UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO PROFESSOR JACY DE ASSIS
CURSO DE DIREITO

ANA LAURA ROSSI SILVA

CIBERCRIMES:
UMA ANÁLISE SOB A PERSPECTIVA DA APLICAÇÃO DO DIREITO INTERNACIONAL

Uberlândia - MG
2019

ANA LAURA ROSSI SILVA

CIBERCRIMES:
UMA ANÁLISE SOB A PERSPECTIVA DA APLICAÇÃO DO DIREITO INTERNACIONAL

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito, pelo Curso de Direito da Universidade Federal de Uberlândia (UFU).

Orientadora: Profa. Dra. Beatriz Côrrea Camargo

Uberlândia - MG

2019

SUMÁRIO

Cibercrimes: Uma análise sob a perspectiva da aplicação do Direito Internacional

Ana Laura Rossi Silva[*]

Resumo[**]

O surgimento e disseminação dos computadores e do acesso à internet propiciaram o aparecimento de crimes e criminosos especializados na linguagem informática, todavia no Brasil existe uma escassez normativa para regulamentação destes crimes. Nesse ponto, apura-se que seja necessário um estudo sobre o enfrentamento desses delitos na esfera penal e do Direito Internacional. O escopo do presente artigo é justamente trazer um panorama acerca da sua regulamentação no Brasil frente à aplicação do Direito Internacional, especialmente a adesão do Brasil a Convenção de Budapeste, além de investigar como essas vicissitudes contemporâneas conduzem a uma expansão do Direito Penal. Partiu-se do referencial teórico que trata do entrave entre o antigo preceito da dogmática tradicional penalista consolidada e a nova criminalidade existente, e nesse sentido, o manejo de instrumentos jurídicos internacionais viabiliza sua solução. Os métodos utilizados de investigação foram indutivos e dedutivos, a partir de revisão bibliográfica dos principais trabalhos acadêmicos, teses, artigos e outros, além de websites, livros e atos normativos. Os Cibercrimes necessita de uma roupagem que possa atender a um crime que extrapole limites territoriais e de uma dogmática diferente da consolidada no que concerne à prova de autoria; *modus operandi* e reconhecimento de uma nova

[*]Acadêmica da Faculdade de Direito "Professor Jacy de Assis", da Universidade Federal de Uberlândia (UFU). Av. João Naves de Ávila, nº 2121, Uberlândia – MG, CEP: 38.400-902. E-mail: analaura-rs@hotmail.com

[**]Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito, pelo Curso de Direito da Universidade Federal de Uberlândia - UFU, sob a orientação da profa. Dra. Beatriz Côrrea Camargo. Uberlândia, 2019.

categoria de bens jurídicos a serem protegidos, que uma vez não regulado por dispositivos normativos nacionais ou internacionais, faz sentir na sociedade como uma fonte de risco.

Palavras Chave: Cibercrimes. Expansão do Direito Penal. Direito Internacional. Novas fontes de risco.

Abstract:

The advent and dissemination of computers and internet access have laid the groundwork for crimes and perpetrators that make use of computer language, however in Brazil there's a normative shortage in regards to how these crimes are dealt with. Within these matters, it is clear that it's necessary to look into how we deal with these felonies in the realms of criminal and international law. The present study's aim is, precisely, to set up a framework surrounding virtual crimes' governance in Brazil compared to its enforcement of International Law, mainly Brazil's support of the Budapest Convention, as well as investigate how these present-day vicissitudes lead to an expansion of Criminal Law. The study builds upon a theoretical framework which deals with the hipothesis of a barrier between the old norm of traditionally consolidated criminalist dogmatics and the new existing criminality, and in this sense, the handling of foreign legal tools is key to solving it. The investigation methods here utilised were both inductive and deductive, as of bibliographical inspection of major academic works, theses, articles and others, as well as websites, books and normative acts. Cybercrimes require a fresh coat of paint so it can properly address a felony that extrapolated territorial borders, and dogmatics that are different from the established one concerning authorship evidence; *modus operandi* and recognition of a new category of legal goods to be looked after, seeing that once it's regulated neither by homeland nor foreign legal devices, reverberates across society as a source of risk.

Keywords: Cybercrimes. Expansion of criminal law. International law. New sources of risk.

1 Introdução

O presente artigo trata do cibercrime como uma figura jurídica que emerge em uma conjuntura de crescente evolução tecnológica que, por sua vez, traz em seu bojo laborioso esforço hermenêutico dos juristas na aplicação dos procedimentos penais tendo em vista a escassa e vaga legislação existente.

Há quase trinta anos a internet era apenas um projeto; o termo "globalização" nem mesmo havia sido cunhado; e a transmissão de informações por meio de fibra óptica não existia. A sociedade nas últimas décadas tem experimentado um crescente avanço na área da informática e da tecnologia. Essas mudanças permitiram que as informações circulassem entre os indivíduos em um curto espaço de tempo, independente de sua localização geográfica, o que tem favorecido maior inclusão digital.[1]

Se por um lado há vantagens do surgimento e disseminação dos computadores e do acesso à internet; por outro, surgiram criminosos especializados na linguagem informática que se apresentam como um risco à sociedade. Os crimes cometidos pela Internet causam por ano um prejuízo estimado de US$ 300 bilhões de dólares à economia global, sendo US$ 100 bilhões somente à economia norte-americana.[2] Nesse ponto, apura-se que essas ações ilícitas implicam em uma perda cada vez maior da segurança de todos, uma vez que, em sua maioria, estão relacionadas a fraudes milionárias, apologia ao crime, pornografia infantil e a demais condutas ilícitas.[3]

Todas essas condições caracterizam a emergência da sociedade de risco que, para Beck, Giddens e Lash, é a expressão que "designa um estágio da modernidade em que começam a tomar corpo as ameaças produzidas até então no caminho da sociedade industrial"[4]. Esses riscos são decorrentes de situações sobre as quais do confronto o homem não possui experiência histórica, ou seja, são aqueles resultantes

---

1 PECK, Patrícia (org.). **Direito Digital.** 6. ed. São Paulo: Saraiva, 2002. p. 01

2 COUNCIL OF EUROPE. **Convention on Cybercrime**. Budapeste, Hungria, 23 nov. 2001. Disponível em: https://conventions.coe.int/Treaty/en/Treaties/Html/185.htm]. Acesso em: 06 nov. 2019.

3 SILVA, Rita de Cássia Lopes. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.p.50

4 BECK, Ulrich; GIDDENS, Anthony; LASH, Scott. **Modernização reflexiva**: política, tradição e estética na ordem social moderna. São Paulo: UNESP, 1997. p.17.

dos impactos gerados nos processos de desenvolvimento econômico, político, social e ambiental.[5] Diante disso, a dinâmica da era da informação exige uma mudança mais profunda na própria forma como o Direito Penal é refletido e exercido em sua prática cotidiana.

Existem várias nomenclaturas utilizadas para designar um crime praticado através de um computador conectado a internet, i.e.: crimes virtuais, crimes digitais; crimes informáticos; fraude informática; delitos cibernéticos; Cibercrimes; abuso de computador; e crime de computação. Neste artigo, adotou-se como designação padrão o termo "Cibercrimes".

Tendo em vista o panorama apresentado, o objetivo deste trabalho é investigar referida figura jurídica como fonte de novos riscos no contexto de globalização. Entende-se que há um entrave entre o antigo preceito da dogmática tradicional penalista consolidada e a nova criminalidade existente. Para tal fim, este artigo esta organizado da seguinte forma: na seção 2 tem-se uma análise das definições de Cibercrimes feita por diversos doutrinadores, Organizações e Comitês; na seção 3 tratou-se das dificuldades da persecução penal; na seção 4 fez-se um estudo da repercussão dos Cibercrimes no expansionismo penal e suas controvérsias; na seção 5 abordou-se a escassa regulamentação normativa dos Cibercrimes; na seção 6 há uma abordagem acerca da necessidade de uniformização da legislação no contexto de globalização. Finalmente conclui-se o artigo na seção 7 no sentido de descrever como a adesão do Brasil á Convenção de Budapeste viabiliza a solução da escassez normativa.

2 Definições de Cibercrimes

Não há, por ora, consenso quanto à definição de Cibercrimes. A Organização para a Cooperação Econômica e Desenvolvimento (Organization for Economic Cooperation and Development - OECD), visando dar maior clareza ao assunto, conceituou o crime informático como "qualquer conduta ilegal, não ética, ou não autorizada, que envolva processamento automático de dados e/ou a transmissão de

[5] BECK; GIDDENS; LASH, 1997, p.16.

dados".[6] Efetivamente, o trabalho de aproximar-se da problemática se deu pelo Comitê Europeu para os Problemas Criminais (CDPC), que por sua vez não chegou a uma definição formal de Cibercrimes, deixando que cada país adaptasse uma classificação que lhe fosse mais funcional de acordo com seu sistema legal.

Em face ao exposto, diversos doutrinadores se debruçaram para produzir um conceito para os Cibercrimes. A partir dessas conceituações, observou-se uma subdivisão de entendimento, em que alguns recepcionam como espécie de Cibercrimes aqueles praticados por meio do computador, enquanto outros admitem apenas aqueles que atingem diretamente o computador.

Sérgio Marcos Roque admite como cibercrime "a conduta definida em lei como crime em que o computador tiver sido utilizado como instrumento para a sua perpetração ou consistir em seu objeto material".[7] Gustavo Testa Correa, nesse mesmo caminho, vislumbra que são "todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico".[8] Com efeito, o uso do computador para a maioria dos doutrinadores se torna necessário para a prática do crime.

Alexandre Jean Daoun constata, numa definição clássica, que o cibercrime se caracteriza por uma "ação típica, antijurídica e culpável com o adendo de ser cometida contra ou pela utilização de sistemas informáticos ou informatizados". Daoun destaca a importância atribuída ao objeto tecnológico informático, tanto como objeto material, quanto como meio de execução de ilícitos.[9]

Segundo Dominick Brodowski, Cibercrime é entendido como toda atividade criminal na qual a Informação e Comunicação Tecnológica (ICT) se constitui ferramenta

---

[6] SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático.** São Paulo: Revista dos Tribunais, 2003. p. 55

[7] ROQUE, Sergio Marcos. **Crimes de informática e investigação policial**. São Paulo: Justiça penal, 2000.p.32.

[8] CORREA, Gustavo Testa. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2000. p. 43.

[9] DAOUN, Alexandre Jean. **Crimes informáticos:** direito eletrônico: a internet e os tribunais. Bauru: Edipro, 2001, p. 206.

para a prática do crime ou é um alvo do crime.[10] A conduta se "dará contra o sistema informático ou com a utilização dessa tecnologia, atentando contra bens juridicamente protegidos, independentemente da natureza dos mesmos. Segundo Brodowski, esse entendimento está alinhado com instrumentos internacionais no campo, especialmente com o Conselho da Convenção Europeia de Cibercrimes. Notadamente, na Convenção não houve a delimitação do conceito de Cibercrimes, havendo apenas a conceituação de vários tipos de condutas relacionadas ao ICT.

Bem percebeu, nessa senda, Marco Aurélio Rodrigues da Costa que a maioria da doutrina define o crime de informática pelo bem jurídico protegido, conferindo uma definição incompleta. Daí a assertiva de que o crime informático é "todo aquele procedimento que atenta contra dados, que faz na forma em que estejam armazenados, compilados, transmitidos ou em transmissão. Buscando uma definição para os Cibercrimes, e fazendo menção da utilização de vantagem, Joao Marcelo de Araújo Júnior o conceituou como "uma conduta lesiva, dolosa, a qual não precisa, necessariamente, corresponder a obtenção de uma vantagem ilícita, porém praticada, sempre, com a utilização de dispositivos habitualmente empregados nas atividades de informática". Ivette Senise Ferreira de forma objetiva reconheceu como crime informático "toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão".

3 Dificuldades da persecução penal

Muito embora não seja o escopo desse artigo realizar uma abordagem criminológica[11], é mister tecer algumas considerações iniciais sobre as dificuldades de persecussão penal diante de elementos criminógenos identificados, para depois

---

[10] BRODOWSKI, Dominik. Transnational Organized Crime and Cybercrime. *In*: HAUCK, Pierre; PETERKE, Sven (ed.). **International Law and Transnational Organized Crime.** New York: Oxford, 2016. p. 334.

[11] Segundo Shecaira, a criminologia é um campo de conhecimentos interligados (interdisciplinaridade), transitando pela sociologia, histórica, psicanálise, antropologia e filosofia, todos focados no fenômeno criminal – é um arquipélago do saber. Objeto de estudo da criminologia é delito, o delinquente, a vítima e o controle social do delito. Cada um desses objetos recebe um conceito próprio. (SHECAIRA, Sérgio Salomão. **Criminologia.** 7. ed. rev.,atual. e ampl São Paulo: R. dos Tribunais, 2018. p.381).

compreendermos as possíveis soluções.[12]

A análise sob o aspecto criminológico se faz necessária à medida que reconhecemos que quando compreendemos o fator criminógeno representado pelos sofisticados sistemas informáticos e o alcance global das condutas, verificamos a necessidade de se adotar medidas de prevenção e combate a este tipo de criminalidade.

Estudos criminológicos já realizados sobre esse fenômeno apontam elementos criminógenos do processamento eletrônico de dados por várias circunstâncias, dentre elas: (a) a enorme velocidade de trabalho e rapidez nas operações; e (b) a flexibilidade e possibilidade de aplicação diversas, inclusive com relação às falhas na segurança dos sistemas de operação mais vendidos no mercado.

No que se refere a enorme rapidez nas operações, temos que as novas práticas ilícitas surgem numa velocidade proporcional às novas tecnologias, aplicativos e ao desenvolvimento e inovações da tecnologia da informação. Tais operações são praticadas à distância, de forma individual ou em grupos organizados de delinquentes, através das redes de computadores, com elevados prejuízos para os usuários comuns, corporações, Estado e o comércio internacional.

É possível compreender, nesse contexto, que há uma grande dificuldade de localização das condutas ilícitas, além da facilidade do agente em esconder o produto do crime, mesmo que este represente altas quantias. Somando-se a isso à repreensão penal, temos que, o delito pode gerar efeitos em locais diferentes, o que gera um elevado custo nas investigações para apuração dos casos, o que é, dessa forma, desvantajoso para vítima.

No tocante a flexibilidade e com relação às falhas de segurança, tem-se uma grande preocupação por parte das empresas e instituições financeiras com sua credibilidade no mercado que pode ser afetada com a divulgação de deficiências de seus sistemas de informática. Em decorrência disso, muitos dos representantes das empresas optam por ressarcir a vítima ou mesmo arcar com seu próprio prejuízo, ao invés de comunicar os crimes às autoridades para que sejam investigados.

---

[12] BOITEUX, Luciana. Crimes informáticos: reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais,** São Paulo, v.12 n.47, 2004.

Assim como as empresas mais atingidas pelo problema evitam oficializar os crimes de que foram vítimas, com receio de expor a vulnerabilidade de seus sistemas, as empresas fabricantes de sistemas informáticos também são vítimas das ações danosas. A exemplo disso temos as notícias de vírus dirigidos à Microsoft, maior fabricante mundial de programas de computador.

Ademais, conforme dados do FBI fornecidos pela análise de Ulrich Sieber, verifica-se que somente chegam ao conhecimento das autoridades americanas 1% (um por cento) dos casos, em relação aos quais somente em 3% (três por cento) são proferidas sentenças condenatórias, ou seja, de cada 22.000 autores destes delitos, somente um deles resultaria condenado pelos tribunais.[13]

Segundo Ricardo M. Mata no contexto criminológico tais condutas são de difícil averiguação e persecução e ainda de custos altos não sendo, nesse contexto, rentáveis para a vítima,

> Además las dificultades para la averiguación y persecución de estos hechos son notables: aparecen reflejados en los sistemas un elevadísimo número de procesos singulares ejecutados, con lo que la individualización del hecho se entorpece gravemente, los procesos sobre los que se ejecuta el delito no son directamente visibles y están cifrados, e incluso finalmente los costos económicos de esta tarea investigadora pueden en muchos casos no resultar rentables para la víctima. Igualmente el autor de estos hechos responde a un cierto perfil criminológico. En unos casos, sobre todo los que se produjeron al comienzo de la aparición de estas modalidades delictivas, se trata de jóvenes infractores que manejan o juegan con el ordenador durante muchas horas al día, y que sin perseguir fines.[14]

Somando-se a isso, temos na prática a dificuldade dos indivíduos e empresas no acesso à Justiça pelas razões já expostas, quais sejam: de ordem política, econômica, social e jurídica. O movimento de acesso à justiça tem descortinado essas dificuldades apontando os vários obstáculos que mitigam ou impedem esse acesso à justiça, dentre os quais enumera-se a pobreza, a falta de informação, alto custo do processo, procedimentos morosos e inadequados, organização dos serviços judiciários e

---

[13] MARTÍN, Ricardo M. Mata y. Delincuencia informática y derecho penal. Madrid: Edisofer S.L., 2001, p.38.

[14] Ibid., p.37..

legislação ultrapassada, insuficiência de recursos financeiros para a capacitação de juízes e funcionários, além de aparelhamento e modernização dos serviços judiciários, dentre outros.

4 Repercussão dos Cibercrimes no expansionismo penal e suas controvérsias

Na presente sociedade há novos paradigmas que precisam conviver com o antigo preceito da dogmática tradicional penalista consolidada, e nesse contexto, o cibercrime se constitui como um de seus desdobramentos. Para Sanchez, o progresso tecnológico permite o uso de novas técnicas que servem como um instrumento para a produção de resultados lesivos, o que reforça ainda mais a vulnerabilidade social frente a esses novos crimes que utilizam de *modus operandi* cada vez mais modernos.[15]

Contudo, a tarefa de solução é ainda mais árdua partindo da premissa que o recurso da legislação penal é utilizado como solução fácil (aparente) aos problemas sociais, e esta, frequentemente, é criticada como produto de uma espécie de perversidade do aparato estatal. Em outras palavras, observa-se que há um deslocamento ao plano simbólico, do que deveria ser resolvido no nível da instrumentalidade[16]. O resultado é insatisfatório, tendo em vista que a visão de um Direito Penal como único instrumento eficaz de pedagogia político-social, ou mesmo, como mecanismo de socialização, supõe *ad absurdum* da outrora *ultima ratio*.[17]

Sanchez defende a tese de uma expansão do Direito Penal voltado ao seu aspecto simbólico, o que não implicaria a aplicação de penas privativas de liberdade, mas sim penas restritivas de direitos ou penas pecuniárias. Dessa forma, haveria sanções meramente reparatórias.

O referido entendimento implicaria em adotar ao Direito Penal "duas velocidades".[18] Primeiramente, sob uma perspectiva minimalista, propõe uma

---

[15] SILVA SÁNCHEZ, Jesús-María. **A expansão do direito penal.** Trad. Luiz Otávio de Oliveira Rocha. São Paulo: RT, 2002, p. 35

[16] Ibid,. p. 29

[17] Ibid., p. 79

[18] Sanchez constata duas velocidades do Direito Penal. A primeira velocidade é a "da prisão", na qual se haveria de manter rigidamente os princípios político-criminais clássicos, as regras de imputação e os princípios processuais. A segunda velocidade é a de "privação de direitos ou pecuniários", em que os

preservação dos esquemas clássicos da dogmática penal para a proteção dos bens jurídicos clássicos e das garantias fundamentais dos acusados. Contudo, dá ao Direito Penal características expansionistas ao vislumbrar mais os riscos e menos a efetiva lesividade das condutas. Dessa forma, quando defende a proteção dos bens jurídicos surgidos na complexidade social acredita na necessidade da criminalização de condutas, mesmo que o fundamento esteja nos riscos gerados e não nos danos efetivamente gerados.

Com efeito, de forma contrária, Winfried Hassemer se baseia em uma postura garantista que nega ao direito penal a possibilidade de intervenção para regular as questões ligadas à nova criminalidade — como aqueles relativos aos meios de comunicação e armazenamento de dados em bases de informática. Outrossim, para o referido autor, essas atuações ilícitas não podem se adequar aos padrões de normatização próprio do Direito Penal, uma vez que exigem uma tipificação que recorra, por exemplo, aos esquemas próprios dos tipos de perigo abstrato, além de se referirem a proteção de bens jurídicos que se mostram vagamente configurados. Trata-se dos mesmos bens jurídicos e de condutas que Sanchez entende ser perfeitamente tuteláveis pelo direito penal.[19]

Neste certame, Hassemer propôs a criação de um novo sistema sancionatório, denominado Direito de Intervenção. Esse direito estaria situado entre o direito penal e o administrativo, entre o direito civil e o direito público, com regras e garantias processuais mais flexíveis, deixando de prever penas restritivas de liberdade, de modo a equilibrar as garantias com consequências penais.[20] Porém, Sanchez defende a renúncia da imputação e mesmo a previsão de penas de prisão, já que a garantia de legalidade, proporcionalidade, lesividade, prova, etc., sofreu a mencionada relativização, exigiu-se a aplicação de sanções que atingisse outros bens jurídicos que não a liberdade do imputado.

---

princípios e regras experimentam uma flexibilização proporcional à menor flexibilização proporcional à menor intensidade da sanção. SILVA SÁNCHEZ, Jesús-María. **A expansão do direito penal.** Trad. Luiz Otávio de Oliveira Rocha. São Paulo: RT, 2002, p. 180.

[19] HASSEMER, Winfried. Perspectivas Del Derecho Penal Futuro. **Revista Penal**, Huelva, v.1, p. 37-41,1998.

[20] HASSEMER, Winfried. Características e crises. **Revista de Estudos Criminais**, Madrid, v.2, n.8, p.156, 2003.

Rita de Cássia Lopes Silva reforça o entendimento de Sanchez dizendo que o direito penal, diante da nova realidade trazida pela informática, não pode continuar alheio às transformações, mas isto não significa reconhecer o surgimento de um novo ramo autônomo do direito. Segundo Silva, o que é necessário é que tais situações encontrem abrigo jurídico, mantendo-se, com isso, a paz social; mesmo porque, em matéria penal, não se pode criar toda uma nova estrutura teórica apenas porque a humanidade conheceu um novo instrumento de prática criminosa. [21]

Em face ao exposto, questiona-se se administrativização seria uma possível solução para o impasse da regularização dos Cibercrimes, de forma a permitir o procedimento e aplicação da sanção? Quanto a condutas lesivas aos bens dignos de tutela penal, vislumbramos a fragmentação em dois grupos. Em um grupo, se reconhece o direito penal para condutas que ofendam o bem jurídico de forma típica; em outro, se sustenta a sua utilização para condutas que ofendam o bem jurídico de forma atípica, isto é, condutas menos ofensivas. E nesse sentido, as condutas que restarem fora do alcance do controle penal serão destinadas a outra forma de intervenção, como a administrativa. Notoriamente, entende-se que a grande dificuldade é delimitar quais os valores deveriam ser protegidos nas interações entre indivíduos de países distintos.

Em outro giro, há diversidade de entendimento quanto à análise de quais bens jurídicos deveriam ser tutelados pelo direito penal. Nesse caso, se discute que a intervenção jurídico-penal não se aplicaria a todos os bens sujeitos a violação, mas apenas aos efetivamente relevantes. Não se buscaria tutelar aqueles socialmente irrelevantes, os chamados crimes de bagatela, cuja ofensa é de mínima expressividade e lesividade.

O Direito Penal moderno, reconhece o Supremo Tribunal Federal, tem a finalidade de tutelar os bens jurídicos mais relevantes, observando que a intervenção penal deve ter o caráter fragmentário, protegendo apenas os bens jurídicos mais importantes e em caso de lesões de maior gravidade. Neste sentido, referindo-se ao princípio da insignificância, o Min. Celso de Mello do STF, no julgamento do HC n.º

---

[21] SILVA, Rita de Cássia Lopes. **Direito penal e sistema informático.** São Paulo: Revista dos Tribunais, 2002.p. 50

84.412, publicado no DJU de 2/8/2004, afirmou que

> considera necessária, na aferição do relevo material da tipicidade penal, a presença de certos vetores, tais como (a) a mínima ofensividade da conduta do agente, (b) a nenhuma periculosidade social da ação, (c) o 82 reduzidíssimo grau de reprovabilidade do comportamento e (d) a inexpressividade da lesão jurídica provocada.

Embora a cessão de responsabilidade pelos diferentes ramos do direito fosse admitida, ainda assim se verificariam inconformidades.[22] O direito administrativo tem entrado em descrédito diante dos instrumentos de proteção por causa da contínua burocratização e, sobretudo, pela corrupção que se prolifera nesse setor. Desconfia-se das Administrações Públicas, nas quais, mais que meios de proteção, se tem buscado pelos agentes cúmplices de delitos socioeconômicos de vários tipos.

Toda essa discussão constrói um arcabouço mínimo da dicotomia entre as teorias minimalistas e expansionistas do Direito Penal.[23] Os autores que adotam a criminalização penal dos Cibercrimes se aproximam nitidamente das noções de expansionismo penal, à medida que propõem a criação de novos tipos penais utilizando-se das formulações de crimes de perigo abstrato, tipos abertos, normas penais em branco, e, consequentemente, a supressão das garantias processuais.

No outro lado da moeda estão aqueles que defendem que o expansionismo penalista têm como fundamento o movimento de "lei e ordem" que difunde o retribuicionismo acentuado como um meio político-criminal. Sustentam a necessidade de uma atuação mínima ou inexistente do Direito Penal aos Cibercrimes, e por isso, se aproximam das ideais minimalistas.[24] Tal atuação seria a mais próxima possível da *ultima ratio.*

Percebe-se que não há um consenso entre os doutrinadores quanto ao ramo que deveria empenhar esforços para proteção dos indivíduos aos crimes virtuais. Contudo, o entendimento claro é que seja necessário que tais situações encontrem abrigo

---

[22] SILVA, 2002. p.79

[23] Ibid., p. 109.

[24] SOUZA, Luciano Anderson de. **Expansão do direito penal e globalização.** São Paulo: Quartier Latin do Brasil, 2007. p. 72-82.

jurídico, inclusive penal, para que haja a referida paz social frente à sociedade de risco. Ademais, é característico do Direito Penal tutelar bens jurídicos que se veem ameaçados por condutas que os ofendam de forma ilícita.

5 Escassa regulamentação normativa dos Cibercrimes no Brasil

Trinta países, em 2001, aderiram ao primeiro tratado de prevenção e combate aos crimes praticados na internet ou com o uso do computador, na chamada Convenção sobre Cibercrimes (ETS 185).[25] A Convenção buscou obter a cooperação de todos os signatários para que fornecessem medidas legislativas locais, ações preventivas e repressivas no combate aos delitos e ofensas praticadas na internet. O Tratado possui quatro capítulos, compostos por: Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais, respectivamente. Além desses temas, possui 48 artigos incorporados num texto de fácil compreensão, sobretudo porque não traz informações muito técnicas.

O tratado surgiu diante de uma convicção da necessidade de prosseguir, com caráter prioritário, uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no espaço virtual, por meio da adoção de legislação adequada e da cooperação internacional. Entretanto, o acordo se deu apenas entre os países que compõem o bloco, embora hoje tenha mais de cem países signatários. O Brasil não participou da convenção, desse modo o país ainda não conta com uma legislação efetiva para a internet e Cibercrimes.

Diante da amplitude dos efeitos e da atuação dessas práticas delitivas, é possível concluir que há certa urgência de resposta penal que regule de forma ampla, flexiva efetiva e específica os Cibercrimes. Pensando nisso, surgiu o projeto de lei proposto em 1999 pelo deputado federal Luiz Piauhylino (PSDB/PE) e que veio a ser emendado em 2003 pelo senador Eduardo Azeredo (PSDB-SP) e, finalmente, aprovado pelo congresso em 2012, dando origem à Lei 12.735. Contudo, a Lei Azeredo teve seu veto quase que por completo sendo matéria que regulava abordada em legislação

[25] BRASIL. Ministério Público Federal. **Convention on Cybercrime Budapest, 23.XI.2001**. Budapeste, 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf . Acesso em: 06 nov. 2019.

posterior, qual seja, na Lei 12.737/2012, também conhecida como Lei Carolina Dieckmann.

A Lei 12.735 teve por objetivo "tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências". Trouxe em seu bojo artigos a serem incorporados na legislação brasileira de forma a prever e punir uma série de condutas criminosas possíveis de execução por meios digitais. [26]

Em seguida, após um longo processo de elaboração e debates, cujo início pode ser traçado ao ano de 2009, houve a aprovação no dia 23 de abril de 2014 a Lei 12.965, conhecida como o Marco Civil Regulatório da Internet, ou Marco da Internet, ou ainda, no plano internacional, como *Brazilian Internet Bill of Rights*. A criação do Marco teve por objetivo estabelecer "princípios, garantias, direitos e deveres para o uso da Internet no Brasil" e também determinar "diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios”.

Os tópicos de maior relevância e os causadores de maior polêmica são os relativos às garantias e direitos dos usuários, à garantia da neutralidade da rede e à limitação da responsabilidade dos provedores. Não obstante, a proposta aqui não é tecer comentários descritivos e detalhados dos artigos da Lei. [27]

Prosseguindo na análise da regulamentação dos Cibercrimes verificamos uma legislação específica no Código Penal dos crimes cometidos contra o computador, ou seja, contra as informações e programas nele contidos, denominados especificamente como *The computer as the object of crime (O computador como objeto de crime)*. Precipuamente, a Lei nº 12.737, de 30 de novembro de 2012, fez a inserção do art. 154-A ao Código Penal, criando o delito de invasão de dispositivo informático. Por meio desse norma penal fez-se, igualmente, a previsão do chamado crime de informática puro, no qual a conduta ilícita tem por objetivo exclusivo o sistema de computador, pelo

---

[26] MORAIS, Daniel M. G., SOUSA,Thiago C. **A Legislação sobre Internet no Brasil**: Projetos, Leis e as Questões de Liberdade e Privacidade. Disponível em: http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2013/0071.pdf. Acesso em: 06 nov. 2019.

[27] RIBEIRO, Samantha S. Moura. O Marco Regulatório da Internet. **Revista Culturas Jurídicas - RCJ,** Fluminense, v. 1, n. 1, 23 abr. 2014. p. 249.

atentado físico ou técnico do equipamento e seus componentes, inclusive aos dados e sistemas”.[28]

No art.154-A do Código Penal exigiu-se a presença dos seguintes elementos, para efeitos de caracterização do delito de invasão de delito informático, a saber: o núcleo invadir, dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança, 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.

No ano de 2016 criou-se a Comissão Parlamentar de Inquérito dos Crimes Cibernéticos com o intuito de investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade brasileira. No relatório feito em março daquele ano a CPI incluiu diversas propostas como: o não bloqueio de aplicativos de mensagens instantâneas, como o WhatsApp; que se mantenha a necessidade de ordem judicial para a remoção de conteúdos idênticos; dispôs que os provedores de internet retirassem da rede, sem necessidade de nova decisão judicial, conteúdos iguais a outros que já tiveram a retirada determinada pela Justiça, e por fim, também dispôs ampliação do crime de invasão de dispositivo informático (computador ou celular), já previsto no art. 154-A do Código Penal.

Segundo relatório final o referido artigo mereceu alteração de tal forma a abarcar condutas que deveriam ser penalizadas não se encontram abrangidas pelo tipo penal. Dessa forma, diversas alterações foram realizadas. Uma das mudanças se refere a não exigibilidade de dolo específico para configuração do delito. Isso porque o acesso indevido, independentemente da finalidade, já viola os direitos relacionados à intimidade e à privacidade da vítima.[29]

O relatório também trouxe outras alterações como a substituição do verbo “invadir” pela expressão “acessar indevidamente” e acrescentou um glossário

---

[28] GRECO, Rogério (2012). **Comentários sobre o crime de invasão de dispositivo informático**: art. 154-A do Código Penal. Disponível em: rogeriogreco.com.br/?p=2183. Acesso em: 06 nov. 2019.

[29] BRASIL. Congresso Nacional. Câmara dos Deputados. **CPI** : crimes cibernéticos, Brasília, 04 maio 2016. p. 297-299. RELATÓRIO FINAL. Disponível em:file:///C:/Users/GS%20Informatica/Downloads/RELATORIO%20FINAL%20AUTENTICADO.pdf . Acesso em: 06 nov. 2019.

com definições que trazem maior clareza sobre os conceitos como “sistema informatizado”, “dados informatizados”, e “mecanismos de segurança”.

Com relação às sanções, a pena original manteve-se, de seis meses a dois anos (mais multa), mas *apenas* por “acessar, indevidamente e por qualquer meio, sistema informatizado, ou nele permanecer contra a vontade expressa ou tácita de quem de direito”, conforme o *caput*. A reclusão para o crime cometido contra à Administração Pública aumentou para um a quatro anos, mais multa.

Destarte, a pena aumenta para seis meses a dois anos (mais multa) se do acesso resultar: prejuízo econômico; obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, arquivos, senhas, informações ou outros documentos ou dados privados; ou controle remoto não autorizado do dispositivo acessado.

Após o surgimento do artigo 154-A que dispõe: *“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”*, muitas críticas emergiram sobre o mencionado instrumento normativo. Constou-se uma falta de suporte técnico-jurídico aos legisladores na redação dos dispositivos, vez que, sob a análise do poder judiciário grande parcelas dos acessos indevidos ao sistema de informática ficariam impunes por não ser acompanhado pelo uso da “força”, como exige o tipo penal ao se valer do verbo “invadir”. Além disso, a legislação é insuficiente para apresentar definições de diversos termos técnicos inseridos na lei, o que inviabiliza a sua aplicação.

Com efeito, em apertada síntese, já experimentamos mudanças legislativas, com o condão de regular aspectos penais do ciberespaco, quais sejam: Lei Carolina Dieckmannt (lei 12.737/12), Lei n. 11.829/08 e Marco Civil da internet (Lei nº 12.965/14). A primeira se deu quando a atriz Carolina Dieckman teve fotos íntimas divulgadas na rede de maneira não consentida, por conseguinte, disciplinou por meio da lei os casos de invasão de dispositivos informáticos. A segunda trouxe um arcabouço jurídico de combate à disseminação de pornografia infantil na internet. Por fim, o Marco

Civil estabeleceu princípios para rede, além de trazer inovação no que diz respeito à previsão de direitos e deveres de usuários e provedores de acesso à internet.

Todavia, verificamos que a escassa legislação específica sobre os crimes virtuais no Brasil repercute, em muitos casos, na impunidade de criminosos, uma vez que determinadas condutas não são tipificadas e as que são, trazem lacunas e dúbias interpretações. Como sustentado nesse artigo tais preceitos normativo dispõe de termos técnicos sem apresentar definições claras, faz referência a conceitos amplos que ensejam interpretações conflitantes, além de não tutelar de maneira efetiva todos os casos de crimes informáticos.

6 Necessidade de uniformização da legislação no contexto de globalização - dogmática e territorialidade

Uma das grandes problemáticas da globalização[30] é impor ao direito penal respostas concretas que sejam jurídico-penais supranacionais tendo em vista o surgimento de novos crimes de cunho global. A globalização da economia e da sociedade exige a globalização do pensamento jurídico, de modo a encontrar mecanismos de aplicação de normas que possam extrapolar o princípio da territorialidade.[31]

Segundo Sanchez, é necessária a criação de um direito penal da globalização que tem por objetivo proporcionar uma resposta uniforme ou, ao menos, harmônica à delinquência transnacional, que evite a conformação de verdadeiros "paraísos jurídico-penais". É forçoso defender a adesão do Brasil a Convenções e tratados que busquem a uniformização legislativa dos países nessa temática. O direito segundo está perspetiva encontraria seu fundamento no direito internacional que já tem se empenhado em regular os Cibercrimes.

Para a efetiva aplicação do direito aos Cibercrimes devem ser criados princípios de relacionamento e diretrizes gerais, cujos requisitos básicos deveriam ser atendidos por todos os websites. A resolução dessas questões já possibilitaria uma segurança maior nas relações virtuais, o que não teria o mesmo êxito se fossem criadas apenas normas específicas no direito interno sem observar as de direito internacional, ficando a eficácia da sua aplicação muito limitada no tempo e no espaço.

---

[30] Terminologia empregada por Sanchez, que se refere a “globalização” econômica: “eliminação de resistências ás transações comercial e ampliação dos mercados”.

[31] PECK, 2002, p.19

No plano da dogmática jurídica penal os crimes de informática sob os efeitos da globalização manifestam necessidade de uma nova versão de delitos tradicionais. Percebe-se o surgimento de delitos impensáveis antes do descobrimento das novas tecnologias. Partindo desse entendimento, a dogmática jurídica penal informática obriga a revisar os elementos constitutivos de grande parte dos tipos penais tradicionais. Por tratar-se de um setor que sofre frequentes mudanças, suas categorias também são efêmeras e variáveis.[32]

Outro ponto enfrentado é a dificuldade judiciária no manejo de instrumentos jurídicos para aplicação do direito no caso concreto diante da extrapolação dos limites territoriais da conduta. Frequentemente averigua-se a origem do ato em local distinto aonde se deu seus efeitos, e nesse caso, questiona-se a aplicação do direito do país que deu origem ao ato ou onde ocorreram os seus efeitos. Considera-se que para os Cibercrimes o cenário é ainda mais crítico porque muitas vezes não é possível reconhecer nem mesmo o país do qual o interlocutor está falando por meio do endereço eletrônico, o que dificulta a responsabilização do agente. [33]

Em análise da redação contida no art. 5° do Código Penal observamos que aplica-se a lei brasileira, sem prejuízo das convenções, tratados e regras de Direito Internacional ao crime praticado no território nacional, adotando, assim, a teoria da territorialidade temperada. Outrossim, quanto aos crimes à distância que se iniciam em um país e terminam em outro, aplica-se a norma penal no espaço, disposta no art. 6° do Código Penal. Esse último considera praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado, adotando assim a teoria da ubiquidade.

Como já abordado, muitas vezes não é possível determinar qual o território em que aconteceram as relações jurídicas, os fatos e seus efeitos. Dessa maneira, a sociedade digital rompe com as barreiras do mundo virtual construindo um novo território, dificilmente demarcável. Além disso, nela a fonte de riqueza é a informação que é inesgotável e infinitamente duplicável, o que propicia pluralidade de danos que dificilmente são identificados.

---

[32] LUÑO, Antônio Enrique Pérez. **Ensayos de Informática Jurídica.** México, Df.: Fontamara, 2001. p. 22.
[33] PECK, 2002, p.34.

Nesse contexto, percebe-se a impossibilidade de solução do crime segundo a lei vigente. É necessário ter em vista que, num mundo cada vez mais globalizado, há a necessidade de que o direito penal acompanhe as constantes evoluções tecnológicas, com o fito de garantir a correta aplicação da lei e, por conseguinte, atingir o ideal de justiça e de promoção da paz social.

É comumente utilizado entre os filósofos sociais como forma de fazer referência aos tempos atuais a terminologia "pós modernidade" e "modernidade reflexiva", para se referir ao contexto de mudanças estruturais de vida e de uma atitude crítica a racionalidade moderna adotada pela atual sociedade.

A defesa de medidas punitivistas efetivas de caráter amplo e flexivo é necessária por se tratar-se de crimes que ganham contornos novos conforme o desenvolver da sociedade, alcançando bem jurídicos que por vezes nem mesmo são tutelados pelo direito penal. Contudo, resta elucidado que os Cibercrimes atingem diferentes países que possuem legislações internas distintas que hodiernamente se mostram insuficientes para resolver a questão dos crimes virtuais.

7 O Direito Internacional frente à insuficiência legislativa brasileira

7.1. Convenção de Budapeste

A Convenção de Budapeste criada em 21 de setembro de 2001, na Hungria, conhecida como Convenção sobre Cibercrimes, atualmente conta como signatários além dos países da União Europeia, outros que estão fora do bloco, como Estados Unidos, Canadá, Austrália e Japão, havendo ainda países latino americanos que aderiram recentemente, como Argentina, Paraguai, Chile, Costa Rica e República Dominicana e aqueles que estão no processo de adesão como a Colômbia.

A Convenção surge como forma de uniformização do direito material e processual penal das várias legislações internas que versam sobre os crimes praticados no ciberespaço nos países membros. Como consequência o tratado multilateral é um importante instrumento de melhoria legislativa relacionadas aos crimes virtuais, ampliando as formas de cooperação dos Estados parte do Sistema Internacional, além de fomentar as ações de capacitação e aprimoramento dos agentes

públicos que intervém na criminalidade.

A despeito do Brasil não ser, ainda, signatário da Convenção de Budapeste, existe atualmente um crescente movimento de defesa pela adesão do país ao referido instrumento internacional por parte especialmente de representantes de instituições que carecem de cooperação internacional para obtenção de provas digitais como indícios de materialidade e autoria de crimes. O Direito Interno brasileiro se mostra paulatinamente insuficiente para regulação dos Cibercrimes.

Como característica marcante dos crimes virtuais vislumbramos se tratar estes de condutas que ultrapassam fronteiras, e por consequência há conflitos com a competência e atuação territorial das autoridades nacionais. Diante disso, os especialistas europeus chegaram à conclusão de que somente um instrumento internacional que fosse vinculante aos países signatários poderia ter a necessária eficiência na luta contra esse novo fenômeno.

Independente de não se tratar de Convenção internacional, mas sim européia, de acordo com seu art. 37, há a possibilidade de países não-membros e que não tenham participado de sua elaboração aderirem a seus termos. Para tanto, o Comitê de Ministros do Conselho da Europa, desde que com o consenso dos países signatários da Convenção, poderá convidar qualquer Estado a fazê-lo.

Com efeito, a este ponto, o grande questionamento que se coloca é se o direito internacional, especialmente a utilização da Convenção de Budapeste, seria a "válvula de escape" para o enfrentamento dos Cibercrimes no Brasil.

Em suma, a Convenção de Budapeste tem por escopo: a) uniformizar as legislações penais substantivas; b) incentivar alterações nas legislações processuais nacionais de maneira a facilitar as investigações e persecução criminal necessárias para combater delitos praticados com o uso de sistemas de computadores, e ainda, demais delitos em que as provas devam ser obtidas mediante meios eletrônicos; c) consolidar importantes meios de cooperação internacional.

A Convenção Européia em estudo, portanto, adaptou medidas processuais tradicionais para o meio ambiente da tecnologia, além de ter criado outras inéditas, especificamente destinadas a um tipo específico de dados de computadores a serem protegidos, impondo, ao mesmo tempo, resguardo relativo à proteção aos direitos

humanos e liberdades individuais.

Nesse contexto, a uniformização promovida pela Convenção tem sido vista por vários juristas como meio de facilitar até mesmo a troca de informações entre Estados. Hodiernamente, a carta rogatória se constitui uma forma de cooperação internacional clássica, em que se solicita auxílio a outro Estado por intermédio da autoridade judiciária de um Estado.

Mostra-se importante chamar a atenção para o tratado dado pela Convenção aos crimes indicados na Convenção. Tem-se referência expressa em seu texto ao princípio da ofensividade, pois tão somente se indica a opção de criminalização das ações mais graves envolvendo o abuso no uso de computadores.

Assim, defende-se nesse artigo que no referido tratado internacional estão descritos roteiros que servirão como base para as alterações das leis nacionais, sendo certo que não se exige dos Estados-parte que eles copiem a descrição dos delitos do texto convencional, mas, ao aderirem ao tratado, estes se comprometem a adotar definições equivalentes em seus sistemas jurídicos. O entendimento está em consonância as decisões do Superior Tribunal de Justiça.

Existem inúmeros casos de prática de crimes pela internet ocorridos fora do território nacional que poderiam ter seu desfecho diferente se constássemos com apoio de instrumentos de cooperação internacional no Brasil. Em apertada síntese, no Acordão Nº 126.768 depreende-se que foi instaurado, pela autoridade Policial Civil do Estado de São Paulo, inquérito policial a fim de apurar suposta prática do crime de estelionato, que teria sido praticado em prejuízo da empresa Cavemac Indústria e Comércio de Máquinas Importação e Exportação. O Ministério Público estadual, após a conclusão das investigações, pleiteou a remessa dos autos à Justiça Federal, tendo por base que o crime, praticado pela internet, teria ocorrido fora do território nacional.

Almir Tadeu Miranda anunciou a venda de aparelhos de celular, pela internet e, após tratativas com o suposto comprador, foi-lhe enviado por mensagem de e-mail, um comprovante de pagamento falso. Induzido a erro, o vendedor enviou os aparelhos celulares para a Nigéria, onde residia o suposto comprador, pelos Correios.

Acolhendo parecer ministerial, o Juízo de Direito da Vara Criminal de Inquéritos Policiais de Belo Horizonte/MG deu-se por incompetente para conhecer dos fatos.

Tendo a vista a transnacionalidade do crime e respeitando os princípios da economia e celeridade processuais, declinou de sua competência para a Justiça Federal de Minas Gerais.

> 3. A hipótese dos autos, não há lesão aos incisos IV e V da Constituição Federal, uma vez que o particular foi vítima direta do delito de estelionato em investigação, e, apesar de os bens terem sido enviados para a Nigéria por meio de transação feita pela internet, **o próprio dispositivo constitucional exige, para o reconhecimento da competência da Justiça Federal, que o crime praticado nesse contexto transnacional tenha sido previsto em tratado ou convenção internacional,** o que não é o caso dos autos, já que o Brasil não ratificou a Convenção de Budapeste de Repressão à Cibercriminalidade, nem qualquer tratado através do qual tenha se obrigado a reprimir o delito de estelionato. (Acordão Nº 126.768 - MG (2013/0039050-5)[34]

Em primeiro lugar, não se vislumbra, na espécie, qualquer ofensa ou lesão a serviços, bens ou interesses da União (art. 109, IV, da CF). De fato, o particular, Almir Tadeu Miranda, foi vítima imediata do estelionato em investigação. Em segundo lugar, porque o simples fato de o delito possuir alguma característica transnacional ou ter sido cometido por meio da internet, não faz incidir o art. 109, V, da CF, uma vez que o próprio dispositivo constitucional exige, para o reconhecimento da competência da Justiça Federal, que o crime praticado nesse contexto transnacional, tenha sido previsto em tratado ou Convenção internacional, o que não é o caso dos autos, uma vez que o Brasil não ratificou a Convenção de Budapeste de repressão à cibercriminalidade, nem qualquer tratado através do qual tenha se obrigado a reprimir o delito de estelionato.

7.2 Jurisdição e seus limites à luz da Convenção

Trata-se de um ponto importante que manifesta a preocupação acerca dos crimes virtuais a aplicação extraterritorial de lei penal nacional, considerando que a rede mundial de computadores permite que um conteúdo gerado no Brasil, por

---

[34] BRASIL. **Superior Tribunal de Justiça**. Acórdão nº 126.768. Plenário. Relator: Ministro Ribeiro Dantas. 3ª Seção . Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/528007256/conflito-de-competencia-cc-148776-df-2016-0243766-9 . Acesso em: 06 nov. 2019.

exemplo, esteja hospedado em um servidor americano e acessado por um usuário na China.

Como forma de solução do impasse alguns países adotaram a doutrina do efeito (potencial) do crime, argumentando que mesmo encontrando-se o material hospedado em um servidor em outro país, ao poder ser acessado em território nacional, produz efeitos ali, permitindo a persecução penal.

Esta doutrina foi utilizada pela Alemanha para justificar a persecução penal em razão de conteúdo relacionado ao nazismo hospedado em servidor canadense, país onde não havia a vedação legal a este tipo de oferta de material. O resultado é que todo servidor estaria sujeito a todos os ordenamentos jurídicos do mundo, o que é impraticável e indesejável.

A Competência e Cooperação Internacional são vistas no Artigo 22º, o qual aponta quando e como uma infração é cometida, além de deixar a critério das partes a "jurisdição mais apropriada para o procedimento legal"

> Artigo 22º - Competência 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infracção penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infracção seja cometida: a) No seu território; ou b) A bordo de um navio arvorando o pavilhão dessa Parte; c) A bordo de uma aeronave matriculada nessa Parte e segundo as suas Leis; ou d) Por um dos seus cidadãos nacionais, se a infracção for punível criminalmente onde foi cometida ou se a infracção não for da competência territorial de nenhum Estado.[35]

A Convenção abre a possibilidade de cada país tratar sua competência de forma jurisdicional de forma um pouco diferente e mais detalhada, no que o § 5.º do mesmo artigo afirma que, nestes casos, os países envolvidos deverão realizar uma consulta com o intuito de determinar a jurisdição mais apropriada para a persecução. A identificação da consequência real dos crimes praticados pela internet será o fator determinante para indicação do local do crime.

---

[35] BRASIL, 2001.

8 Conclusão

Pelo exposto, nota-se que as condutas que caracterizam os Cibercrimes não possuem um alcance efetivo e claro da legislação brasileira, o que torna difícil o combate dessas condutas delituosas.

Ademais, é nítida a necessidade de uniformização do combate transnacional aos crimes cibernéticos, tendo em vista sua extraterritoridade. Para se atingir uma efetividade plena da legislação, seria necessária uma norma de regulação internacional que estipulasse parâmetros mínimos aceitáveis e, precipuamente, um sistema de cooperação internacional. Nesse ponto, diante do contexto brasileiro verifica-se que à adesão a Convenção de Budapeste é uma forma de uniformização do direito material e processual penal das várias legislações internas que versam sobre os crimes praticados no ciberespaço e que possibilitará uma repressão mais célere ao delito.

A cooperação judicial internacional, se adotada como política criminal para a Internet, tem então o potencial de fazer regredir o movimento amplo de criminalização de condutas, reservando o Direito Penal e as limitações graves a direitos fundamentais ao tempo em que forem realmente necessários.

A despeito do Brasil não ser, ainda, signatário da Convenção de Budapeste, sustenta-se ainda nesse artigo a defesa pela adesão do país ao referido instrumento internacional por parte especialmente de representantes de instituições que carecem de cooperação internacional para obtenção de provas digitais como indícios de materialidade e autoria de crimes.Como mencionado, o Direito Interno brasileiro se mostra paulatinamente insuficiente para regulação dos Cibercrimes.

Assim, a repressão dos crimes cibernéticos com a utilização de normas eficientes, práticas e quando necessárias, permitirá que a sociedade se sinta segura em meio a um contexto social de riscos gerados nos processos de desenvolvimento econômico, político, social e ambiental. Contudo, o combate aos Cibercrimes não se resolve tão somente com a edição de leis e mais leis criminais, envolve educação digital, políticas criminais e estrutura investigativa de combate ao crime digital.

Referências

BECK, Ulrich; GIDDENS, Anthony; LASH, Scott. **Modernização reflexiva**: política, tradição e estética na ordem social moderna. São Paulo: UNESP, 1997.

BRASIL. Ministério Público Federal. **Convention on Cybercrime Budapest, 23.XI.2001**. Budapeste, 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf . Acesso em: 06 nov. 2019.

BRASIL. Congresso Nacional. Câmara dos Deputados. **CPI**: crimes cibernéticos, Brasília, 04 maio 2016, p. 297-299. Disponível em:file:///C:/Users/GS%20Informatica/Downloads/RELATORIO%20FINAL%20AUTENTICADO.pdf . RELATÓRIO FINAL. Acesso em: nov. 2019.

BRASIL. **Superior Tribunal de Justiça**. Acórdão nº 126.768. Plenário. Relator: Ministro Ribeiro Dantas. 3ª Seção . Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/528007256/conflito-de-competencia-cc-148776-df-2016-0243766-9 . Acesso em: 06 nov. 2019.

BRODOWSKI, Dominik. Transnational Organized Crime and Cybercrime. *In*: HAUCK, Pierre; PETERKE, Sven (ed.). **International Law and Transnational Organized Crime.** New York: Oxford, 2016.

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

DAOUN, Alexandre Jean. **Crimes informáticos:** direito eletrônico: a internet e os tribunais. Bauru: Edipro, 2001, p. 206.

GRECO, Rogério (2012). **Comentários sobre o crime de invasão de dispositivo informático**: art. 154-A do Código Penal. Disponível em: rogeriogreco.com.br/?p=2183. Acesso em: 06 nov. 2019.

HASSEMER, Winfried. Perspectivas Del Derecho Penal Futuro. **Revista Penal**, Huelva, v.1, p. 37-41,1998.

HASSEMER, Winfried. Características e crises. **Revista de Estudos Criminais**, Madrid, v.2, n.8, p.156, 2003.

LUÑO, Antônio Enrique Pérez. **Ensayos de Informática Jurídica.** México, Df.: Fontamara, 2001.

MARTÍN, Ricardo M. Mata y. Delincuencia informática y derecho penal. Madrid: Edisofer S.L., 2001. Disponível em: http://lcweb5.loc.gov/glin/jurisdictions/Nicaragua/pdfs/231930-259339.pdf. Acesso em: 05 nov. 2019.

MORAIS, Daniel M. G., SOUSA,Thiago C. **A Legislação sobre Internet no Brasil**: Projetos, Leis e as Questões de Liberdade e Privacidade. Disponível em: http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2013/0071.pdf. Acesso em: 06 nov. 2019.
PECK, Patrícia (org.). **Direito Digital.** 6. ed. São Paulo: Saraiva, 2002.

RIBEIRO, Samantha S. Moura. O Marco Regulatório da Internet. **Revista Culturas Jurídicas - RCJ,** Fluminense, v. 1, n. 1, 23 abr. 2014. p. 249.

ROQUE, Sergio Marcos. **Crimes de informática e investigação policial**. São Paulo: Justiça penal,2000.

SHECAIRA, Sérgio Salomão. **Criminologia.** 7. ed. rev.,atual. e ampl São Paulo: R. dos Tribunais, 2018.

SILVA SÁNCHEZ, Jesús-María. **A expansão do direito penal.** Trad. Luiz Otávio de Oliveira Rocha. São Paulo: RT,2002.

SILVA, Rita de Cássia Lopes. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.

SOUZA, Luciano Anderson de. **Expansão do direito penal e globalização.** São Paulo: Quartier Latin do Brasil, 2007.