com estelionato eletrônico ou virtual, é um tipo de crime no qual o agente se utiliza de um meio de comunicação eletrônico, como a Internet, para atingir o seu objetivo de obter para si ou outrem vantagem patrimonial ilícita, induzindo ou mantendo a vítima em erro.

Esse tipo de crime pode ser cometido tanto por especialista em informática quanto por um leigo que tenha o mínimo de conhecimentos sobre dispositivos computacionais. Uma das formas de se cometer esse tipo de crime é através da transferência de valores via Internet realizada por vítimas para a conta do criminoso, quando as mesmas são enganadas através de páginas falsas de bancos oficiais, por exemplo.

Há a possibilidade de prática de estelionato também através de mensagem eletrônicas enviadas por e-mail na qual se convidam vítimas a depositarem uma certa quantia em dinheiro para participação em correntes de sorte, com a ideia de que isso lhes renderá muito dinheiro.

O Supremo Tribunal Federal, em julgamento da Extradição 1.029/Portugal, entendeu ser correspondente o crime de burla informática, tipificado no código penal português, com o crime de estelionato previsto no Código Penal Brasileiro. O pedido de extradição foi parcialmente deferido devido à ausência de previsão no sistema jurídico brasileiro de crime correspondente ao delito de falsidade informática.

Interessante observar que o entendimento acerca do estelionato virtual vem sendo modificado. O Supremo Tribunal de Justiça, através do agravo regimental CC 74.255-SP entende que o saque fraudulento realizado em conta corrente da Caixa Econômica Federal configura o delito de furto mediante fraude, e não o de estelionato. Na fraude de furto, haveria a redução da vigilância da vítima para que ela não compreenda estar tendo seu patrimônio subtraído. Já no estelionato o criminoso procura deixar a vítima em erro para com isso ela o entregue o bem de forma espontânea.

No julgamento do conflito de competência 67.343-GO, o STJ afirma que embora os valores recebidos e transferidos por meio de manipulação de dados digitais não sejam tangíveis, nem por isso deixam de ser dinheiro. Assim , o bem mesmo de forma virtual circula como qualquer outra coisa de valor econômico, sendo possível o crime de furto por meio de sistema informático.

É um dos tipos de conduta criminosa mais comum na Internet, já tendo gerado

prejuízos a várias pessoas. Está muito associado ao delito de *phishing scam*, ou página falsa, na qual o agente cria páginas falsas de instituições financeiras e fazem com que os indivíduos acessem essa página, e com o engano gerado pela suposta confiabilidade do site, acabem fornecendo suas credenciais de acesso, o que pode acabar culminando em prejuízos econômicos.

Através do julgamento do Habeas Corpus 124.419-PA, o STJ defendeu a imposição de penas-base acima do mínimo legal para os crimes de furto qualificado e quadrilha, para delito de subtração de contas bancárias realizadas através da rede mundial de computadores. Na decisão foi registrada a posição estratégica do paciente, que possuía alto conhecimento de informática, além de atuar por intermédio de organização criminosa “no recesso do lar, sem alarde, e de forma insidiosa”.

4.4.4 Racismo na Internet

Um crime que vem crescendo nos dias atuais, e que desafia a atividade policial devido à grande quantidade, são os crimes de racismo e injúria racial, cometidos através da *internet*. Ofensas de racismo e injúria racial, protagonizadas por pessoas que incitam preconceitos de raça, cor, etnia, religião ou origem, ocorrem diariamente em todo país. Chama a atenção o fato desses crimes terem se perpetuado na *internet*, com trocas de informações depreciativas, que deixam evidentes as marcas de um passado de discriminação. São comentários feitos em postagens de fotos, que divulgam também endereços de sites racistas e fazem intercâmbio com símbolos nazistas.

Como exemplo de um caso de repercussão nacional temos a ofensa direcionada à filha adotiva dos atores Bruno Gagliasso e Giovanna Ewbank. Após a denúncia realizada pelos pais da vítima, foi descoberto que uma adolescente de 14 anos foi responsável pelas ofensas raciais. A menina afirma ter criado um perfil falso em uma rede social utilizando o nome e as fotos de uma amiga, e que fez tudo isso para “zoar” sua amiga, tendo escolhido a filha do casal aleatoriamente. Merece destaque a rapidez com a qual tal denúncia foi apurada.

Causa espanto a falta de sensibilidade que algumas pessoas terem ao acessarem o ambiente virtual, tendo ímpeto de cometer condutas que dificilmente fariam sem o anonimato proporcionado pela Internet. Muito comuns também vários casos de racismo cometidos contra os nordestinos através das redes sociais, principalmente em períodos eleitorais.

Há um projeto de lei, o PLS 80/2016, que procura prever pena de prisão para os indivíduos que cometerem racismo e discriminação pela internet, inclusive para aqueles que passarem tais mensagens racistas adiante. Na justificativa desse projeto se alega que a internet tem se tornado para muitos um território livre, de modo a ser usada como cenário para manifestação de discriminações e preconceitos variados, facilitado pelo fato da ausência de confronto físico.

Em entendimento unânime da 1ª Turma do Tribunal do Tribunal Regional Federal da 3ª Região, foi negado recurso do Ministério Público Federal que pretendia invalidar decisão da 2ª Vara Federal de Dourados (MS). Na decisão, o juiz se declarou incapaz de julgar processo sobre crime de preconceito racial contra a etnia Guarani-Kaiowá por parte de colunista do site do jornal “O Tempo” por preconceito racial praticado na internet. O MPF interpôs recurso alegando que se deveria aplicar a teoria do resultado, de tal modo que a competência para julgar deveria ser no local onde o crime foi consumado. é crime independente do conhecimento por parte de quem é ofendido.

A 1ª Turma do TRF-3ª Região entendeu que não se pode confundir crime de preconceito racial com o crime de injúria racial, que se consuma quando a ofensa é conhecida pela vítima. Portanto, o conteúdo preconceituoso se estabelece no momento em que é publicado, sendo irrelevante o conhecimento do conteúdo ofensivo pelos grupos atacados. Assim, a ação judicial deve correr no local onde está instalado o servidor do site que publicou as ofensas. Isso deve facilitar até a investigação criminal devido à proximidade do servidor.

4.4.5 Pedofilia na Internet

Nos últimos anos o crime de “pedofilia” tem avançado junto com a tecnologia. Os pedófilos aproveitam-se criando perfis falsos em redes sociais, e utilizando de linguagem de fácil entendimento para conseguirem a confiança das crianças e adolescentes. O Estatuto da Criança e do adolescente (ECA), através do princípio da proteção integral visa defender a criança e o adolescente de atos abusivos à sua integridade, independentemente do meio utilizado para prática da conduta criminosa.

O art. 241 do ECA proíbe apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo

criança ou adolescente, estabelecendo uma punição de detenção de 2 a 6 anos e multa. Apesar de tal previsão esse tipo de crime continua a crescer. Um dos fatores que contribuem para isso é a falta de cultura digital, e até mesmo devido a um acompanhamento familiar falho.

A pedofilia é uma manifestação e prática do desejo sexual que alguns adultos ou outros menores desenvolvem em relação a criança de ambos os sexos na pré-puberdade. Em decisão referente ao Acórdão HC 2.121-CE, a segunda turma do Tribunal Regional Federal da 5ª Região considera a divulgação de fotos pornográficas de menores na Internet crime previsto em convenção internacional, o que acaba atraindo a competência da Justiça Federal.

No julgamento do Acórdão ACR 6.380-CE, referente à prisão de um indivíduo em sua residência, no momento em que foi constatada a transmissão de imagens pornográficas envolvendo crianças pela Internet, o tribunal entendeu que o fato de o apelante se encontrar sozinho no momento da prisão não descaracteriza o delito do art.241, pois basta o computador estar online para que o compartilhador de arquivos EMULE transmitisse imagens e vídeos envolvendo pornografia infantil para o mundo inteiro. Nesse caso o réu foi condenado a oito anos de Reclusão. Importante observar que o crime de pedofilia é um dos poucos delitos cometido por meios virtuais que tem uma legislação proporcional à gravidade do delito.

4.4.6 - INVASÃO DISPOSITIVO INFORMÁTICO

Atualmente o ordenamento jurídico apresenta a norma do artigo 154-A que trouxe o denominado crime de “invasão informática”. Consiste na conduta de 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, cominando a este delito a pena de detenção, de 3 (três) meses a 1 (um) ano e multa. É um crime cibernético próprio, o que significa que há a necessidade do dispositivo computacional para configuração do delito.

Importante observar que o STF já negou prisão preventiva para extradição, no PPE 732 do Distrito Federal, de um indivíduo que cometeu o delito de invasão de dispositivo informático devido a inexistência na época de legislação correspondente no Brasil. Atualmente com a Lei Carolina Dieckman já é possível a condenação desse tipo de crime. O que se pode observar é que dificilmente se punirá tal tipo de crime, até mesmo porque

geralmente a invasão de dispositivo acaba sendo absorvida por um crime mais grave como furto qualificado, por exemplo, o que faz com que tal invasão influencie mais na dosagem penal. Dificilmente se pune apenas tal dispositivo, até mesmo porque geralmente se percebe a invasão quando se advêm delitos mais graves, sem falar da penalidade pífia desse tipo de conduta.

5. CONSIDERAÇÕES FINAIS

As novas tecnologias estão impulsionando o processo de globalização, e os avanços da computação estão fazendo surgir uma nova era onde os dispositivos computacionais se tornam indispensáveis para grande parte das atividades do dia a dia, havendo, portanto, uma repercussão social, econômica, e política sem precedentes. A informação passou a se tornar um ponto vital em um cenário de acirrada competição mundial, sendo os mercados virtuais novas conquistas a serem exploradas.

A relativização do tempo e do espaço torna a rede mundial de computadores um diferencial para as mais diversas espécies de negócios, e até mesmo apresenta uma forte utilidade científico- acadêmica. Entretanto, a *internet* e seus recursos criam no ser humano a ideia de liberdade irrestrita, de modo que as pessoas se sentem protegidas pela possibilidade de anonimato proporcionada pela tecnologia. Todas essas facilidades, por outro lado, vem acompanhadas de uma nova forma de criminalidade denominada de crimes cibernéticos, devido ao fato de tais condutas delituosas envolverem uma nova modalidade espacial, o ciberespaço.

Na exposição dos conceitos acerca do que se entende por crimes cibernéticos ou virtuais, percebe-se uma série de nomenclaturas, além de uma certa controvérsia doutrinária acerca do que seriam esses crimes. Isso porque além da denominação desse delito não ser uníssona, há quem acredite que alguns crimes virtuais são condutas típicas, ilícitas, e culpáveis, que podem ser praticadas independentemente do uso de dispositivos informáticos. Outros estudiosos já acreditam que ainda há necessidade de tipificação desses delitos virtuais, o que demonstra a falta de amparo na legislação vigente.

Nesse trabalho aceita-se a ideia de que os delitos virtuais são aqueles que utilizam de dispositivos computacionais para a realização da conduta, e que embora necessitem de um tratamento legislativo especializado, ainda assim é valido o uso de tipos penais convencionais na falta da legislação específica. Entretanto, acredita-se na necessidade de leis voltadas para essa modalidade de crime devido as peculiaridades do mesmo .

A grande incidência de Crimes Cibernéticos vem exigindo uma atitude mais proativa das autoridades em respeito a todos os cidadãos que merecem ter sua segurança e boa-fé

defendida. Logicamente não podemos esquecer que o Direito Penal em respeito ao princípio da intervenção mínima deve ser a “última ratio” para a inibição desse tipo de delitos. Entretanto, o Estado não pode se afastar da sua responsabilidade perante os novos meios de interação social.

Perceptível o atraso que o direito tem em relação à tecnologia e a novos campos sociais, até mesmo porque as normas jurídicas ainda possuem entre uma das suas maiores características sua utilização como mecanismo que visa manter o “status quo” ou a estabilidade social. Natural, portanto, o atraso do Direito na normatização dos crimes cibernéticos. O que não se pode aceitar é uma reação acentuadamente atrasada para lidar com esse novo paradigma tecnológico.

O ordenamento jurídico brasileiro necessita de mudanças com o objetivo de tentar deter a prática desses crimes que cada dia crescem mais sem que haja punição adequada. Uma legislação voltada para os crimes da *internet* é uma solução que além de evitar lacunas na lei, facilita para que as pessoas envolvidas na apuração desses delitos consigam obter informações de forma rápida e eficaz.

Outro problema encontrado está relacionado com a omissão da legislação penal quanto ao tipo penal da invasão de sistema de informático, no caso de o invasor não objetivar fins ilícitos, de modo que o mesmo não poderá vir a ser alcançado pela esfera penal, o que acaba por ficar a questão apenas para o direito civil.

É uma tarefa a limitação do seu território dos delitos informáticos, e e além disso tem a problemática do anonimato oferecido pelas interfaces computacionais. A falta de conhecimento e treinamento por parte das autoridades investigativas também é um fator que dificulta sobremaneira a prisão desses cibercriminosos, que cada vez mais se multiplicam ao redor do globo.

Conclui-se que além de a legislação sobre cibernéticos ainda não ser suficiente, ainda existe a dificuldade quanto à investigação criminal no Brasil, que não apresenta resultados eficientes, o que demonstra o despreparo das estruturas das instituições penais para o combate ao delito virtual. Favorece a prática desses atos ilícitos a falta de estrutura dos órgãos policiais e a precariedade da regulamentação.

Os investigadores se deparam com uma série de dificuldades como a demora na concessão dos mandados judiciais, das perícias, da dificuldade em terem atendidas solicitações de alguns provedores de acesso e conteúdo. Há carência de condições mínimas para a persecução penal.

A atribuição no Brasil para a apuração das infrações cibernéticas pertence à Polícia Federal e às policias civis dos Estados e do Distrito Federal. A peça chave para o registro das investigações é o inquérito policial, instrumento esse que deve seguir as normas do Código de Processo Penal brasileiro.

A Polícia Federal deve atuar nos crimes de sua competência, a maioria que afete os interesses da União, e como possui melhores condições estruturais acaba por apresentar uma melhor atuação com inteligência. Já as policias civis, com exceção de algumas delegacias concentradas nos crimes virtuais, não reúnem condições para as investigações dos crimes cibernéticos devido à falta de agentes capacitados e equipamentos, sobrecarga de serviço, desvios de função (muitos investigadores exercem papel de agente penitenciário), além da falta de unidades especializadas, e falta de integração internacional.

Os crimes virtuais acontecem todos os dias no Brasil, e na grande maioria das vezes é difícil localizar o criminoso. Além de identificar o infrator há também a preocupação em fazer com que as provas obtidas sejam legítimas para embasar uma futura decisão judicial. A perícia deve trabalhar em conjunto com a investigação criminal para auxiliar a investigar de maneira detalhada do caso e da autoria, causas, e circunstâncias do delito.

Para que o inquérito policial apresente a robustez necessária para a denúncia oferecida pelo Ministério Público ou demais legitimados, as provas periciais são essenciais para justificar uma condenação justa. A perícia funciona assim como auxiliar da justiça na busca da verdade real no processo criminal, sendo peça chave para o deslinde de um processo criminal.

A Perícia Forense Computacional é uma área da Criminalística que envolve a coleta de evidências digitais em dispositivos computacionais envolvidos em ilícitos e crimes. Para lidar com essas tecnologias digitais as técnicas forenses necessitam ser apuradas por profissionais capacitados, a fim de se realizar uma investigação de qualidade, relatando satisfatoriamente a autoria, a dinâmica, e a materialidade dos fatos.

A situação da perícia criminal no Brasil é crítica devido a falta de equipamentos para a realização das investigações e a dificuldade dos peritos criminais, que acabam por ter que realizar o seu trabalho sem o mínimo de suporte. Isso acaba por causar acúmulo de inquéritos e muitos crimes cibernéticos ficam sem solução, e consequentemente as vítimas ficam sem a devida assistência. Além disso o número de profissionais é insuficiente para o crescente número de delitos da *internet*.

O Estado brasileiro deve buscar uma interação maior com outros países na busca de um canal mais rápido e menos burocrático para o levantamento de informações que ajudem na investigação de crimes que superam as fronteiras internacionais. Em um cenário globalizado como o atual, não se justifica o atraso brasileiro em aderir a Convenções e Tratados como a Convenção de Budapeste, que busca dar uma resposta ao crescimento gritante dos delitos virtuais.

Mecanismos de colaboração policial devem ser uma alternativa analisada com critério para que exista uma ponderação entre os valores da intimidade e da segurança das pessoas. Um procedimento muito burocrático mais atrapalha do que auxilia no combate a esse tipo de crime, mas uma invasão injustificada da privacidade das pessoas contrasta fortemente com os ideais de um Estado constitucional de direito que tem em sua Constituição um mecanismo de defesa essencial dos cidadãos contra as possíveis arbitrariedades do Estado.

Observa-se também que a pena aplicada a essa modalidade de crime ainda é muito branda, visto que no Brasil existe a possibilidade de modificação das penas de até quatro anos de reclusão por penas de restrição de direitos, o que não serve de efeito inibitório para esse tipo de crime, o que acaba ajudando a aumentar a sensação de impunidade. A pena não precisa ser desrespeitosa em relação à dignidade humana, podendo inclusive ter um efeito econômico mais forte até do que a restrição de liberdade e interdição de direitos.

Foi criticado também a diferenciação no acesso à justiça, na qual as pessoa famosas e de melhor influência tem respostas judiciais mais rápidas que a grande maioria das vítimas. Como o acesso à um processo célere é um direito de todos, questiona-se a morosidade com que o judiciário tem lidado com os seus processos, ainda mais no caso de delitos virtuais, no qual o fator temporal é bastante crítico..

À medida que as pessoas observarem uma atuação mais eficaz da polícia judiciária, um maior número de boletins de ocorrência pode surgir, diminuindo a chamada “cifra

negra”, o que acaba por oferecer uma medida real do número de incidentes e ameaças relacionados com crimes informáticos. Deste modo cria-se uma cultura que fornece subsídios para que a análise criminal auxilie na criação de melhores políticas para lidar com esse tipo de criminalidade.

A *internet* pode e deve ser vista não apenas como uma tecnologia a ser utilizada com parcimônia e cuidado, mas como um importante mecanismo para o combate aos Crimes transnacionais que cada vez mais utilizam a tecnologia como forma de facilitar a interação de grupos criminosos a nível globalizado.

Apesar de normalmente o criminoso estar a um passo à frente da justiça e da polícia na questão criminal devido ao fato dos mesmos não apresentarem uma “bola de cristal”, atitudes proativas devem ser um dos diferenciais que possibilitem uma resposta do Estado que realmente iniba condutas cibercriminosas.

Para que se haja eficiência no combate aos crimes cibernéticos é necessário maior comprometimento quanto à criação de leis penais mais efetivas, na realização de acordos internacionais para cooperação, além de investir nas policias investigativas e perícias científicas, de forma a melhorar as condições e investir em estruturas, equipamentos, treinamento, e inclusive ter a iniciativa de criação de núcleos de combate aos crimes virtuais em cada estado.

Como trabalhos futuros planeja-se aprimorar os estudos acerca das cooperações internacionais, além de analisar a questão da concorrência entre a liberdade na utilização desse meio virtual, e da relação desse direito com a possível necessidade de controle do Estado em casos que envolvem a criminalidade cibernética .

REFERÊNCIAS BIBLIOGRÁFICAS E WEBIOGRÁFICAS

ABREU, Karen Cristina Kraemer. "História e usos da Internet." *Biblioteca on-line de Ciências da Comunicação, 2009. Universidade da Beira Interior. Covilhã* . Disponível em:<http://www.bocc.ubi.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf>. Acesso em: 29 de agosto.2017.(2009).

ABREU, Leandro Farias dos . A Segurança das Informações nas Redes Sociais. Disponível em: <http://www.fatecsp.br/dti/tcc/tcc0023.pdf> Acesso em: 18 de setembro.2017.

ADACHI, Tomi. Comitê Gestor da Internet no Brasil (CGI. br): uma evolução do sistema de informação nacional moldada socialmente. Tese de Doutorado. Universidade de São Paulo, 2009.

AGARWALL, Nidhi; **KASUHIK,** Dr Neeraj. Cybercrimes against women. Disponível em: <http://www.publishingindia.com/GetBrochure.aspx?query=UERGQnJvY2h1cmVzfC8yMjE3LnBkZnwvMjIxNy5wZGY=>. Acesso em 11 de setembro de 2017.

ALBUQUERQUE, Cândido. Polícia Civil. Povo, Ceará, 02 09.2014. Jornal de Hoje. Disponível em: <https://www20.opovo.com.br/app/opovo/opiniao/2014/09/02/noticiasjornalopiniao,3307828/policia-civil.shtml>. Acesso em: 15 set. 2017.

ALBUQUERQUE, Cândido. Segurança. 2014 Disponível em:<*http://www.direito.ufc.br/index.php?option=com_content&task=view&id=559&Itemid=65*> Acesso em: 25 de setembro.2017.

ALMEIDA, Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais, 2011. Trabalho de Conclusão de Curso (Tecnólogo em processamento de dados)- Faculdade de Tecnologia de São Paulo. Disponível em:<*http://www.fatecsp.br/dti/tcc/tcc0035.pdf*> Acesso em: 30 de setembro.2017.

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

AYRES, Nathalia Rodrigues da Cunha Penido. A Preservação do Local do Crime e a Atuação dos órgãos de Segurança Pública no Distrito Federal: Um Estudo em Campo. 2015. Disponível em:<*http://www.repositorio.uniceub.br/bitstream/235/8441/1/21135520.pdf*> Acesso em: 30 de setembro.2017.

BARCELLOS, Bruno Lima. A duração razoável do processo, 2008. Trabalho de Conclusão de Curso (Especialização Direito Processual)- Universidade da Amazônia. Disponível em:<*http://www.defensoriapublica.mt.gov.br/portal/uploads/artigos %20juridicos/Art_Duracao_razoavel_processo.PDF*> Acesso em: 10 de outubro.2017.

BARROS, Marcos Antônio de. A Busca da Verdade no processo penal. São Paulo: Editora Revista dos Tribunais, 2002.

BECCARIA, Cesare. **Dos Delitos e das Penas:** São Paulo: Martin Claret, 2001.

BEZERRA, Clayton; **AGNOLETTO**, Giovani Celso. Breves Apontamentos sobre o uso da prova digital. Rio de Janeiro: Mallet, 2016.

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

BOCK, a.m. et al. Psicologias: uma introdução ao estudo da psicologia. São Paulo: saraiva, 2001

BUENO, Neide . Breves Considerações sobre os Crimes Eletrônicos e a Regulação da Internet (Marco Civil), 2013. Disponível em:<*http://riccipi.com.br/wp-content/uploads/2013/10/doutrina_01.pdf*> Acesso em: 10 de setembro.2017.

BRASIL. **Decreto-lei nº 2.848**, de 07 de dezembro de 1940 (Código Penal). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 14 set. 2017.

_____. **Lei nº 3.689**, de 03 de outubro de 1941 (Codigo de Processo Penal Brasileiro). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 14 set. 2017.

_____. **Lei nº 8.069**, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente). Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8069.htm>. Acesso em: 14 set. 2017.

BRASIL. **Decreto Lei 8.078**, de 11 de setembro de 1990 **(**Código de Defesa do Consumidor). Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 19 ago. 2017.

_____. **Decreto Lei 10.406**, de 10 de janeiro de 2002 (Código Civil Brasileiro). Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 19 ago. 2017.

_____.**Lei nº 10.446**, de 8 de maio de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10446.htm>. Acesso em: 14 set. 2017.

_____. **Lei nº 11.829**, de 25 de novembro de 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em: 14 set. 2017.

_____.**Lei nº 12.030**, de 17 de setembro de 2009. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12030.htm>. Acesso em: 14 set. 2017.

_____. **Lei nº 12.735**, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 14 set. 2017.

_____. **Lei nº 12.737**, de 30 de novembro de 2012 (Lei Carolina Dieckman). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 14 set. 2017.

_____. **Lei nº 12.965**, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 14 set. 2017.

_____. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 19 ago. 2017.

BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. Operacional Padrão em Perícia Criminal. Brasília, 2013.

CALDEIRA, Felipe Machado.A evolução histórica, filosófica e teórica da pena. Revista da EMERJ, Rio de Janeiro, nº45, v.12, 2009.Disponível:<http://www.emerj.rj.gov.br/revistaemerj_online/edicoes/revista45/Revista45_255.pdf> Acesso em: 29 de agosto.2017.

CARDOSO, Fábio Fettuccia . Brasil está atrasado em estratégia de combate aos crimes cibernéticos, 2015. Disponível em:<*https://fabiofettuccia.jusbrasil.com.br/noticias/180688777/brasil-esta-atrasado-em-estrategias-de-combate-a-crimes-ciberneticos*> Acesso em: 09 de setembro.2017.

CARNEIRO, A. G. Crimes Virtuais: Elementos Para uma Reflexão Sobre o Problema na Tipificação. In:Âmbito Jurídico, Rio Grande, 15, n. 99, abr. 2012. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=11529>. 18 de setembro.2017.

CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Rio de Janeiro: Brasport, 2014

CASTELLS, MANUEL. **A Sociedade em Rede. A Era da Informação: Economia, Sociedade e Cultura**. Vol. 1. Paz e Terra. São Paulo, 2000.

CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. Disponível em: <http://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf>. Acesso em 11 de setembro de 2017.

CASTRO, Luís Fernando Martins. Direito da Informática e do Ciberespaço, 2014. Disponível em:<http://noosfero.ucsal.br/articles/0006/4224/12.2-Castro-ARTIGO-Direito_do_Ciberespaco.pdf> Acesso em: 05 de setembro.2017.

CAVALCANTI, Rosângela Batista. Problemas e desafios da polícia civil: as percepções dos delegados. Rio de Janeiro: Centro Edelstein de Pesquisas Sociais, 2009.pp. 107-125.Disponível em:<*http://books.scielo.org/id/s7v75/pdf/sadek-9788579820144-05.pdf*> Acesso em: 30 de setembro.2017.

CERT.br. Cartilha de Segurança para Internet. Sao Paulo: Comite Gestor da Internet no Brasil, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 15 setembro. 2017.

CINTRA, Antônio Carlos de Araújo; **GRINOVER**, Ada Pellegrini; **DINAMARCO**, Cândido Rangel. Teoria Geral do Processo. 30.ed. São Paulo: Malheiros, 2014.

COBRA, Coriolano Nogueira. Manual de Investigação Policial. São Paulo: Sugestões Literárias, 1969

COIMBRA, Valdinei Cordeiro. Teoria da Pena. Disponível em:<https://www.conteudojuridico.com.br/pdf/cj028976.pdf> Acesso em: 29 de agosto.2017.

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

CORRÊA Júnior, Alceu; **SHECARIA**, Sérgio Salomão. Teoria da pena: finalidades, direito positivo, jurisprudência e outros estudos de ciência criminal.São Paulo: Editora Revista dos Tribunais, 2002.

COSTA, Marcelo Antônio Sampaio Lemos. Computação Forense. Campinas: Millenium, 2011.

DIMOULIS, Dimitri. Manual de introdução ao estudo do direito. São Paulo: Editora Revista dos Tribunais, 2011.

DUARTE, Henrique. O que são hijacker e como eles podem colocar o seu pc em risco, 2015. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2014/02/o-que-sao-hijackers-e-como-eles-podem-colocar-o-seu-pc-em-risco.html>. Acesso em: 15 setembro. 2017.

FERRARESI, José Meneghini. Investigação policial de homicídios: análise de métodos, técnicas e do procedimento policial. Revista Transdisciplinar de Ciências Penitenciárias, 524(1):51-71, Jan-Dez/2005

FERREIRA, Marcos. Defacement: Como evitar que o seu site seja acessado e alterado, 2012. Disponível em: <https://imasters.com.br/infra/seguranca/defacement-como-evitar-que-

seu-site-seja-acessado-e-alterado/?trace=1519021197&source=single>. Acesso em: 15 setembro. 2017.

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

FILHO, Fernando da Costa Tourinho. **Processo Penal.** 20.ed. São Paulo: Saraiva, 1998.

_____, Fernando da Costa Tourinho. Processo Penal 1. São Paulo: Saraiva, 2010

GIMINEZ, Emanuel Alberto Sperandio Garcia. Crimes Virtuais. Disponível em: <https://bdjur.stj.jus.br/jspui/bitstream/2011/64929/crimes_virtuais_gimenes.pdf>. Acesso em 12 de setembro de 2017.

GRECO, Rogério. Curso de Direito Penal: Parte Geral. Rio de Janeiro: Editora Impetus, 2014.

GUTIER, Murilo Sapia. Introdução ao Direito Internacional Público. 2009. (Desenvolvimento de material didático ou instrucional - APOSTILA).

HALDER, D.; **JAISHANKAR**, K.Cyber Crime and the Victimization of Women: Laws, Rights and Regulations. Premier reference resource. Igi Global, 2011, ISBN 9781609608309.

HUEBNER, EWA; **BEM**, DEREK; **BEM**, OSCAR; Computer Forensics – Past, Present And Future, 2007.

INSTITUTO DA DEFESA NACIONAL. Estratégia da Informação e Segurança no Ciberespaço. Lisboa, 2013. Disponível em:<http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf> Acesso em: 05 de setembro.2017.

JESUS, Damásio de. Direito penal, volume 1 : parte geral / Damásio de Jesus. — 32. ed. — São Paulo : Saraiva, 2011.

_____, Damásio E. de. Direito Penal. 29. ed. São Paulo: Saraiva, 2008. v. 1.

KOHN, Karen; **MORAES**, Claúdia Herte. **O impacto das novas tecnologias na sociedade: conceito e características da Sociedade da Informação e da Sociedade Digita**l. 2007. Disponível em:<http://www.intercom.org.br/papers/nacionais/2007/resumos/R1533-1.pdf>. Acesso em: 28 de abril.2017.

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

LAU, Marcelo. Análise das fraudes aplicadas sobre o Internet Banking, 2006. Trabalho de Dissertação de Mestrado do Curso (Mestrado em Engenharia)- Escola Politécnica da Universidade de São Paulo. Disponível em:<www.teses.usp.br/teses/disponiveis/3/3142/tde-19092006-164238/.../Dissertacao.pdf> Acesso em: 15 de setembro.2017.

LAUDON, K. C.; LAUDON, J. P. Sistemas de Informação Gerenciais. 9ª ed. São Paulo: Pearson Prentice Hall, 2010.

LEAVITT, N. Mobile Phones: The next frontier for Hackers?, 2005. Disponível em:<http://leavcom.com/pdf/Mobilecode.pdf> Acesso em: 01 de setembro.2017.

LEMOS, Ronaldo. Tecnologia e cultura. Rio de Janeiro: FGV, 2006

LENZA, Pedro. Direito Constitucional Esquematizado. São Paulo: Editora Saraiva, 2014.

LÉVY, Pierre. Cibercultura. 1 ed. São Paulo: 34, 1999.

LISBOA, Roberto Senise. Direito na Sociedade da Informação, 2016. Disponível em:<http://www.egov.ufsc.br/portal/conteudo/direito-na-sociedade-da-informa %C3%A7%C3%A3o> Acesso em: 03 de setembro.2017.

LISBOA, Cícero de Barros; **LOPES,** Gustavo Matias . Os Três Pilares do Marco Civil da Internet. . Disponível em:<*http://periodicoalethes.com.br/media/pdf/5/os-tres-pilares-do-marco-civil-da-interne.pdf*> Acesso em: 25 de setembro.2017.

LOVISON, Henrique Dalla Costa. Uma metodologia de análise de programas daninhos. 2012. Disponível em:<http://www.lume.ufrgs.br/bitstream/handle/10183/54141/000855650.pdf?...1> Acesso em: 31 de agosto.2017.

MACHADO, Jonathan. O que é um keylogger?, 2012. Disponível em: <https://www.tecmundo.com.br/spyware/1016-o-que-e-keylogger-.htm>. Acesso em: 15 setembro. 2017.

MAIA, Daniel. Criminalidade: A Culpa é de quem?. Povo, Ceará, 12 07.2017. Jornal de Hoje. Disponível em: <http://www.candidoalbuquerque.adv.br/artigo-assinado-por-dr-daniel-maia-para-o-jornal-o-povo-criminalidade-a-culpa-e-de-quem/>. Acesso em: 15 set. 2017.

MAIA, Daniel. Criminalidade: A culpa é de quem?. 2017. Disponível em:<*http://www.candidoalbuquerque.adv.br/artigo-assinado-por-dr-daniel-maia-para-o-jornal-o-povo-criminalidade-a-culpa-e-de-quem/*> Acesso em: 30 de setembro.2017.

MAIA, Francisco Silvio. Noções de Criminalística. 2007. (Desenvolvimento de material didático ou instrucional - Curso de Formação de Peritos Legistas).

MARTINS, Pablo Luis; **MELO,** Bruna Martins. Tecnologia e Sistemas de Informação e suas influências na Gestão e Contabilidade, 2012. Disponível em:<https://www.aedb.br/seget/arquivos/artigos12/28816533.pdf> Acesso em: 05 de setembro.2017.

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

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

MEDEIROS, T. A. D. de.Utilização do Linux como ferramanenta antivírus em redes corporativas . Dissertação (Mestrado) — Universidade Federal do Rio Grande do Norte, 2005. Disponível em:<https://repositorio.ufrn.br/jspui/bitstream/123456789/15445/1/TeobaldoADM.pdf> Acesso em: 01 de setembro.2017.

MENDES, Maria Eugênia Gonçalves; **VIEIRA**, Natália Borges. **Os Crimes Cibernéticos no Ordenamento Jurídico Brasileiro e a Necessidade de Legislação Específica**. s.d. Disponível em:<http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2>. Acesso em: 29 de abril.2017.

MIRANDA, Napoleão. Globalização, Soberania Nacional e Direito Internacional. Revista CEJ (Brasília), Brasília, v. 27, p. 86-94, 2004.

MITSHASHI, Roberto Akio. Segurança de Redes, 2011. Trabalho de Conclusão de Curso (Tecnólogo em Processamento de Dados)- Faculdade de Tecnologia de São Paulo. Disponível em:<*http://www.fatecsp.br/dti/tcc/tcc0017.pdf*> Acesso em: 15 de setembro.2017.

MORAES, Alexandre Fernandes de. Segurança em Redes: Fundamentos. Rio de Janeiro: Forense, 2011

NADER, Paulo. Introdução ao Estudo do Direito. 24 ed. Rio de Janeiro: Forense: 2004.

NETO, Claúdio Pereira de Souza; **SARMENTO**, Daniel . Direito Constitucional: Teoria, História, e Métodos de Trabalho. Belo Horizonte: Editora Fórum, 2013.

NETO, Lindolfo Pires. **Crimes Cibernéticos: Necessidade de uma Legislação Específica no Brasil**. Disponível em:<http://www.fespfaculdades.com.br/painel/uploads/arquivos/trabArquivo_11052010080523_LINFOLFO.pdf> Acesso em: 28 de abril.2017.

NOBRE, J. C. A.. **Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar**. Cadernos UniFOA , Volta Redonda, ano 2, nº. 5, dez. 2007. Disponível em:<http://web.unifoa.edu.br/cadernos/edicao/05/11.pdf> Acesso em: 28 de abril.2017.

OLIVEIRA, Flávio de Souza. Metodologias de Análise Forense para Ambientes Baseados em NTFS. 2001. Disponível em:<*http://www.lasca.ic.unicamp.br/paulo/papers/2001-SSI-flavio.oliveira-forense.ntfs.pdf*> Acesso em: 30 de setembro.2017.

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

OVERILL, R.E . Trends in Computer Crime", Journal of Financial Crime, Vol.6, nº2, pp. 157-162, 1998. Disponível em:<https://pdfs.semanticscholar.org/5268/1e2ddd58c0df308637bd4623c09d8b8144e2.pdf> Acesso em: 01 de setembro.2017.

PACHECO, Wilfredo Enrique Pires . Manual de Responsabilização Penal dos Hackers, Crackers, e Engenheiros Sociais. Disponível em: <http://s.conjur.com.br/dl/guia-crimes-digitais.pdf> Acesso em: 18 de setembro.2017.

PAIVA, Mário Antônio Lobato de. A Ciência do Direito Informático, 2011. Disponível em:<http://www.egov.ufsc.br/portal/sites/default/files/anexos/30390-31543-1-PB.pdf> Acesso em: 02 de setembro.2017.

PERRIN, Stephanie. O Cibercrime. Disponível em: <https://vecam.org/archives/article660.html>. Acesso em 11 de setembro de 2017.

PICON, Leila Cássia; **ANTUNES,** Solange; **DUARTE**, Isabel Cristina Brettas . O Papel do Direito na Sociedade da Era Informacional, 2013. Disponível em:<http://coral.ufsm.br/congressodireito/anais/2013/6-17.pdf> Acesso em: 04 de setembro.2017.

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

PINHEIRO, Emeline Piva . Crimes Virtuais: Uma análise da Criminalidade Informática e da Resposta Estatal, 2006. Trabalho de Conclusão de Curso (Direito)- Pontifícia Universidade Católica do Rio Grande do Sul. Disponível em:<*http://www.egov.ufsc.br/portal/sites/default/files/emeline.pdf*> Acesso em: 09 de setembro.2017.

PINHEIRO, José Maurício dos Santos. Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar, 2007. Disponível em:<*revistas.unifoa.edu.br/index.php/cadernos/article/download/885/790*> Acesso em: 02 de setembro.2017.

RABELLO, Eraldo. Curso de criminalística. Porto Alegre: sagra luzzatto,1996.

REALE, Miguel. Lições preliminares de direito. 27. ed. São Paulo: Saraiva, 2002.

REIS, Daniel. Criminalística: Manual Básico. 2013. Disponível em:<*http://albani-perito.blogspot.com.br/2013/04/criminalistica.html*> Acesso em: 30 de setembro.2017.

REIS, Maria Helena Junqueira. Computer Crimes. Belo Horizonte: Del Rey, 1997

RIBEIRO, Luiz Julião. Investigação Criminal: homicídio. Brasília: Fábrica do Livro, 2006.

ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004, p. 110.

SAGAN, Carl. O mundo assombrado pelos demônios. São Paulo: Cia das Letras, 1997. p. 39.

SANCHEZ, Bernardo Feijoo. A Legitimidade da Pena Estatal: Uma breve análise das teorias da pena. Florianópolis: Conceito, 2015

SANTOS, Loirto Alves dos; **CAMARGO**, Luiz Henrique Pires de . Vírus de Computador: Uma Abordagem do Código Polimórfico, 2013. Disponível em:<http://www.inf.ufpr.br/bmuller/TG/TG-LoirtoLuiz.pdf> Acesso em: 01 de setembro.2017.

SCOTTI, Gledson. Análise e comparação entre os tipos de ataques aos servidores do Brasil, 2005. Trabalho de Conclusão de Curso (MBA em Banco de Dados)- Universidade do Extremo Sul Catarinense. Disponível em:<http://www.bib.unesc.net/biblioteca/sumario/000028/0000280A.PDF> Acesso em: 15 de setembro.2017.

SCHMIDT, Guilherme. Crimes cibernéticos. Jusbrasil, 2014. Disponível em: < http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em: 11 set.2017.

SEGURADO, Rosemary. Política da Internet: A regulamentação do Ciberespaço, 2011. Disponível em:<https://www.revistas.usp.br/revusp/article/view/34011> Acesso em: 05 de setembro.2017.

SEGURADO, Rosemary; **LIMA**, Carolina Silva Mandú de; **AMENI**, Cauê S. Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. Disponível em: http://www.scielo.br/pdf/hcsm/2014nahead/0104-5970-hcsm-S0104-59702014005000015.pdf. Acesso em: 04 de setembro.2017.

SHECAIRA, Sérgio Salomão. Criminologia. 5. Ed. São Paulo: Revista dos Tribunais, 2013.

SHECAIRA, Sérgio Salomão; CORREA **JUNIOR**, Alceu. Teoria da Pena: Finalidades, direito positivo, jurisprudência e outros estudos de ciência criminal. São Paulo: Editora Revista dos Tribunais, 2002

SILVA, Ana Carolina Calado da . O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira, 2015. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/o-estudo-comparado-dos-crimes-cibern %C3%A9ticos-uma-abordagem-instrumentalista-constitucional> Acesso em: 19 de setembro.2017.

SILVA, Gilson Marques da; **LORENS,** Evandro Mário. Extração e Análise de dados em memória na Perícia Forense Computacional, 2009. Trabalho de Conclusão de Curso (Tecnólogo em processamento de dados)- Faculdade de Tecnologia de São Paulo. Disponível em:<*http://icofcs.org/2009/ICoFCS2009-PP03.pdf*> Acesso em: 30 de setembro.2017.

SILVA, Patrícia Santos da. Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

SILVA, Paulo Quintiliano da. Crimes Cibernéticos e seus Efeitos Internacionais. In: First International Conference on Forensic Computer Science, 2006. Proceeding of the International Conference of Forensic Computer Science. v. 1. p. 10-14.

SILVA, Tânia Ventura. Crimes Cibernéticos: A era da Informação traz ameaça para a sociedade, 2016. Disponível em:<http://www.conteudojuridico.com.br/artigo,crimes-ciberneticos-a-era-da-informacao-digital-traz-ameaca-para-sociedade,56091.html>. Acesso em: 31 de agosto.2017.

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

em:<https://semanaacademica.org.br/system/files/artigos/artigo_sobre_internet_corrigido_0.pdf> Acesso em: 03 de setembro.2017.

SILVEIRA, Fernanda. A Autonomia da Perícia Criminal Capixaba como ferramenta de mudança na segurança pública do Espírito Santo, 2015. Trabalho de Conclusão de Curso (Especialização em Criminologia)- Centro de Ensino Superior de Vitória. Disponível em:<*http://br.monografias.com/trabalhos-pdf/autonomia-pericia-criminal-capixaba-ferramenta/autonomia-pericia-criminal-capixaba-ferramenta.pdf*> Acesso em: 30 de setembro.2017.

SOUZA, Gills Lopes Macêdo; **PEREIRA**, Dalliana Vilar. A convenção de Budapeste e as leis brasileiras, 2009**.** Disponível em: <http://www.mpam.mp.br/images/stories/A_convencao_de_Budapeste_e_as_leis_brasileiras.pdf> Acesso em: 15 mar. 2012.

SOUZA, Rafael Pinto Marques de; **CABRAL**, Bruno Fontenele . Manual Prático de Polícia Judiciária. Salvador: Juspodivm, 2013

SPAFFORD, Eugene H. “Computer Viruses as Artificial Life.” Technical report, 1994. Disponível em:<http://people.scs.carleton.ca/~soma/biosec/readings/spafford-viruses.pdf> Acesso em: 01 de setembro.2017.

STARLLINGS, Willliam. Criptografia e Segurança de Redes. - São Paulo: Prentice Hall, 2008

STUMVOLL, Victor Paulo. Criminalística. Campinas: Millenium, 2014.

TAMEGA, Flávio. Hacker Inside Top Secret. Goiânia: Terra, 2003

TAVARES, Tarcísio Alves. Análises Iniciais e Críticas à Lei 12.737/2012- Lei Carolina Dieckmann, 2013. . Disponível em:<*http://www.unipac.br/site/bb/tcc/tcc-0463074a098a0f1e76f9ad1376e21e2b.pdf*> Acesso em: 25 de setembro.2017.

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

TERCEIRO, Cecilio da Fonseca Vieira Ramalho. O problema na tipificação penal dos crimes virtuais. Disponível em: <http://jus.uol.com.br/revista/texto/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais>. Acesso em: 17 jul. 2012.

TORRE, Marina Giantomassi della. Aspectos Processuais e Penais dos Crimes de Computador, 2009. Dissertação de Mestrado (Mestrado em Direito Processual Penal)- Pontifícia Universidade Católica de São Paulo. Disponível em:<*http://www.dominiopublico.gov.br/download/teste/arqs/cp090690.pdf*> Acesso em: 15 de setembro.2017.

UMBACH, Kenneth W. The Internet: A California Police Perspective. 1997. Disponível em:<http://www.library.ca.gov/CRB/97/02/97002a.pdf>. Acesso em: 31 de agosto.2017.

U.S. Department of Justice. National Institute of Justice. Computer Crime: Criminal Justice Resource Manual. 1989.

U.S. DEPARTMENT OF JUSTICE. Eletronic Crime Scene Investigation: A Guide for First Responders. 2ªed. Washington, 2008.

VECCHIA, Evandro Della. Perícia Digital: Da Investigação à Análise Forense. Campinas: Millenium, 2014.

VERSIANNI, José Augusto Campos. Cooperação Internacional na Investigação de Crimes Cibernéticos. Rio de Janeiro: Mallet, 2016.

VIANNA, Túlio Lima . Do Acesso Não Autorizado a Sistemas Computacionais: Fundamentos de Direito Penal Informático, 2001. Dissertação de Mestrado (Direito)- Universidade Federal de Minas Gerais. Disponível em:<*http://www.bibliotecadigital.ufmg.br/dspace/bitstream/handle/1843/BUOS-96MPWG/disserta__o_t_lio_lima_vianna.pdf?sequence=1*> Acesso em: 11 de setembro.2017.

VIANA, Tulio; **MACHADO**, Felipe. Crimes informáticos. Belo Horizonte: Fórum, 2013

WENDT, Emerson; **JORGE**, Higor Vinicius Nogueira. Crimes Cibernéticos: Ameaças e procedimentos de Investigação. Rio de Janeiro: Brasport, 2013.

ZAFFARONI, Eugenio Raúl; **PIERANGELI**, José Henrique.Manual de Direito Penal: parte geral**.** 4. ed. rev. São Paulo: Editora Revista dos Tribunais, 2002.