MECANISMOS DE COOPERAÇÃO INTERNACIONAL DE REPRESSÃO E COMBATE DOS CRIMES CIBERNÉTICOS

Jéssica Rodrigues Lopes

RESUMO

O presente estudo analisa a influência da globalização e do desenvolvimento tecnológico no surgimento dos crimes cibernéticos, apontando os impactos dessa incidência na atual sociedade do risco, bem como os instrumentos que vem sendo utilizados pelo Estado para minimizar a incidência dessa modalidade de crime. A internet trouxe diversos benefícios para a sociedade, porém, também fomentou o surgimento de novas formas de criminalidade, bem como a prática de crimes tradicionais com a aplicação de avançadas técnicas informacionais disponíveis. Em decorrência da natureza transnacional dos cibercrimes, torna-se mais difícil a instrução e a persecução penal, tendo em vista diversidade legislativa, a soberania dos Estados na aplicação do *jus puniendi,* a falta de capacitação dos envolvidos na persecução penal, a dificuldade na identificação da autoria, entre outros. Diante disso, a cooperação internacional penal e a harmonização legislativa são mecanismos essenciais para reprimir os delitos informáticos. A Convenção sobre o cibercrime, também chamada de Convenção de Budapeste foi a primeira convenção a tratar sobre os crimes cibernéticos e representa uma ferramenta para combater a criminalidade supranacional. Para essa finalidade foi utilizado o método de abordagem dedutivo, prosseguindo da análise da regra geral, referente aos efeitos da globalização sobre os crimes cibernéticos e suas problemáticas, para a situação mais específica, isto é, de verificar e pontuar quais os mecanismos utilizados atualmente para coibir e reprimir os crimes cibernéticos no Brasil e no mundo, frente às dificuldades enfrentadas, e de apresentar melhores soluções de aplicação. Utilizou-se o tipo de procedimento de análise textual e de conteúdo, com abordagem teórica e legal baseada em pesquisas bibliográficas e documentais, acerca da interferência da globalização no direito penal, na tratativa do crimes informáticos como um fenômeno jurídico, bem como as formas de se obter uma cooperação internacional para combater o crime cibernético. A pesquisa bibliográfica foi baseada no levantamento de doutrinas, periódicos, artigos científicos e teses obtidas tanto em bibliotecas e livrarias quanto em acervos digitais na Internet, e efetuou-se pesquisa documental em legislação nacional.

Palavras-chave: Globalização. Crime Cibernético. Cooperação Penal Internacional.

RESUMEN

El presente estudio analiza la influencia de la globalización y el desarrollo tecnológico en el surgimiento de los delitos cibernéticos, señalando los impactos de esta incidencia sobre la actual sociedad de riesgo y las herramientas que están siendo utilizadas por el Estado para minimizar la incidencia de esta modalidad de delito. La Internet ha traído muchos beneficios a la sociedad, sino también fomentado el surgimiento de nuevas formas de delincuencia, así como la práctica de delitos tradicionales con la aplicación de avanzadas técnicas informacionales disponibles. Debido a la naturaleza transnacional de la delincuencia en el ciberespacio, se hace más difícil la instrucción y la persecución penal, dada la diversidad legislativa, la soberanía de los Estados en la aplicación del *ius puniendi*, la falta de capacitación de los comprendidos en la persecución penal, la dificultad en la identificación de la autoría, entre otros. Por lo tanto, la cooperación penal internacional y la armonización legislativa son mecanismos esenciales para la represión de los delitos informáticos. El Convenio sobre la Ciberdelincuencia, también conocida como la Convención de Budapest, fue la primera convención a discurrir sobre los delitos informáticos y es una herramienta para combatir la delincuencia supranacional. Para este fin se utilizó el método de enfoque deductivo, prosiguiendo del análisis de la regla general, que se refiere a los efectos de la globalización sobre los delitos cibernéticos y sus problemáticas, para la situación más específica, es decir, para comprobar y señalar los mecanismos utilizados en la actualidad para disuadir y reprimir los delitos cibernéticos en Brasil y en el mundo, frente a las dificultades enfrentadas, y de presentar mejores soluciones de aplicación. Se utilizó el tipo de procedimiento de análisis textual y de contenido, con abordaje teórico y legal basado en la investigación bibliográfica y documental sobre la interferencia de la globalización en el derecho penal, en el trato de los delitos cibernéticos como un fenómeno jurídico, así como las formas de obtener la cooperación internacional para combatir el delito cibernético. Se basó la investigación bibliográfica en el levantamiento de doctrinas, publicaciones periódicas, artículos científicos y tesis obtenidos tanto en bibliotecas y librerías como en acervos digitales en Internet, y se efectuó la investigación documental en legislación nacional.

Palabras-clave: Globalización. Ciberdelincuencia. Cooperación Penal Internacional.

SUMÁRIO

1 INTRODUÇÃO

A globalização tem grande influência no surgimento dos crimes cibernéticos, tendo em vista que foi através dos avanços tecnológicos e da quebra das fronteiras espaciais que as pessoas puderam ter um maior acesso às redes e à internet.

Foram feitas diversas discussões e elaborações legislativas a respeito dos crimes informáticos e chegou-se à conclusão que não há como cogitar uma solução estritamente de uma só nação, mas, sim, por meio de acordo e debate internacional.

A expansão do chamado cibercrime vem crescendo em um ritmo acelerado frente ao cenário mundial, e é necessário que haja uma mobilização internacional com vista a combater os crimes cometidos por meio da internet.

Assim, a Convenção de Budapeste tem um papel fundamental no que diz respeito a mecanismos de prevenção e combate ao crime cibernético, pois tem como principal fundamento a elaboração de uma política criminal comum, com auxílio mútuo entre os Estados-membros, com a finalidade de fornecer proteção à sociedade contra a criminalidade no espaço virtual.

A convenção de Budapeste propõe uma legislação comum entre as nações, bem como medidas de capacitação de pessoal, melhores equipamentos, maior controle de dados, maior proteção dos sistemas como um todo, criação de novos mecanismos de defesa da rede, criação de softwares que facilitem a busca dos infratores, entre outros (DELGADO, 2007).

O Brasil vem tentando criar legislações a respeito do tema, de modo a coibir a prática desse tipo de crime, como a Lei nº 12.965, de 23 de abril, mais conhecida como o Marco Civil da Internet, e a Lei nº 12.737, de 30 de novembro de 2012, comumente chamada de “Lei Carolina Dieckmann”, entre outras. Neste sentido, o Direito Penal possui grande valia no combate aos crimes cibernéticos, porém, individualmente não possui a eficácia desejada.

De certa forma a legislação ajuda no combate aos crimes cibernéticos, porém, ela por si só não tem o condão de combater os chamados cibercrimes, sendo necessária uma atuação conjunta das nações internacionais. Dessa forma, o presente estudo se propõe a evidenciar os mecanismos capazes de combater os crimes cibernéticos.

Dada a relevância do tema, o objetivo do presente trabalho é de verificar os aspectos mais importantes sobre o crimes informáticos, de forma a conceituar, demonstrar quem são os sujeitos ativos do crime e suas motivações, citar algumas formas que estão sendo aplicadas no Brasil e no mundo para combater esses crimes, bem como de apresentar soluções que evitem as dificuldades enfrentadas atualmente, no que se refere a diversidade das legislações

existentes entre os países, falta de preparo dos agentes, princípio da territorialidade penal e processual penal, entre outros.

Para tanto, será feito um estudo introdutório do que vem a ser a globalização e a influência da mesma no Direito Penal, traçando o papel da internet nessa evolução tecnológica. A seguir, será realizada uma análise da realidade dos crimes cibernéticos como fruto da globalização, e trará a definição do que vem a ser o cibercrime. Neste diapasão, fará abrangência à Legislação brasileira e aos projetos de lei em tramitação que tratam sobre o combate ao crime cibernético e ainda sobre a cooperação internacional sobre o tema, demonstrando, em seguida, algumas formas mais eficazes que deverão ser adotadas pelo Estado para que se consiga punir os criminosos e evite a impunidade dos mesmos. Por fim, será demonstrado o papel da Convenção de Budapeste como instrumento inovador para minimizar a incidência do cibercrime, bem como, as dificuldades enfrentadas para a investigação preliminar, a persecução penal e o *jus puniendi*.

Como o foco do trabalho é apontar os mecanismos utilizados atualmente no Brasil e no mundo e dar soluções mais eficazes para o combate do crime cibernético, não serão estudadas, a fundo, todas as legislações, projetos de lei, e ramos jurídicos sobre o tema, mas sim um enfoque penal e processual penal. Também não serão analisados pontualmente os artigos existentes na Convenção de Budapeste, eis que o intuito do trabalho é apenas de mostrar os avanços trazidos por essa Convenção Internacional e o seu papel na prevenção e repressão dos crimes informáticos.

Para a elaboração do presente estudo, foi utilizado o método de abordagem dedutivo, partindo da análise geral no que diz respeito aos impactos que a globalização causou ao Direito Penal com o surgimento dos crimes cibernéticos e suas problemáticas, para a situação particular, que se materializa nos modos utilizados atualmente para prevenir e coibir a incidência dos crimes cibernéticos no Brasil e no mundo, frente às dificuldades enfrentadas, e de propor formas mais eficazes para esse controle.

O tipo de procedimento foi o de análise textual e de conteúdo. Foram realizadas pesquisas bibliográficas e documentais, com abordagem teórica e legal, referente ao conceito de crime cibernético, os mecanismos utilizados pelo Estado para minimizar a incidência de crimes de natureza transnacional, bem como, o conceito e os benefícios da cooperação jurídica internacional.

A pesquisa bibliográfica se baseou no levantamento de doutrinas, periódicos, artigos científicos e teses obtidas tanto em bibliotecas e livrarias quanto em acervos digitais na Internet, e efetuou-se pesquisa documental em legislação nacional.

2 A ERA DA INFORMAÇÃO E INFLUÊNCIA DA GLOBALIZAÇÃO

Atualmente vivemos a era da informação onde quase tudo é realizado por meio da internet, até mesmo as tarefas diárias, as pesquisas científicas, os avanços tecnológicos, entre outros. A grande motivação dessa evolução foi a Globalização, que inovou as maneiras de como a informação era utilizada e ampliou sua aplicação de forma transnacional, fazendo com que o mundo fosse interligado.

2.1 Efeitos da globalização no contexto jurídico e no direito penal

A sociedade moderna está passando por grandes transformações, que muitos chamam de pós-modernidade. O que antes era pautado na industrialização, na divisão social do trabalho, ou mesmo da classe do proletariado como propulsor da história e da individualidade, hoje se tem uma realidade voltada para uma forma transnacional de produção, onde o foco está na intensificação da concorrência no mercado de trabalho, na existência de uma intercomunicação global, em que os países se interrelacionam economicamente, politicamente, socialmente, culturalmente, entre outros. E a esses fenômenos, o autor Sérgio Salomão Shecaira (2007) convencionou denominar como globalização.

Conforme o mesmo autor, existem algumas consequências que advêm com a globalização dentre as mais relevantes estão: a) o crescimento da incompatibilidade entre as legislações processuais e o tempo de tramitação de um processo nas relações transnacionais, eis que, na solução de conflitos, existe um procedimento tradicional a ser respeitado nos ditames legais, que podem inviabilizar negócios; b) a redução da coercibilidade do Direito Positivo por meios dos processos de desregulamentação e deslegalização do direito material e processual; c) regressão dos direitos sociais e dos direitos humanos, já que com a nova concepção voltado para o mercado, estes direitos colidem com os interesses principais da economia, quais sejam, o da competitividade e o da produtividade (SHECAIRA, 2007).

A evolução da vida moderna como resultado da globalização trouxe diversas inovações na vida política, econômica, social e jurídica. No Direito penal, através do populismo penal, essas mudanças também ocorreram, e com isso, surgiram novos patamares punitivos, aumentando a repressão penal. As tendências apresentadas atualmente pelos países globalizados, na era do encrudecimento penal, é de aumentar os tipos penais e tornar as penas mais severas. Além disso, existe a tendência de substituir o clássico Direito Penal do Dano,

para um Direito Penal do perigo, assim, haveria uma maior prevenção no que se refere ao cometimento do delito, antes mesmo de sua consumação (SHECAIRA, 2007).

Em função do gradativo crescimento das relações econômicas e com o incremento da globalização, uma nova espécie de crime se despontou como sendo um ilícito sem fronteiras geográficas e que estava fora do domínio legislativo do Estado, cujos elementos principais desses ilícitos são: a transnacionalidade, a organização e o poder econômico (BECK, 2004). Assim, conforme Beck (2004), o aparato estatal global não está preparado para o controle da delinquência globalizada, o que é um grande problema para a repressão desses crimes.

Com o aumento da insegurança decorrente da criminalidade moderna, é difundida a ideia equivocada de que apenas um Estado punitivo é capaz de reduzir a criminalidade, fazendo com que surjam aqueles que propõem a diminuição dos direitos, garantias e liberdades, como forma de coibir a prática delituosa. Este posicionamento de nada ajuda no desenvolvimento de ferramentas eficazes para o enfrentamento da marginalidade atual e globalizada (ANTUNES, 2013).

A globalização do Direito Penal e a integração supranacional, conforme preleciona Jesus Maria Silva Sánchez (2001), são típicos das sociedades pós-industriais e acabam desconstruindo o aspecto conceitual da teoria do crime. Para ele, a globalização e integração levarão a uma unificação normativa e terão, como consequência, uma flexibilização da imputação, onde as garantias políticas criminais será algo substantivo e o processual será algo relativo. Isso porque a globalização leva a demandas de direito penal mais práticas, no sentido de uma abordagem mais eficaz e ágil à criminalidade, criando respostas mais concretas para combater certos tipos de crimes.

Em decorrência dessa nova forma de criminalidade existente que emerge em razão do fenômeno da globalização é necessário que os países se voltem para um posicionamento mais prático e eficiente para combater a marginalidade, ou seja, ao invés de se criar teorias perfeitas para reprimir o crime, criar mecanismos que surtam efeitos no poder político e na aplicação judicial do Direito (SILVA, 2001). O grande problema é que os ordenamentos internos estão tentando combater uma modalidade de crime que é transnacional, e por isso a melhor forma de lutar contra esse tipo de crime é de desenvolver respostas “jurídico-penais” supranacionais, que concedam soluções concretas para o caso no sentido de promover uma uniformização das legislações penais, para garantir uma aplicação homogênea das mesmas (SILVA, 2001).

É certo que com o fenômeno da globalização, o ordenamento jurídico e a forma de agir dos Estados tiveram que sofrer modificações a fim de se adequarem a nova realidade

global. E isso foi algo positivo para o desenvolvimento econômico, social e tecnológico, porém, no âmbito do Direito Penal, surgiram novas formas de delitos os quais os ordenamentos não estavam aptos a combater. Assim surgiram diversos empasses no que tange aos crimes transnacionais que deverão ser solucionados com ferramentas inteligentes e céleres, conforme se verá adiante.

2.2 O papel da internet frente ao surgimento dos crimes cibernéticos

A internet surgiu na década de 60 por meio de um projeto elaborado nos Estados Unidos que se chamava *Arpanet* (*Advanced Research Projects Agency*), produzido pela Agência de Projetos Avançados (ARPA) do Departamento de Defesa americano, que confiou à empresa *Rand Corporation* o desenvolvimento de um sistema de telecomunicações que assegurasse que, caso ocorresse um ataque nuclear russo, o comando dos Estados Unidos não estaria prejudicado, já que o contexto mundial vivenciado na época era o da guerra fria. (NETO; GUIMARÃES, 2003). Assim, a maneira encontrada foi a formação de pequenas redes locais (LAN), colocadas em locais estratégicos do país, associadas por meio de redes de telecomunicação geográfica (WAN). Dessa forma, caso houvesse um ataque nuclear, o conjunto de redes criadas possibilitaria uma comunicação entre as cidades coligadas (NETO; GUIMARÃES, 2003).

Ulteriormente, Vinton Cerf, do Departamento de Pesquisa avançada da Universidade da Califórnia e responsável pelo projeto, em 1973, registrou o Protocolo de Controle de Transmissão/Protocolo internet (protocolo TCP/IP), que consistia em um código que possibilitou que os computadores e programas incompatíveis se comunicassem entre si, e atuassem em grupo (NETO; GUIMARÃES, 2003). Mas, conforme o mesmo autor, o mais importante impulsionador da criação da internet como ferramenta de comunicação em massa foi a criação da Web, em 1989, no Laboratório de Física, de altas energias, em Genebra, comandada por T. Berners – Lee e R. Cailliau, que era uma composição de documentos no qual os textos, os sons e as imagens poderiam correlacionar com outros documentos, permitindo com que com um único clique, o usuário pudesse ter acesso quase irrestrito a diversas informações e serviços. Com isso, a internet se tornou o meio de comunicação mais recorrente e que interliga milhões de computadores no planeta e permite o acesso à informações de uma forma que se anula qualquer distância de tempo espaço (NETO; GUIMARÃES, 2003).

Em 1965 foi criado no Brasil o Serviço Federal de Processamento de Dados e a Empresa Brasileira de Telecomunicações, mas o primeiro computador brasileiro só foi criado em 1972, pela Universidade Federal de São Paulo (USP) (LIMA, 2014).

Foi criada em 1992 a Secretaria de Política de Informática e ainda, a primeira rede conectada à internet, onde tudo era simples, tendo em vista que não existia interface interativa, mas que já representava um grande avanço (LIMA, 2014). Mas, conforme o mesmo autor, apenas em 1995 a internet foi liberada de maneira comercial.

Os crimes cibernéticos resultam de um fenômeno social, cultural e econômico trazidos pela globalização e os avanços tecnológicos conquistados neste período. É certo que a multinacionalização trouxe várias benesses e conquistas para a humanidade, porém, como já dito, trouxe alguns problemas, dentre os quais estão a intensificação do cibercrime e a violação do direito à intimidade, direito este, garantido constitucionalmente conforme artigo 5º, X, da Constituição Federal (CF) que diz "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, Constituição Federal, 1988).

Os benefícios que a internet trouxe para os usuários são incontestáveis, porque além de facilitar e agilizar o cotidiano dos internautas, permite que possam trocar informações e experiências com pessoas do mundo todo, e ainda, impulsionou o avanço das relações comerciais mundiais. Porém, como todo benefício traz uma consequência, criaram-se os riscos inerentes do desenvolvimento da informática, que são os chamados crimes cibernéticos.

2.3 Impactos do cibercrime frente à sociedade de risco

O termo Sociedade de Risco foi desenvolvido pelo teórico social Ulrich Beck e, em busca de sistematizar as transformações ocorridas pela globalização, se convencionou distinguir essas mudanças em primeira e segunda modernidade. No qual utiliza essa expressão para retratar a modernidade pautada nas sociedades de estado-nação, em que as relações, as comunidade ou mesmo redes sociais são essencialmente interpretadas em um sentido territorial (BECK, 2002).

Porém, segundo o mesmo autor, os padrões de vida, o progresso, o controle da exploração da natureza e do emprego típicos da primeira modernidade, estão sendo dizimados por cinco processos interligados, como a globalização, a individualização, o chamado subemprego, a revolução de gênero e por fim, os riscos globais, como a crise ambiental e o enfraquecimento dos mercados financeiros mundiais. E o desafio teórico e político da segunda

modernidade é de enfrentar os problemas criados, e responder as consequências, onde os riscos não são nacionais, mas globais (BECK, 2002).

Conforme o mesmo autor, a sociedade de risco se mostrou mais evidente na década de oitenta, nas sociedades pós-industriais, na qual existia um modelo social marcado pela instabilidade, em que não era mais oriunda de catástrofes naturais, problemas sociais, causados por agentes não humanos, mas por problemas advindos de decisões humanas (BECK, 2002).

Os riscos atuais tratam-se de danos improváveis decorrentes de escolhas da própria sociedade, ou seja, a própria sociedade tem causado os riscos que teme. Além disso, os riscos têm tomado proporções globais, de modo que a população local tem de se preocupar com sua atuação em seu território, mas também com as executadas em todo o mundo (BECK, 2002).

As dificuldades trazidas da sociedade do risco se dividem em três: primeiro, a sociedade caracterizada pelo aumento dos riscos de grande proporção, em razão do progresso tecnológico; segundo, a sociedade de risco se traduz em uma sociedade insegura, tendo em vista os novos riscos criados e percebidos; e por fim, a sociedade que deixa de se perguntar se foi a vida que se tornou perigosa, e passa a transformar os perigos imprevisíveis e incontroláveis em riscos, aprendendo a conviver com toda a insegurança ao invés de saná-la (SILVA, 2004).

Segundo Eduardo Diniz Neto, seguindo a ideia do papel do direito penal nesse novo cenário mundial, no contexto de uma sociedade globalizada caracterizada como uma sociedade de riscos, exige-se do direito penal uma intervenção em ramos jamais alcançados, os quais ampliam o progresso tecnológico, o desenvolvimento do conhecimento e a força das pessoas poderosas, em um mundo controlado pelas leis de mercado e da eficiência econômica, também chamada de neoliberalismo (NETO, 2010).

Neste diapasão, o Direito Penal moderno tem uma relevante missão, porque além de amparar os bens jurídicos já existentes, também tem que proteger os bens jurídicos surgidos na sociedade pós-industrial, e com isso, o Direito penal tem que reformular seus métodos e fundamentos para reprimir essa nova criminalidade emergente (NETO, 2010).

Nessa perspectiva, conforme preleciona o mesmo autor, o direito penal na sociedade de risco, com a proliferação de diversas novas espécies de crime, denominados de delitos de perigo, não mais espera a produção efetiva de danos, lesões ou mortes, mas age antes mesmo do mesmo acontecer, de uma forma preventiva, de modo a tutelar efetivamente o bem jurídico (NETO, 2010).

Uma maneira de absorver os influxos sociais causados pela sociedade de risco é por meio de uma política criminal eficiente e precisa, que conceba uma resposta preventiva apta a influir no sistema jurídico-penal. E como proposta apresentada para essa questão, surge a chamada expansão do Direito Penal, com posicionamento diferente do modelo penal liberal, pautado nos bens jurídicos supraindividual e de tutela penal preventiva, anterior ao dano e até mesmo do próprio perigo, mediante a utilização dos crimes de perigo abstrato e dos delitos cumulativos (SILVA, 2010).

O autor Cornelius Prittwitz demonstrou que o papel do Direito em Geral e do Direito Penal na sociedade globalizada do risco é de fortificar o direito, evitar que o Direito seja mal utilizado, apresentando respostas ineficazes para problemas reais e o de aplicar o Direito em questões que exige demandas superiores às suportadas (PRITTWITZ, 2013).

Porém, o Direito Penal é incapaz de, sozinho, combater os problemas da sociedade de risco, tendo em vista que as demandas atuais ao Direito Penal tem mudado vertiginosamente. E segundo o mesmo autor, esta expansão do Direito Penal causado pela criação de novas formas de crimes e tutela de novos bens jurídicos, bem como pela redução de princípios e condições para a imputação objetiva e subjetiva, apesar de o Direito Penal estar evoluindo, ainda não é capaz de solucionar os empasses atuais sistemáticos da sociedade de risco. (PRITTWITZ, 2013).

Em razão do crime cibernético pertencer a esse novo tipo de criminalidade resultante da sociedade do risco, do crescimento da globalização e do avanço tecnológico, o impacto causado na sociedade é de grande proporção. E se não forem criados mecanismos para suprimir essa forma delitiva, o Estado e até mesmo o Direito Penal irão perder a credibilidade no combate de crimes, e, com isso, a incidência dos delitos irá aumentar exponencialmente.

3 O CRIME CIBERNÉTICO COMO UM FENÔMENO JURÍDICO

O ordenamento jurídico, em especial o Direito Penal, está passando por grandes desafios, tendo em vista que com o avanço tecnológico e a relação indissociável com o cotidiano das pessoas, teve que acompanhar essa evolução e ainda, tutelar bens jurídicos que se quer existiam, fazendo nascer uma necessidade de punição de ilícitos de uma forma diferenciada.

Um desses crimes trazidos pela modernidade foi o crime cibernético, que se tornou um fenômeno jurídico de grande proporção, eis que sua abrangência é transnacional e seus efeitos, de grande escala.

3.1 Conceito de crime cibernético e suas espécies

Existe muita discussão acerca do que vem a ser o crime informático, e muitos autores não têm medido esforços para se chegar a um conceito. Têm-se, assim, várias definições que abarcam o tema, contudo, vistas de formas diversas.

Para Gustavo Testa Corrêa, crimes cibernéticos são todos aqueles delitos vinculados às informações armazenas ou em trânsito por computadores, que são utilizadas ilicitamente para fraudar ou mesmo ameaçar as vítimas (CORRÊA, 2000).

Conforme preleciona Ivete Ferreira, o crime informático pode ser entendido como sendo uma ação típica, antijurídica e culpável que pode se dar contra o computador, ou qualquer outro meio informático, ou por meio destes, utilizando-se do processamento de dados ou de sua transmissão (FERREIRA, 2000). Trata-se, portanto, conforme a mesma autora, de um conceito muito mais amplo, tendo em vista que o computador pode ser tanto o alvo, atacando os dados armazenados ou em transmissão (bem jurídico), ou também, a ferramenta utilizada pelos criminosos para a prática do delito.

Neste sentido preleciona Gomes ao dizer que toda a estrutura da informática viabiliza a prática de crimes tradicionalmente praticados, e não só a de novos crimes. Assim, o delito poderia ser cometido através do computador, sendo este utilizado como instrumento para a prática do crime, ou ainda, cometido contra o computador, ou seja, contra seus *hardwares* (que compreende a parte física do computador) e *softwares* (que compreende a parte lógica do computador) (GOMES, 2000).

Já Felipe Cardoso Moreira de Oliveira (2004) aduz que delitos informáticos nada mais são que uma conduta criminosa que tenha algum tipo de relação com instrumentos

informáticos, e que tenha por objetivo alterar, copiar, veicular ou destruir dados, que possam afetar o funcionamento do sistema. Porém, são vários os empecilhos existentes para a aplicação de uma solução penal, como a identificação do agente, a dificuldade de se identificar o sujeito passivo em relação aos crimes que atingem toda uma sociedade digital e o tempo em que o crime foi praticado (OLIVEIRA, 2004).

Diante das várias formas dos delitos informáticos, a maioria da doutrina brasileira convencionou dividir a classificação desses crimes em três espécies: puros, mistos e comuns (PINHEIRO, 2002).

Os chamados crimes virtuais puros são aqueles cujo objeto jurídico, seja o sistema informático, podendo ser tanto o *hardware* quanto *software*. Neste diapasão, destacam-se as condutas dos *hackers* e *crackers*, tendo em vista que estas pessoas passam grande parte do seu tempo manipulando computadores, e possui grande conhecimento nesta área (PINHEIRO, 2002).

Já os crimes virtuais mistos são aqueles em que a utilização da internet é essencial para que o delito se concretize, apesar do objeto jurídico visado seja diferente do sistema informático (PINHEIRO, 2002).

Por fim, os crimes virtuais comuns incorporam essa terminologia pelo fato da internet ser apena o meio para a realização do delito, ou seja, tratam-se daqueles crimes que já existem no ordenamento jurídico, e com a implantação da rede mundial de computadores, estes delitos também passaram a ser praticados por meio da internet (PINHEIRO, 2002).

Para que se possa combater, ou ao menos minimizar os crimes cibernéticos, se faz necessário um estudo aprofundado desses delitos, para que se possam conhecer as ferramentas utilizadas por esses delinquentes e antecipar as suas condutas.

3.2 Atividade dos *hackers* e *crackers*: *modus operandi* e a motivação para a prática delituosa

Existem vários outros tipos de sujeitos ativos dos delitos virtuais, porém, os mais comuns são as atividades dos *hackers* e dos *crackers*, que serão abordados neste tópico.

O termo *Hacker* tem o significado de piratas do computador, e se refere àqueles que invadem um determinado sistema em benefício próprio, conseguindo dados e informações de outrem, mas sem que, para isso, tenham que danificar algo. Ou seja, são pessoas que detêm um amplo conhecimento sobre computadores e invasões, contudo, não danificam o sistema e nem sempre almejam o prejuízo alheio (CRESPO, 2011).

Os crackers, diferentemente dos *hackers*, podem ser qualificados como os criminosos da internet, eis que os mesmos praticam os atos para causar destruição ou prejuízo, valendo-se da internet para roubar dados, dinheiro e, ainda, para disseminar conteúdo ofensivo e racista (CRESPO, 2011).

Na atualidade, o modo de agir dos delinquentes virtuais está cada vez mais sofisticado e com um rol cada vez mais amplo, devido ao fato de que, hoje, estão surgindo novas tecnologias e, na medida em que os aparelhos vão evoluindo, os *hackers* e *crackers* têm que aprimorar suas técnicas para conseguir invadir o sistema informático.

Em uma abordagem sobre o *Modus Operandi* dos sujeitos ativos, os autores Mário Furlaneto Neto e José Augusto Chaves Guimarães (2003) citam algumas condutas ilícitas, entre elas estão: o *spamming*, que é utilizado como forma de envio de *e-mails* indesejados por meio do correio eletrônico para os usuários; *cookies*, que são pequenos arquivos de textos que são armazenados no computador do internauta para a obtenção de informações relativas ao consumidor, como, por exemplo, a frequência com que o mesmo costuma visitar o site, entre outros; *spywares*, que são programas espiões que expedem informações do internauta à desconhecidos; *hoaxes* são *e-mails* que possuem conteúdo falso onde, usualmente, os criminosos colocam, como remetente, empresas de grande renome ou órgãos governamentais, podendo ainda estar vinculado a vírus; *sniffer*, que também são programas espiões, mas que são implantados no disco rígido, visando rastrear e reconhecer *e-mails* que estão na rede, com a finalidade de os controlar e os ler; cavalo de tróia, que, quando instalado, abre a possibilidade do roubo de informações, dados, senhas, arquivos, entre outros, sendo esta a espécie mais perigosa e destrutiva referente aos crimes cibernéticos (NETO; GUIMARÃES, 2003).

Conforme os mesmos autores, existem vários outros delitos e meios capazes de lesar o usuário, como a manipulação de dados e programas; espionagem industrial; sabotagem de sistemas; pornografia infantil; fraudes; ameaça via internet; crimes contra a honra praticados via *e-mail* ou redes sociais; até mesmo de homicídio doloso, quando determinada pessoa, intencionalmente, modifica a programação de um aparelho, cujo paciente dependia do aparelho para sobrevier (NETO; GUIMARÃES, 2003).

No que tange à motivação, os delinquentes, independente de qualquer outra coisa, necessitam de muito estudo, no que se refere às técnicas desempenhadas na prática dos delitos informáticos, e para isso, se utilizam de pessoas mais experientes no ramo e de técnicas disponibilizadas na própria rede (VIANNA, 2001). Mas, o interesse não está relacionado ao mero aprendizado, e sim ao reconhecimento de sua capacidade intelectual e no prestígio,

vinculados à subcultura *cyberpunk*, onde o indivíduo é induzido a praticar delitos informáticos para a obtenção de respeito e mais informações para conseguir maiores proezas (VIANNA, 2001).

Segundo o autor Glênio Leitão Marques Filho (2010), existem diversas motivações que levam os *hacker* ou *crackers* a invadirem o sistema e seus crimes são os mais variados possíveis, dentre eles estão: a espionagem industrial, que é uma situação em que uma empresa contrata um determinado cracker para invadir o sistema de uma outra empresa para roubar informações sigilosas; proveito próprio (roubar dinheiro, burlar concursos, quitar dívidas); vingança; ganhar status ou ser aceito em determinado grupo; curiosidade e aprendizado; busca de aventuras; maldade, que é aquela situação em que o indivíduo age apenas pelo desejo de ver as pessoas sendo destruídas (FILHO, 2010).

Diante do exposto, faz-se necessário que sempre se busque manter a segurança do sistema e que se criem novas técnicas de blindagem do mesmo, para que se minimizem os danos causados pelos *hackers* e *crackers*, a fim de que os usuários possam ter mais liberdade e proteção ao navegar na internet.

3.3 A ação do Estado para coibir o crime virtual

A necessidade de se produzir normas coerentes e eficazes com o fim de se controlar a incidência de crimes está estritamente ligada ao conteúdo do bem jurídico a ser tutelado, tendo em vista que o Direito Penal não pode interferir em todas as ações lesivas que ocorrem dentro da sociedade, mas tão somente quando a proteção desses bens jurídicos fundamentais não se mostrar eficaz de outra maneira. Dessa forma, impõe-se a aplicação do Direito Penal como *ultima ratio*, tendo a intervenção penal apenas quando as agressões se mostrarem intoleráveis no meio social, impondo uma sanção quando alguém ofende ou expõe a perigo um bem jurídico tutelado pelo Direito Penal (SILVA, 2007).

Conforme preleciona Felipe Cardoso Moreira de Oliveira (2004), existem diversas alternativas propostas por alguns doutrinadores que tentam buscar uma resposta eficaz, tangível, e que não transgridam os fundamentos constitucionais, a exemplo de três: a defendida especialmente por Hassemer, que aduz que o Direito Penal não pode ser utilizado como resposta à criminalidade contemporânea, devendo ser criado o chamado pela Escola de Frankfurt de “O Direito de Intervenção”, o qual consiste em um novo ramo do direito, que tem como principal função intervir, prevenindo o ato danoso, ao contrário do Direito Penal, que age após o fato lesivo (OLIVEIRA, 2004).

Outra alternativa, agora apresentada por Jesús Maria Silva Sánchez, propõe a criação de um direito de duas velocidades, abrindo mão de uma teoria geral penal, em que na primeira velocidade os princípios políticos-criminais punidos com pena privativa de liberdade ficariam intocáveis, já nos de segunda velocidade, em relação aos crimes punidos com restritivas de direito ou prestação pecuniária, haveria uma flexibilização das regras e garantias tradicionais, mantendo-se, assim, a atuação do Direito Penal (OLIVEIRA, 2004).

Por fim, existe a alternativa proposta por Stratenwerth, que propõe a proteção jurídica direcionada para o futuro, sem fazer menção a direitos individuais, deslocando a imputação voltada para o bem jurídico para o novo ramo de problemáticas, direcionadas para o futuro (OLIVEIRA, 2004).

Oliveira faz uma crítica em relação às alternativas propostas pelos doutrinadores citados, primeiramente, em relação à trazida por Stratenwerth, que entende que se deve ter uma atuação do Direito Penal independente ao bem jurídico tutelado, devendo ser imposta uma pena privativa de liberdade aos crimes futuros, tal teoria, segundo o autor, se traduz em verdadeira afronta aos princípios da tipicidade, culpabilidade e da ofensividade, próprios do Direito Penal, o que a torna ilegítima e impossível esse posicionamento (OLIVEIRA, 2004).

A próxima tese rechaçada é a de Silva Sánchez, que defende a permanência do Direito Penal para tratar desses delitos, reservando a pena privativa de liberdade aos crimes já existentes, conjuntamente com os princípios e diminuindo a característica dogmática de um Direito Penal paralelo, em relação aos delitos que não são puníveis com pena privativa de liberdade, onde Oliveira rebate tal alegação, afirmando que ao criar um Direito Penal de duas velocidades poderia causar um dano na estrutura do ordenamento, o que causaria o rompimento dos valores penais clássicos (OLIVEIRA, 2004).

Por fim, conforme o mesmo autor, a solução que se torna mais viável é a proposta por Hassemer, que propõe o Direito de Intervenção como forma de solucionar esses impasses criados com essa nova modalidade de crimes, tendo em vista que esse novo ramo pode se voltar ao combate dessa criminalidade atual, sem que tenha que desestruturar os princípios basilares do Direito Penal, e nem mesmo sofra limitações de sua atividade por princípios que regem o Estado Democrático de Direito, eis que trata-se de um novo ramo do Direito, com características próprias e com possibilidade de criação de novos fundamentos e princípios (OLIVEIRA, 2004).

Tendo em vista a crescente difusão da Internet no Brasil, o Estado deve criar mecanismos preventivos e repressivos para a práticas ilícitas, de forma positivada, nas esferas civil e penal, e também, otimizar órgãos de persecução criminal, como a Polícia Judiciária e o

Ministério Público, por meio da criação de setores especializados no combate ao crime cibernético. Pois, muito embora existam no Brasil algumas legislações a respeito, ainda é muito esparsa e pouco difundida, fazendo com que grande parte dos agentes que cometem crimes virtuais fiquem impunes (ARAS, 2014).

Embora o anseio de grande parte da doutrina seja de reduzir a intervenção do Direito Penal face às relações humanas, no tocante à teoria da intervenção mínima, é necessário se atentar que determinadas condutas que atinjam bens informáticos, ou que os delinquentes se utilizem deles para a prática de outros ilícitos, têm que ser penalmente sancionadas e reprimidas, eis que esses delitos possuem um elevado potencial de lesividade e tratar esse tipo de criminalidade com esmero é de essencial importância para a segurança da sociedade global, que está cada vez mais conectada e dependente da internet (ARAS, 2014).

Neste sentido, Ivette Senise Ferreira afirma que a informatização acelerada nos mais diversos setores da sociedade veio colocar novos instrumentos a disposição dos criminosos, cujo alcance ainda é indeterminado, eis que novas modalidades delitiva vêm sendo criadas, provocando lesões aos diversos bens e interesses jurídicos que cabe ao Estado garantir, fazendo com que seja incorporada uma específica da informática, cuja propensão é de aperfeiçoar cada vez mais os seus métodos (FERREIRA, 2000).

Com o aumento indiscriminado dos crimes cibernéticos, é primordial que o Estado crie maneiras ágeis e eficazes para combater essa nova criminalidade emergente, não só criando órgãos novos, mas otimizando e especializando os que já existem, criando legislações que sejam efetivas para evitar a impunidade, inovando em novas formas de aplicação da política criminal brasileira, aderindo a Tratados internacionais que tratem sobre a repressão dos cibercrimes e, principalmente, alertando e conscientizando a população sobre os perigos da internet e de como evitar as armadilhas criadas pelos *crackers* e *hackers*.

4 COOPERAÇÃO PENAL INTERNACIONAL PARA REPRESSÃO DO CIBERCRIME

A cooperação jurídica internacional penal sofreu mudanças ao longo do tempo no que tange a forma de requerimento judicial a outro país, eis que tradicionalmente essa colaboração se dava por meio de carta rogatória, que representava um meio não tão eficaz, tendo em vista a morosidade e a complexidade deste procedimento. Com o passar dos anos, esse sistema foi substituído pela cooperação direta, que representa um meio mais ágil e efetivo para a produção de provas e atos processuais penais no estrangeiro. O que, consequentemente, foi um fator de grande valia para a repressão dos crimes cibernéticos, já que com a simplificação do processo de cooperação internacional é possível agir de forma mais rápida e ter uma resposta mais eficiente no combate desses crimes.

4.1 Definição de cooperação jurídica internacional e a relativização da soberania como forma de viabilizar a punição dos crimes transnacionais

Segundo o Ministério da Justiça a Cooperação Jurídica Internacional pode ser entendida como um instrumento formal por meio do qual um Estado faz um requerimento a outro Estado, a fim de que este execute uma decisão ou profira uma decisão sobre uma lide, de forma que seja aplicada a Justiça no caso concreto (BRASIL, 2012).

Ou seja, é um mecanismo utilizado para solicitar a um outro Estado uma determinada medida, seja ela judicial, administrativa ou investigativa para a elucidação de um caso concreto que esteja em andamento. Já que com a crescente criminalidade transnacional causada pela movimentação de bens, pessoas, serviços e informações exige cada vez mais um Estado colaborativo e proativo, que crie mecanismos que promovam o auxílio mútuo entre os Estados, a fim de exercerem de forma satisfatória a sua atividade jurisdicional (BRASIL, 2012).

Para Nádia Araújo a cooperação jurídica internacional consiste, de forma mais ampla, na permuta internacional para que medidas processuais sejam cumpridas de forma extraterritorial pelo Poder Judiciário de um outro país. Tendo em vista que em razão da limitação jurisdicional do Poder Judiciário, é necessário requerer ao Poder Judiciário de outro Estado a sua colaboração (ARAÚJO, 2013).

A doutrina indica algumas classificações no que tange a Cooperação Jurídica Internacional. As principais se referem à posição do solicitante, que se divide em ativa e passiva, e o meio jurídico aplicado que se divide em informal e formal (SOUZA, 2008).

Na modalidade de cooperação ativa o Estado brasileiro é quem precisa da colaboração do Estado estrangeiro, eis que alguns dos elementos para que a persecução penal seja atingida encontra-se fora do território brasileiro. Nesse caso, o pedido é enviado por meio do Ministério da Justiça e é direcionado à autoridade central do país requerido ou por meio de vias diplomáticas (SOUZA, 2008).

A cooperação passiva é quando a autoridade estrangeira roga auxílio ao Estado brasileiro, onde o andamento se dá da mesma forma do ativo (por autoridades centrais ou por vias diplomáticas). Posteriormente, o pedido será concretizado de acordo com as normas do Direito brasileiro, que ditará as diretrizes para a efetivação da medida (SOUZA, 2008).

Em relação ao canal utilizado tem-se a cooperação direta ou informal que se dá quando diligência pode ser realizada diretamente pela autoridade requerida e a requerente, sem qualquer necessidade de outros meios formais, nem mesmo de intervenção do Poder Judiciário. E ainda, a cooperação formal, que é quando se faz necessária a instituição da via fixada ou para garantir a validade da prova que deva ser produzida ou do ato a ser realizado, como atos judiciais de comunicação, produção de provas, medidas assecuratórias, atos judicias definitivos ou destinados a integrar o processo penal (SOUZA, 2008).

A cooperação internacional pode ser aplicada de duas formas: com o implemento do preceito da reciprocidade, no qual o Estado, independentemente de terem estabelecido tratados ou acordos internacionais, podem cooperar uns com os outros; ou por vias formais, onde se comprometem por meio de tratados ou acordos, a cooperarem entre si (RODRIGUES; SILVA, 2012).

Com a crescente interdependência entre os Estado a cooperação internacional ganhou um destaque e, com isso, o conceito de soberania que antes era tido como um princípio absoluto teve que sofrer algumas alterações em seu conceito, e hoje está mais ligado à noção de assistência mútua.

Surgiram duas teorias que discutem sobre a soberania estatal e conduta do Estado dentro desse novo cenário mundial: a teoria dualista, que aduz que o direito internacional e o direito interno são coisas diversas, defendendo a soberania estatal absoluta; e a teoria monista, que afirma que o direito interno e o internacional são parte de um sistema uno, corroborando com a relativização da soberania estatal (CIDRACK, 2014).

A soberania pode ser entendida como o poder que Estado exerce dentro de seu território sobre as pessoas e as coisas. Assim, cabe ao Estado se proteger de interferências externas, exercendo seu poder apenas na sua circunscrição territorial. Portanto, quando determinados atos judicias extrapolarem a jurisdição do país, é necessária a colaboração de outro país para cumprir sua atividade jurisdicional (BARBOSA JÚNIOR, 2011).

Vale ressaltar que a expressão território compreende todo o espaço, seja ele terrestre, marítimo, fluvial e aéreo onde o Brasil exerce, de forma exclusiva, sua soberania. Dessa forma abrange todo o solo delineado por suas fronteiras externas e internas, bem como rios ou lagos fronteiriços, o mar territorial e seu espaço aéreo (DELMANTO, 2002).

O território sofreu evoluções no direito internacional, tendo em vista que além de ser caracterizado pela porção da superfície global onde o Estado exerce sua soberania e a noção espacial estritamente considerada, tem-se atualmente que analisar a interação entre os Estados e interesses e as necessidades dos indivíduos em um plano internacional (ACCIOLY; SILVA; CASELLA, 2012).

Em relação à soberania do Estado na aplicação do *jus puniendi*, Tourinho Filho entende que esse poder do Estado é um de seus principais atributos, e que pode ser dividido em *jus puniedi in abstracto* e *in concreto* (TOURINHO FILHO, 2010). Nesse contexto, quando o Estado, através de seu Poder Legislativo, edita normas abstratas penais, cominando sanções a quem infringir tais mandamentos, tem-se o *jus puniendi* abstrato e, caso o indivíduo pratique tal conduta proibida, surge para o Estado o *jus puniendi* em concreto, devendo o Estado punir tal indivíduo com a pena devida (TOURINHO FILHO, 2010).

Em razão dessa nova visão de soberania, não se pode afirmar que a cooperação internacional ofenda o poder soberano do Estado, eis que os pedidos de colaboração devem atender aos preceitos da ordem pública e do interesse nacional (TOFFOLI; CESTARI, 2008).

O Instituto da cooperação está previsto na Constituição Federal no artigo 4˚, inciso XI, onde dispõe que o Brasil orienta-se em suas relações internacional pelo princípio da cooperação entre os povos para que haja o desenvolvimento da humanidade. Sendo assim, essa prática não se trata de mero compromisso moral, ou ajuda voluntária, mas sim, de uma obrigação jurídica (TOFFOLI; CESTARI, 2008).

A relativização da soberania estatal não está relacionada com o enfraquecimento do Estado diante da comunidade internacional, pelo contrário, está ligada com o novo papel do Estado perante os outros países e perante seus nacionais no cumprimento de suas obrigações (CIDRACK, 2014). Não podendo o Estado conforme o mesmo autor, se basear no conceito de soberania absoluta para cometer violações de direitos e deveres dentro do seu território.

Segundo Ricardo Lewandowski as transformações ocasionadas pela globalização não foi capaz de desestruturar os preceitos da soberania. De forma que no âmbito interno, a soberania continua tendo a decisão final sobre as competências, e no plano internacional continua preservando a independência que lhe proporciona assumir ou não certas obrigações (LEWANDOWKI, 2008). Desse modo, conforme o mesmo autor, a concessão de alguns poderes para autoridades transnacionais, a fim de proporcionar maior eficácia estatal não só permite a conservação da soberania, como também fomenta as possibilidades políticas de seu exercício.

A cooperação jurídica internacional representa uma das principais formas de combater os crimes supranacionais, mas também se faz necessário a harmonização das legislações estatais, relativizando sua soberania para que viabilize o implemento de ferramentas capazes de solucionar o problema trazido por essa nova realidade globalizada.

4.2 Os mecanismos de combate e as legislações existentes sobre o crime cibernético no Brasil e no mundo

A característica da transnacionalidade e a aumento dos crimes dessa natureza fizeram com que os países se unissem para harmonizar suas legislações penais e processuais penais, bem como intensificaram-se os tratados e convenções internacionais (FERNANDES, 2008). O reflexo disso no Brasil foram, principalmente, o rigor majorado na prisão de pessoas envolvidas e o implemento de medidas para recuperar os valores obtidos ilicitamente (FERNANDES, 2008).

Outro importante mecanismo de combate aos crimes que vão além da esfera de soberania do Estado é o Tribunal Penal Internacional, pois tem como principal característica, a punição dos crimes internacionais na ausência ou insuficiência dos ordenamentos jurídicos nacionais.

O Tribunal Penal Internacional possui caráter sui generis e segue princípios como o da complementariedade e o da excepcionalidade, eis que tem como objetivo de atuar apenas em crimes de relevante gravidade e nos casos em que houver a clara incapacidade ou ausência de dispositivo estatal em punir os responsáveis (GORAIEB, 2003).

Importante ressaltar que o Tribunal Penal Internacional instituiu uma cláusula contra o abuso, segundo a qual, a existência de um pseudoprocesso nacional para impedir uma intervenção subsidiária do Tribunal Penal Internacional, sob o argumento de violação ao

princípio do *bis in idem*, gerando uma absolvição, não obsta a interferência do Tribunal (ESER, 2013).

O Estatuto de Roma foi um divisor de água referente ao Direito Internacional Público, tendo em vista que ele possibilitou uma maior agilidade referente às infrações a direitos essenciais, bem como proporcionou uma proteção maior aos indivíduos, já que estende a todos os países que violaram algum dos princípios fundamentais para o Direito Internacional (SANTOS; BORGES, 2014).

Uma importante aliada para a investigação criminal em âmbito internacional é a INTERPOL (*International Criminal Police Organization*), que representa um banco de dados com informações de criminosos procurados, dentro de uma rede de 186 (cento e oitenta e seis) países membros da organização (VASCONCELLOS, 2013). E ainda, a chamada Rede 24/7, que já conta com a participação de mais de 50 (cinquenta) países, e que foi constituída com a finalidade de apurar crimes cibernéticos (VASCONCELLOS, 2013).

A criação de tratados e convenções internacionais em matéria penal contribuiu de forma significativa para a diminuição dos empecilhos existentes pela diversidade de legislações entre os países, e possibilitou uma maior integração entre eles, com o intuito de elaborar formas eficazes de repressão dos crimes supranacionais.

Em que pese os crimes cibernéticos terem natureza transnacional, existem mecanismos que podem ser adotados no âmbito nacional, não só de caráter legislativo, mas também de caráter preventivo, referente a estudos mais aprofundados sobre o assunto.

Existem diversos instrumentos que podem ser usados para diminuir a incidência dos cibercrimes, dentre os quais, estão a criação de um grupo especializado em diversas áreas de conhecimento, para que possam analisar as qualidades e deficiências legislativas, propondo maneiras mais eficazes de assegurar a proteção do sistema e dos usuários; a promoção de cursos, em instituições educativas, enfatizando sobre os riscos existentes na internet e sobre posturas éticas que devem ser seguidas quando se está na rede; a instalação de medidas de segurança aos os usuários, entre outros (CRESPO, 2011).

No Brasil, existem atualmente órgãos especializados no combate aos cibercrimes, tanto no âmbito federal quanto no estadual. Na esfera federal há uma ação conjunta do Ministério Público Federal (MPF), a Polícia Federal (PF) e a Organização Não-Governamental Safernet, em que recebem e direcionam as denúncias envolvendo os crimes cometidos por meio do computador (WENDT, 2011). Já, conforme o mesmo autor, em esfera estadual, as Polícias Civis não possuem muitos órgãos especializados no controle e investigação dos crimes virtuais.

Uma maneira de prevenir os crimes cibernéticos é a participação do Comitê Gestor Internet do Brasil, fundado em 1995 pela Portaria Interministerial n. 147, que possui o intuito de dar efetividade à participação da sociedade em questões que envolve a internet, de modo a impulsionar o bom uso da internet, vindo a auxiliar a política de prevenção criminal contra os crimes virtuais (MAZONI, 2009).

Como forma de criar uma legislação que se adequasse a nova forma criminosa e para criar condições de punição dos crimes informáticos foi sancionada em 30 de novembro de 2012 a Lei 12.735, que teve como relator o senador Eduardo Azevedo. Porém, essa lei possui somente dois artigos que tratam sobre o assunto, de forma que um deles prevê que os órgãos das Polícias Civis e Federais deveriam se estruturar a fim de combater as ações delituosas em rede de computadores, sistema informatizado e dispositivos de comunicação; e o outro artigo preleciona que nos casos de crime de racismo, quando usado por meio de publicação de meio social, o juiz poderá determinar a cessação das transmissões de qualquer meio, inclusive antes do inquérito policial (WENDT, 2013).

Outrossim, o Brasil já está antenado nesse novo cenário de crimes, e por isso, foi incorporada a legislação atual brasileira a lei 12.737, de novembro de 2012, comumente chamada de “Lei Carolina Dieckmann”, que surgiu devido ao ocorrido de que a atriz da Globo foi vítima de invasão indevida de imagens contidas em sistema informático de natureza privada (CABETTE, 2013).

Essa lei, conforme o mesmo autor, trouxe para o ordenamento jurídico um novo crime de "Invasão de Dispositivo Informático”, que representa na conduta do agente de "invadir dispositivo alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagens ilícita (CABETTE, 2013).

Outro grande avanço para a nossa Legislação foi o Marco Civil da Internet, Projeto de Lei 2.160/2011, que trouxe como pontos principais, a proteção da neutralidade da rede, vetando que provedores concedam privilégios de acesso a pessoas que pagam por melhores pacotes; garantia do direito à privacidade, inviolabilidade e sigilo das informações dos usuários da rede; e também, a proibição ao chamado “metados", ou seja, para que as redes sociais não vendam seus dados a terceiros (STEECK, 2014).

O Marco Civil da Internet instituiu princípios, garantias, direitos e deveres para a utilização da internet, vislumbrando a atuação da internet em proporções globais, enfatizando a finalidade social, cultural, o exercício da cidadania nos meios digitais, a cooperação entre os

usuários, a defesa do consumidor, dentre outras medidas para a utilização democrática da internet (DARÓS MALAQUIAS, 2015).

Alguns projetos de lei estão em tramitação no Congresso Nacional sobre o crime cibernético, os mais conhecidos são: o Projeto de Lei nº 76, de 24 de março de 2000, que foi proposto pelo Senador Renan Calheiros, que aborda o acesso não permitido de computadores e sistemas eletrônicos, a sabotagem por computadores, a fraude eletrônica, entre outros; o Projeto de Lei nº 279, de 2003, proposto pelo senador Delcídio Amaral, que tem por objetivo impor aos prestadores de serviços de correio eletrônico, a manutenção do cadastro detalhado dos usuários das contas (DULLIUS; HIPLLER; FRANCO, 2012).

Existem algumas leis e artigos esparsos dentro do ordenamento brasileiro que abordaram de forma sucinta os crimes informáticos, entre eles está o Código Penal brasileiro em seus artigos 313-A e 313-B, que tratam, respectivamente, de crime de inserção de dados falsos em sistema e modificação ou adulteração não permitida de sistema de informações, bem como os artigos 325§1º, I e II e o artigo 153, §1-A. Estes crimes só podem ser cometidos por funcionários públicos. (SILVA, 2007).

Outra lei esparsa é a 9.609/98 referente a proteção da propriedade intelectual de programa de computador, em que o núcleo do tipo é violar, infringir um determinado objeto, que no presente caso são os direitos de determinado autor de programa de computador (NUCCI, Guilherme de Souza, 2013). Segundo o mesmo autor, o crime pode ser cometido por qualquer pessoa, porém o ofendido é restrito às pessoas criadoras de programa de computador. Se no caso a violação deste programa consistir em alienação, ou mesmo a exposição à venda passa-se para a figura qualificada do delito, por conseguinte, a pena é aumentada para reclusão de um, a quatro anos e multa, e não mais detenção de 6 (seis) meses a 2 (dois) anos. (NUCCI, Guilherme de Souza, 2013).

Com relação às legislações existentes no mundo com o crescimento descontrolado dos crimes informáticos, Portugal incorporou a conduta delitiva através da Lei 109/1991, onde previa a figura da interceptação ilegítima de comunicações que se processavam dentro de um sistema ou rede de informática (CRISPIN, 2012).

A Itália elaborou a Lei 547/1993, na qual incorporou novas figuras em seu Código penal, penalizando as condutas de danos a sistemas informáticos e telemáticos, de qualquer alteração, supressão ou falsificação nos conteúdos telemáticos ou informáticos, bem como de difusão de programas que tenham o intuito de atrapalhar o bom funcionamento de um sistema informático (CRISPIN, 2012).

Nos Estados Unidos, a principal legislação criada para responsabilizar criminalmente o indivíduo que cometesse condutas ilícitas no âmbito informático foi a Lei de Fraude e Abuso Computacional, feita em 1986,com intuito de proteger sistemas nacionais, e impedir vantagens financeiras através dos ilícitos (SILVA, 2013).

Apesar do esforço exercido para solucionar a criminalidade existente na era informacional, tem surtido pouco efeito a implementação de leis incriminadoras no ordenamento jurídico nacional, tendo em vista que grande parte desses delitos transcendem as barreiras físicas dos Estados e acaba dificultando a punição dos envolvidos. Dessa forma, a elaborações de tratados e convenções internacionais para harmonizar as legislações penais referentes aos crimes cibernéticos é de grande importância para evitar e punir esses crimes.

4.3 O papel da Convenção de Budapeste e os desafios para a cooperação penal internacional em matéria de cibercrimes

Em decorrência da interconectividade, as pessoas podem trocar dados e informações simultaneamente pelo mundo todo, o que torna difícil a apuração de condutas ilícitas em situações em que um mesmo fato repercuta seus efeitos em diferentes locais, em distintas regiões do mundo, como no caso de disseminação de vírus na internet, que pode afetar milhares de sistemas informáticos no mundo todo, já que os efeitos não são restringidos por quaisquer limites geográficos ou fronteiras nacionais (DELGADO, 2007).

Segundo o mesmo autor, são encontrados diversos empecilhos que podem dificultar as investigações. Uma delas é a jurisdição de cada país de forma isolada, em que a simples tentativa de colheita de dados pode ser encarada como uma violação à soberania territorial do país em que os dados encontrem-se armazenados; outro ponto é a diferença na legislação de cada estado, o que acentua ainda mais o problema. São justamente esses problemas que o Tratado de Budapeste visa erradicar, propondo uma harmonização das leis nacionais no tocante à tipificação das condutas relacionadas aos dados e sistemas informáticos e o implemento da cooperação internacional neste aspecto. (DELGADO, 2007).

A comunidade internacional, com o intuito de harmonizar as legislações nacionais, melhorar as técnicas de combate ao crime cibernético e aumentar a cooperação entre as nações assinou em 2001, na Hungria, o tratado internacional, chamado de Convenção de Budapeste, que inovou na forma de cooperação penal e ofereceu uma regulamentação que ia além da jurisdição nacional, com vista a combater de forma mais eficiente as infrações relacionadas aos cibercrimes (MORAIS NETO, 2009).

A convenção de Budapeste entrou em vigou em 1˚ de julho de 2004, quando foi ratificada por cinco Estados, e contemplou diversos aspectos e conceitos envolvendo o crime cibernético, porém, a principal inovação foi em relação ao auxílio mútuo em matéria penal, que estabeleceu uma série de regras, princípios gerais e modalidades de cooperação, com o intuito de atender as necessidades atuais tangentes aos modos de investigação e procedimentos envolvendo esse novo tipo de crime (DELGADO, 2007).

Outro aspecto relevante da convenção de Budapeste que viabiliza a cooperação entre os países é a flexibilização do princípio da dupla incriminação, na medida em que impõe somente a equivalência dos elementos do tipo dos Estados requerente e requerido, não importando a catalogação ou o nome atribuído ao demandado (DELGADO, 2007).

Dessa forma, a Convenção de Budapeste sobre o Cibercrime se traduz em importante marco para a cooperação penal internacional, tendo em vista a promoção de medidas de aprimoramento de ferramentas de auxílio mútuo e de produção de provas, bem como o implemento de mecanismos de preservação dos elementos probatórios em forma de dados e a celeridade nas investigações e processos penais por meio da divulgação expedita de dados de tráfego preservados, com vista a atender de forma mais eficaz à persecução penal para combate às manifestações da criminalidade informática, que antes não existiam (DELGADO, 2007).

A convenção de Budapeste foi o primeiro tratado internacional a tratar sobre os crimes cibernéticos, abordando sobre a segurança nas redes, as violações aos direitos autorais, a pornografia infantil, a fraude cometida por meio do computador, dentre outros (MAZONI, 2009). Esse tratado, segundo a mesma autora, teve por escopo proteger a sociedade dos crimes informáticos, desenvolvendo para isso, uma legislação apropriada que trouxesse maior facilidade e agilidade na cooperação entre os países e maneiras mais eficazes de reprimir o cibercrime.

A diversidade legislativa é apontada como um dos principais fatores que geram a insegurança jurídica e os conflitos, especialmente nesse contexto de crescimento das negociações transnacionais entre países com idiomas e legislações diferentes (OLIVEIRA, 2008). Conforme a mesma autora, são devidos a esses aspectos que a harmonização jurídica se traduz como um instrumento facilitador, já que o intuito é de adotar medidas que possibilitem a redução, ou até mesmo a eliminação de conflitos de ordenamentos diferentes.

Oliveira indica alguns instrumentos que viabilizam a harmonização do Direito, entre eles estão: os atos de organismos supranacionais (atos emitidos por órgãos supranacionais de organizações internacionais de integração); as convenções internacionais (que pode se dar por

reciprocidade, por regulamentação uniforme de uso geral, ou por lei uniforme); as leis modelos (são textos fixados para substituir as leis dos Estados, por meio de um ato legislativo nacional); as regras (assim como os princípios, servem para determinar diretrizes, e não tem caráter vinculatório), os princípios, as leis paralelas (leis confeccionadas por dois ou mais Estados, com o intuito de harmonizar ou unificar as leis sobre determinado assunto); e os *Restatements* (formulações de proposições gerais sobre determinado assunto) (OLIVEIRA, 2008).

Outro problema que não se encontra só no Brasil, mas em grande parte do mundo, é a insuficiência de capacitação referente aos envolvidos na persecução penal como os policiais, o Ministério Público e o Judiciário, o que acaba dificultando a punição dos delinquentes e, por conseguinte, gerando a impunidade referente aos crimes cibernéticos (WENDT, 2013).

Quando o crime é cometido por meio de um computador, uma das principais ferramentas de investigação para identificar a autoria é o log de conexão, que é um emaranhado de informações sobre o uso da internet pelo usuário, emitindo dados sobre o dia, o hora, o fuso horário, o tempo de utilização do sistema, e o IP (*Internet Protocol*), bem como o *log* de acesso que permite acessar informações sobre os serviços utilizados na internet, relativos ao conteúdo, contendo data, horário e o IP (WENDT, 2013).

O problema é que os órgãos investigativos não são obrigados a permanecer um tempo mínimo com os logs de conexão e de acesso, o que acaba inviabilizando a descoberta da autoria delitiva, mesmo com o advento da Lei 12.737 (conhecida como Lei Carolina Dieckmann) (WENDT, 2013). Mas, conforme o mesmo autor, para resolver esse impasse, a Agência Nacional de Telecomunicações (ANATEL) confeccionou um novo regramento, no qual os provedores tinham a obrigação de armazenar os *logs* pelo prazo mínimo de 01 (um) ano (art.53 da Resolução 614/2013).

Outra dificuldade encontrada pelos órgãos investigadores é a possiblidade de burlar as evidências, ocultando o IP por meio dos chamados *proxies*, que são serviços que mascaram o verdadeiro IP, o que prejudica o rastreamento do autor da conduta (CAVALCANTE, 2013).

A investigação dos crimes cibernéticos é complexa pois, além de serem levados em conta os três elementos que compõe o crime, quais sejam tipicidade, ilicitude e culpabilidade, deve ser considerada a dificuldade na definição do tempo e lugar do crime, bem como no alto risco de perecimento das provas coletadas, o que torna captura do criminoso mais difícil (IOCCA, 2012).

Por sua própria natureza, os crimes cibernéticos são crimes mais difíceis de serem descobertos e investigados, e isso ocorre por vários motivos, como a falta de denúncia por

parte das vítimas, por desconhecimento do fato, ou por outro motivo diverso, o que consequentemente, cria o que se chama de cifras negras (crimes que não foram levados a conhecimento da autoridade competente) (HERMAN, 2013) .

Outras vítimas, especialmente empresários, geralmente não levam o caso adiante por ter medo de que os consumidores fiquem receosos pelo fato de seu sítio da Internet ou seus registros empresarias não serem seguros (HERMAN, 2013).

Preleciona a mesma autora que a cooperação internacional se torna essencial nesses casos, pois, além de fornecer cooperação nas investigações e processos, ter fontes legislativas uniformes também facilita a coleta de dados sobre crimes cibernéticos e um maior conhecimento sobre quais mecanismos de execução estão aptos para serem aplicados com efetividade.

A impunidade está muito mais relacionada com a falta de estrutura e a fragilidade das informações de rastreamento do que a falta de legislação especifica para tratar desse tipo de crime, eis que o trânsito de dados é livre e veloz, e ocorre de forma instantânea, facilmente manipulados pelos criminosos (PINHEIRO, 2006).

A combinação entre as leis penais internas e os tratados e convenções internacionais sobre os crimes cibernéticos, a partilha e conexão dos dados entre os órgãos investigadores e as companhias que disponibilizam o acesso à internet (com o devido respeito aos princípios e garantias fundamentais), e a implementação de unidades especializadas na prevenção e repressão dos cibercrimes, representaria um grande avanço em relação às ferramentas utilizadas atualmente, o que facilitaria a cooperação entre os países e traria maior eficácia na apreensão dos envolvidos (COLLI, Maciel; LOPES JÚNIOR, Aury, 2009).

Existem diversas ferramentas que podem ser implementadas com o intuito de minimizar a incidência dos delitos informáticos, mas para isso, o Estado tem que estar disposto a investir, e apoiar a causa, não só estimulando a criação de leis, mas de políticas públicas que conscientize a população sobre os riscos situados na internet, e ainda, da ratificação do Brasil à Convenção de Budapeste, que é a principal e mais completa legislação que aborda os cibercrimes.

5 CONSIDERAÇÕES FINAIS

Com os avanços trazidos pela globalização, ocorreram diversas mudanças na sociedade, o que influenciou não só na economia ou na diversidade cultural, mas também no Direito Penal, eis que, com o implemento da internet, surgiu uma nova espécie de crime que antes não existia, bem como, se aperfeiçoaram as técnicas utilizadas no cometimento de crimes tradicionais oferecidas pelo crescimento tecnológico.

O crime cibernético pode ser cometido de duas formas: a) ou o computador é usado como meio para a prática do delito; b) ou o crime é cometido contra o computador. Nestes dois casos, os impactos causados na sociedade de risco em que se vive atualmente são de grande proporção, podendo causar diversos prejuízos para empresas ou para os usuários.

Diante disso, é essencial que haja uma mobilização do Estado para criar mecanismos que reprimam, de forma ágil e eficaz, a incidência dos delitos informáticos.

O Brasil ainda é precário no que diz respeito aos instrumentos utilizados na investigação dos cibercrimes, tendo em vista a falta de órgãos especializados, a legislação vaga, esparsa e pouco eficaz e as dificuldades em se identificar a autoria, o que acaba gerando a impunidade dos criminosos.

Outro problema recorrente é a ausência de barreiras geográficas para prática dos delitos informáticos, o que acaba colidindo com a soberania de outros Estados na aplicação do *jus puniendi*. Dessa forma, a cooperação penal internacional é um mecanismo essencial para o auxílio mútuo entre os países, e representa uma nova forma de se conceituar a soberania que, hoje, é tida como um princípio relativo e que está mais ligada à ideia de assistência recíproca.

A diversidade legislativa é um dos principais problemas encontrados para a apuração e punição dos envolvidos, eis que se não houver uma harmonização dos ordenamentos, a chance dos delinquentes não responderem pelo crime é muito maior.

Devido à natureza transnacional dos crimes cibernéticos houve uma tentativa de se harmonizar as legislações nacionais e aumentar a cooperação internacional entre os países, criando técnicas inovadoras e inteligentes para a prevenção e erradicação desses crimes, através da ratificação da Convenção de Budapeste.

Essa convenção foi a primeira a tratar de crimes informáticos e representou um grande avanço para a comunidade internacional. Porém, o Brasil não faz parte desse tratado, apesar de sua discreta legislação nacional sobre o cibercrime estar em consonância com os ditames estabelecidos pela convenção, o que representa um grande retrocesso, já que a mesma trouxe

diversas benesses no que diz respeito ao aprimoramento de técnicas de investigação e auxílio mútuo dos Estados-membros.

Elaborar uma legislação nacional que aborde os cibercrimes de forma clara e objetiva, tipificando as condutas delitivas é importante, porém, a legislação por si só não é suficiente para combater esses delitos.

Nesse sentido, com base no estudo apresentado, considera-se que é necessária uma atuação efetiva do Estado no sentido não só de criação de novos centros especializados na redução da criminalidade informática, mas de estudar a fundo novas técnicas para aprimorar e otimizar os órgãos que já existem, implementando políticas públicas com a finalidade de alertar e conscientizar a população sobre os riscos existentes na internet e de como evitá-los, bem como, de elaborar legislações que sejam efetivas para impedir a impunidade e que inovem as formas de aplicação das políticas criminais brasileiras.

Também se faz necessária, em razão da natureza supranacional dos crimes cibernéticos, uma maior cooperação penal internacional por meio de adesão a Tratados e Convenções Internacionais, principalmente a aderência do Brasil à Convenção de Budapeste, já que trata especialmente e de forma detalhada, do conceito de cibercrime, normas procedimentais de cooperação e auxílio mútuo, entre outros mecanismos que permitem uma harmonização entre as legislações e, por conseguinte, uma maior eficácia na prevenção e combate dos crimes cibernéticos.

REFERÊNCIAS

CASSELLA, Paulo Borba; ACCIOLLY, Hildebrando; SILVA, G. E do Nascimento e. **Manual de Direito Internacional Público**. 20. ed. São Paulo: Saraiva, 2012.

ANDREUCCI, Ricardo Antônio. **Legislação penal especial**. 9. ed. atual. e ampl. São Paulo: Saraiva, 2013.

ANTUNES, Leonardo Leal Peret, A Expansão do Direito Penal na era da Globalização e a Criminalidade Moderna. In: **Tribuna Virtual IBCCRIM**, ano 1, ed.3, ISSN nº 2317-1898, abril 2013. Disponível em: <http://zip.net/bwthzV>. Acesso em 02 fev. 2016.

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 5, n. 51, out. 2001. Disponível em: < http://zip.net/bkth33>. Acesso em: 17 fev. 2016.

ARAÚJO, Nádia. A importância da Cooperação Jurídica Internacional para a Atuação do Estado Brasileiro no Plano Interno e Internacional. In: Secretaria Nacional de Justiça; Departamento de Recuperação de Ativos (DRCI). **Manual de Cooperação Jurídica Internacional e Recuperação de Ativos** – 2. ed. Brasília: Ministério da Justiça, 2012. Disponível em: <http://zip.net/bfthWJ>. Acesso em 04 mai. 2016.

BARBOSA JÚNIOR, Márcio Mateus. O novo Código de Processo Civil e o Auxílio Direto: Contexto do Direito Brasileiro Contemporâneo. In: **Âmbito Jurídico**, Rio Grande, XIV, n. 90, jul 2011. Disponível em: <http://zip.net/bnth9F>. Acesso em 04 maio 2016.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <http://goo.gl/Y9JnrU>. Acesso em: 01 mar. 2016.

_____. Ministério da Justiça. **Cartilha Cooperação Jurídica Internacional em matéria Penal**. Brasília, DF, 2012. Disponível em: <http://zip.net/bxtjZ9>. Acesso em: 25 mar. 2016.

BECK, Rafael Francis. Perspectivas de Controle do Crime Organizado na Sociedade Contemporânea: Da crise do modelo liberal às tendências de antecipação de punibilidade e flexibilização das garantias do acusado. In:Salo de Carvalho (Org). **Leituras Constitucionais do Sistema Penal Contemporâneo**. Rio de Janeiro: Editora Lumen Juris, 2004.

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei 12.737/12 e o crime de invasão de dispositivo informático. **Âmbito Jurídico**, Rio Grande, XVI, n. 109, fev. 2013. Disponível em: <http://zip.net/bwthzX>. Acesso em 09 mar. 2015.

CAVALCANTE, Waldek Fachinelli. Crimes cibernéticos: investigação e ameaças na internet. **Revista Jus Navigandi**, Teresina, ano 18, n. 3782, 8 nov. 2013. Disponível em: < http://zip.net/bmth0b>. Acesso em: 12 mai. 2016.

CIDRACK, Luiza B. V.. A Relativização da Soberania Estatal e a Proteção aos Direitos Humanos à luz do Controle de Constitucionalidade. In: Wagner Menezes; Clodoaldo S. da Anunciação; Gustavo M. Vieira Org(s). **Direito Internacional em expansão**. Belo Horizonte: Arraes Editores, 2014.

COLLI, Maciel; LOPES JÚNIOR, Aury. Cibercrimes: **Limites e perspectivas da investigação preliminar policial brasileira de crimes cibernéticos**. Programa de pós-graduação em Ciências Criminas, Mestrado, faculdade de direito, PUCRS. 2009. Disponível em: <http://zip.net/blthRN>.Acesso em: 07 mai. 2016.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. São Paulo: Editora Saraiva, 2000.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

CRISPIN, Mirian Cristina Generoso Ribeiro. **Doutrina nacional: Crimes praticados pela internet e crimes de informática**. 2012. Disponível em: <http://zip.net/bdtjzY>. Acesso em 20 fev. 2016.

DARÓS MALAQUIAS, Roberto Antônio. **Crime cibernético e prova: a investigação criminal em busca da verdade**. 2ª edição. Curitiba: Juruá, 2015.

DELGADO, Vladimir Chaves. **Cooperação Internacional em Matéria Penal na Convenção sobre o Cibercrime**. Brasília, 2007. Disponível em: <http://zip.net/bcth4m >. Acesso em 13 mar. 2015.

DELMANTO, Celso. **Código penal comentado**...[et al]. 6.ed. atual e ampliada. Rio de Janeiro: Renovar, 2002.

DULLIUS, Aladio Anastacio; HIPPLER, Aldair; FRANCO, Elisa Lunardi. **Dos Crimes Praticados em Ambientes Virtuais**. 2012. Disponível em: <http://zip.net/bttjKr>. Acesso em 14 maio. 2016.

ESER, Albin. Medidas nacionais e transnacionais contra a impunidade da criminalidade amparada pelo Estado e de crimes internacionais: conclusões de política jurídica a partir de um projeto comparado sobre a justiça de transição. In: Kai Ambos; Mariá Laura Böhm Coord. (s). **Desenvolvimentos atuais das ciências criminais na Alemanha**. 1.ed- Brasília, DF: Gazeta Jurídica, 2013.

FERNANDES, Antônio Scarance. O Processo Penal Internacional. In: Guido Fernando Silva Soares, Paulo Borba Casella... [et al.], (organizadores).**Direito Internacional, Humanismo e Globalidade**. São Paulo: Atlas, 2008.

FERREIRA, Ivete Senise . A criminalidade informática. In: Newton de Lucca; Adalberto Simão Filho. (Org.). **Direito e Internet – aspectos jurídicos relevantes**. Bauru: Edipro, 2000.

FILHO, Glenio Leitão Marques. Hackers e Crackers na internet: as duas faces da moeda. **Revista eletrônica Temática**. Ano VI, n. 01 – janeiro/2010. Disponível em: <http://zip.net/bptjG4>. Acesso em 20 fev. 2016.

GOMES, Flávio Luiz. **Crimes informáticos**. Disponível em: <www.direitocriminal.com.br>. Acesso em 24 jan. 2106.

GORAIEB, Elizabeth. Tribunal Penal Internacional: Uma conquista contra a impunidade. In: Florisbal de Souza Del'Olmo (coord.).**Curso de Direito Internacional Contemporâneo: estudos em homenagem ao Prof. Dr. Luís Ivani de Amorim Araújo pelo seu 80° aniversário**. Rio de Janeiro: Forense, 2003.

HERMAN, Susan N.. Os desafios do crime cibernético. **Revista Eletrônica de Direito Penal e Política Criminal**, [S.l.], v. 1, n. 1, dez. 2013. ISSN 2358-1956. Disponível em: < http://zip.net/bptjG6>. Acesso em: 12 mar. 2015.

IOCCA, Érica Cristiane. Crimes Cibernéticos e a sociedade atual. **JUDICARE, Revista Eletrônica da Faculdade de Direito de Alta Floresta**. V.4, n. 4, 2012. Disponível em: <http://zip.net/bqtjZ9>. Acesso em: 15 mar. 2016.

STRECK, Lênio Luiz. Apontamentos hermenêuticos sobre o Marco Civil regulatório da internet. In: George Salomão Leite, Ronaldo Lemos (coord.). - **Marco Civil da Internet** -São Paulo: Atlas, 2014.

LEWANDOWSKI, Enrique Ricardo. Globalização e Soberania. In: Guido Fernando Silva Soares; Paulo Borba Casella... [et al.], (organizadores). **Direito Internacional, Humanismo e Globalidade**. São Paulo: Atlas, 2008.

LIMA, Simão Prado. Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. In: **Âmbito Jurídico**, Rio Grande, XVII, n. 128, set. 2014. Disponível em: <http://zip.net/bmth0g>. Acesso em 02 mai. 2016.

MAZONI, Ana Carolina. **Crimes na internet e a Convenção de Budapeste**. Brasília, 2009. Disponível em: <http://zip.net/bstjhw>. Acesso em: 20 fev.2016.

NETO, Arnaldo Sobrinho de Morais. **Cibercrimes e Cooperação Penal internacional: Um Enfoque à luz da Convenção de Budapeste**. 2009. Disponível em: <http://zip.net/bdtjB6>. Acesso em 26 mar. 2015.

NETO, Eduardo Diniz. Sociedade de Risco, Direito Penal e Política Criminal. Ensaio: **Revista de Direito Público**, Londrina, v. 5, n. 2, 2010.

NETO, M. F.; GUMARÃES, J. A. C. Crimes na internet: elementos para uma reflexão sobre a ética informacional. **Revista CEJ**, n. 20. Brasília, 2003.

NUCCI, Guilherme de Souza. **Leis Penais e Processuais Penais Comentadas**. v.2. 7 ed. São Paulo: Revista dos Tribunais, 2013.

OLIVEIRA, Felipe Cardoso Moreira. Delitos Informáticos - Resposta Penal. In: **Leituras Constitucionais do Sistema Penal Contemporâneo**. Rio de Janeiro: Lumen Juris, 2004.

OLIVEIRA, Renata Fialho de. **Harmonização Jurídica no Direito Internacional**. São Paulo: Quartier Latin, 2008.

PINHEIRO, Emeline Piva- Crimes Virtuais: **Uma Análise da Criminalidade Informática e da Resposta Estatal**- Rio Grande do Sul, 2006. Disponível em: <http://zip.net/blthrK>. Acesso em 27 jan. 2016.

PINHEIRO, Reginaldo César. Dos Delitos praticados no âmbito da internet em face da legislação penal brasileira. **Revista de Ciência Jurídica e Soc. da Unipar**, Toledo-PR, v.5, n.1, jan./jun. 2002. Disponível em: <http://zip.net/blthsV>. Acesso em 27 jan. de 2015.

PRITTWITZ, Cornelius. A função do Direito Penal na sociedade globalizada do risco: defesa de um papel necessariamente modesto. In: Kai Ambos; María Laura Bohm (coordenadores). **Desenvolvimento Atuais das Ciências Criminais na Alemanha**. Brasília: Gazeta Jurídica, 2013.

SANTOS, Hannah Abram; BORGES, Thiago Carvalho. Desafios e Limites na Construção de um Sistema de Justiça Criminal: Uma análise crítica sobre a superação do conceito Ex Post Facto pelo Tribunal Penal Internacional. In: Wagner Menezes; Clodoaldo S. da Anunciação; Gustavo M. Vieira Org(s). **Direito Internacional em expansão**. Belo Horizonte: Arraes Editores, 2014.

SHECAIRA, Sérgio Salomão. Globalização e Direito Penal. In: Walter Barbosa Bittar. (Org.). **A criminologia no Século XXI**. 1ª ed. v. 1. Rio de Janeiro: Ed. Lumen Juris, 2007.

SILVA, Ana Karolina Calado da. O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira. **Âmbito Jurídico**, Rio Grande, XVI, n. 109, fev. 2013. Disponível em: <http://zip.net/bptjHf>. Acesso em 02 maio 2016.

SILVA, Kathy Aline de Medeiros ; RODRIGUES, F. A. . A Cooperação Jurídica Internacional em Matéria Penal e a Efetividade da Tutela Penal nos Sistemas Econômicos. In: Valeska Raizer Borges Moschen; Monica Paraguasu; Wagner Menezes. (Org.). **Direito internacional: XXI Congresso Nacional do Conpedi**. 21ed.Florianópolis: Fundação José Arthur Boiteux, 2012.

SILVA, Marco Antônio Marques da. **Acesso à justiça penal e Estado Democrático de Direito**. São Paulo: Juarez Oliveira, 2001.

SILVA, Pablo Rodrigo Alflen da. In: Salo de Carvalho (Org). **Leituras Constitucionais do Sistema Penal Contemporâneo**. Editora Lumen Juris. Rio de Janeiro, 2004.

SILVA SANCHES, Jesus Maria**. La expansion del derecho penal -Aspectos de la política criminal en las sociedades postindustriales.** 2.ed., Civitas, 2001.

SILVA, Rita de Cássia Lopes. A informação como Bem Jurídico-Penal e o Sistema Informático. In: **Direito Penal Contemporâneo- Estudos em Homenagem ao professor José Cerrazo**. São Paulo, 2007.

SOUZA, Carolina Yumi de. Cooperação jurídica internacional em matéria penal: considerações práticas. **Revista Brasileira de Ciências Criminais**, n.71 - maio-junho, São Paulo: RT, 2008.

TOFFOLI, José A. Dias; CESTARI, Virgínia C. J. Mecanismos de Cooperação Jurídica Internacional no Brasil. In: **Manual de Cooperação Jurídica Internacional e Recuperação de Ativos – Matéria Penal**. Departamento de Recuperação de Ativos e Cooperação Jurídica

Internacional, Secretaria Nacional de Justiça, Ministério da Justiça, 1ª ed. Brasília: 2008. Disponível em: <http://zip.net/bhtjc2>. Acesso 02 mai. 2016.

TOURINHO FILHO, Fernando da Costa. **Processo Penal** – 32ª ed. Rev. e atual. –São Paulo: Saraiva, v. 1, 2010.

VASCONCELLOS, Helena. **Cooperação Jurídica Internacional em matéria Penal: uma análise do *Mutual Legal Assistance treaty* Brasil/ Estados Unidos**. 2013. Disponível em: <http://zip.net/bmth0m>. Acesso em 05 mai. 2016.

VIANNA, Túlio Lima . **Do acesso não autorizado a sistemas computacionais: fundamentos de Direito Penal Informático**. 2001. 241 f. Tese (Mestrado) – Curso de Direito, Universidade Federal de Minas Gerais, Belo Horizonte. Disponível em: < http://zip.net/bstjhD>. Acesso em 28 jan. 2016.

WENDT, Emerson. **Inteligência Cibernética - A (in)segurança virtual no Brasil**. São Paulo: Editora Delfos, 2011.

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