BJIR
Brazilian Journal of International Relations

77ISSN: 2237-7743 | Edição Quadrimestral | volume 7 | edição nº 1 | 2018

A oportuna e necessária aplicação do Direito Internacional nos ciberespaços: da Convenção de Budapeste à legislação brasileira

Tais Vasconcelos Cidrão,
Antônio Walber Muniz,
Ana Abigail Costa Vasconcelos Alves

Igepri
Instituto de Gestão Pública e Relações Internacionais

unesp
Universidade Estadual Paulista "Júlio de Mesquita Filho"

A Brazilian Journal Of International Relations (BJIR) está indexada no International Political Science Abstracts (IPSA), EBSCO Publishing e Latindex

A OPORTUNA E NECESSÁRIA APLICAÇÃO DO DIREITO INTERNACIONAL NOS CIBERESPAÇOS: DA CONVENÇÃO DE BUDAPESTE À LEGISLAÇÃO BRASILEIRA

Taís Vasconcelos Cidrão[1]

Antônio Walber Muniz[2]

Ana Abigail Costa Vasconcelos Alves[3]

Resumo: O objetivo primordial do presente trabalho é analisar o avanço da legislação brasileira, especialmente as leis 12.737/2012 (Lei Carolina Dieckmann) e 12.965/2014 (lei do Marco Civil da Internet), em diz respeito às inovações nas abordagens quanto aos crimes nos ciberespaços (cibercrimes). Posteriormente, far-se-á uma análise dentro do direito internacional, bem como da Convenção de Budapeste que visa solucionar as questões quanto ao mau uso da internet. Justifica-se o presente estudo através do avanço tecnológico do mundo moderno, que por sua vez contribuiu para a criação de novéis hábitos nas "novíssimas" formas de comunicação, que passaram a se valer de meios inovadores capazes de promover diálogo com as pessoas em tempo real e em qualquer lugar do mundo. Entretanto, não só no Brasil, mas emtodos os países em geral o mau uso da internet tem gerado muitos confrontos que ultrapassam as barreiras fronteiriças, como a prática de atos que violam direitos da personalidade, direito de propriedade intelectual e outros delitos criminais. Desta feita, os problemas que envolvem a internet, geralmente, têm suas repercussões extrapolando a legislação interna de cada Estado, que muitas vezes é insuficiente para resolver tal questão. Acredita-se ser, não só oportuna, mas necessária a utilização do Direito Internacional como opção catalisadora para o combate aos males que envolvem a rede mundial dos computadores. Para isso, será utilizada uma metodologia de pesquisa baseada em estudo bibliográfico de natureza qualitativa, pura em relação ao seu resultado, e descritivo-exploratória quanto aos seus objetivos.

Palavras-chave: Direito Internacional. Internet. Cibercrimes.

[1] Graduada em Direito pela UNIFOR Aluna da especialização em Direito e Processo Constitucionais pela UNIFOR. Mestranda em Direito, Acesso à Justiça e ao Desenvolvimento pela Unichristus. E-mail: taisvcidrao@hotmail.com.

[2] Professor de Direito Internacional na UNIFOR. Especialista em negócios internacionais pela UNIFOR. Mestre em Direito Constitucional pela UNIFOR. Doutor pela USP. E-mail: walber@unifor.br.

[3] Especialista em Direito Processual Civil (UECE/Escola Superior do Ministério Público) e em Direito e Relação Internacional (UNIFOR), graduada em Direito pela UNIFOR. E-mail: anaabigail27@gmail.com.

THE TIMELY AND NECESSARY IMPLEMENTATION OF INTERNATIONAL LAW IN THE CIBERSPACE: FROM THE BUDAPEST CONVENTION TO BRAZILIAN LEGISLATION

Abstract: The main objective of this work is to analyze the progress of Brazilian legislation, especially laws 12,737 / 2012 (Carolina Dieckmann Law) and 12,965 / 2014 (Internet Civil Law Law), regarding innovations in approaches to cyber crimes (cybercrimes). Subsequently, an analysis will be made under international law, as well as the Budapest Convention, which will address the issues of misuse of the internet. The present study is justified by the technological advance of the modern world, which in turn has contributed to the creation of new habits in the "newest" forms of communication, which have come to use innovative means capable of promoting dialogue with people in time real and anywhere in the world. However, not only in Brazil, but in all countries in general, the misuse of the Internet has generated many confrontations that go beyond border barriers, such as the practice of acts that violate personality rights, intellectual property rights and other criminal offenses. This time around, the problems involving the Internet generally have their repercussions, extrapolating the internal legislation of each State, which is often insufficient to resolve this issue. It is believed to be not only timely but necessary to use International Law as a catalyst for combating the evils that surround the global computer network. For this, a research methodology based on a bibliographic study of a qualitative nature, pure in relation to its result, and descriptive-exploratory in terms of its objectives will be used.

Keywords: International Law. Internet. Cybercrime.

I. INTRODUÇÃO

O surgimento da internet, entendida como um conjunto de redes interligadas de abrangência mundial, isto é, um conjunto de tecnologias para acesso, distribuição e disseminação de informação em rede de computadores certamente gerou uma grande mudança na forma de comunicação em todo o mundo. São poucas as dimensões das vidas que não se veem afetadas, dirigidas ou controladas (ainda que indiretamente) pela rede de computadores (PINHEIRO, 2007, p. 46).

No final da década de 1990, a internet começou a se popularizar mundialmente. Surgia, desse modo, a necessidade de entender aquele novo espaço social, o ciberespaço (1° SEMINÁRIO CIBERCRIME E COOPERAÇÃO PENAL INTERNACIONAL, 2009, p. 2). O fato é que a rede trouxe um novo paradigma nas relações sociais com consequências que, ainda hoje, são imprevisíveis. Fato que impõe uma nova forma de encarar estas questões fazendo com que os juristas hajam com maior sagacidade em decorrência das novas tecnologias que se apresentam no mundo globalizado. A passagem para uma era da informação vem exigindo a constituição de novos espaços e instrumentos de regulação política e jurídica que respondam as múltiplas questões que estão sendo suscitadas em sociedade.

Em decorrência deste processo, diga-se, dessa verdadeira revolução tecnológica filha da era da globalização, percebe-se claramente que se intensificamas relações sociais em escala *mundi*, que por sua vez começaram a interligar localidades distantes de maneira tal que acontecimentos locais são modelados por eventos que ocorrem a muitas milhas de distância e vice versa (PINHEIRO, 2007, p. 45). Os meios de comunicação de massa, portanto, são capazes de romper fronteiras nacionais influenciando culturas, religiões, regimes políticos, economias etc.

É sabido que, com o fenômeno da globalização e da popularização da internet, as fronteiras indelimitáveis do ciberespaço abrigaram, não apenas criações em prol da cidadania e da participação universal, como também facilitaram que crimes, comumente praticados no "mundo real", também fizessem parte do ciberespaço.

Uma das grandes discussões que circundam a utilização da internet como meio para prática de infrações penais é a dificuldade em definir o tempo e o lugar de determinada conduta criminosa, uma vez que, na *web*, inexistem fronteiras impeditivas que barrem criminosos de realizarem qualquer delito dentro do seu território (PINHEIRO, 2007, p. 46). Isso faz com que as questões que envolvem a internet sejam de alta complexidade, devido ao fato de estarem relacionadas a várias jurisdições distintas, afetando diferentes países, o que dificulta o

entendimento de qual o país seria realmente competente para processar, julgar e penalizar esses infratores cibernéticos. Com efeito, a colisão entre o Direito pátrio e o Direito alienígena quanto à questão do mau uso da Internet faz crer que, para a solução desses conflitos, há a necessidade de se socorrer ao Direito Internacional por meio de acordo de cooperação e tratados. É nesse cenário que os tratados internacionais se fazem um importante instrumento para o combate aos cibercrimes.

No Brasil, o uso da internet com fulcro de gerar danos a terceiros tem gerado muitos conflitos internos, principalmente em diz respeito à dificuldade de se aplicar normas e controles judiciais efetivos. No Ordenamento pátrio, cabe apenas ao Marco Civil da Internet e à Lei Carolina Dieckmann resolverem as demandas virtuais, que, na prática, se mostram insuficientes para dirimirem conflitos relacionados ao mau uso da internet. Dessa forma, o que se pretende com o presente estudo é analisar um pouco da legislação pátria e também a legislação estrangeira que tem sido considerada um passo a mais, já que leis nacionais não são suficientes para solucionar o problema da ubiquidade (muito embora o Brasil não seja signatário da Convenção de Budapeste).

A metodologia utilizada na investigação da hipótese foi a análise de pesquisa bibliográfica e de dispositivos legislativos. A base do estudo descritivo-analítico das fontes foi realizada mediante leitura e compreensão dos estudos publicados sob a forma de livros, revistas, artigos, publicações especializadas e outros, além dos dados e informações publicados que abordem direta ou indiretamente o tema em análise e os dispositivos legais a ela intrínsecos.

No que diz a respeito à tipologia da pesquisa, ou seja, sobre a utilização e abordagem dos resultados, é pura, à medida que não busca mudar a realidade, mas compreendê-la melhor; e qualitativa no âmbito em que busca analisar e apreciar a realidade do ordenamento jurídico pátrio e dos tratados internacionais. Quanto aos objetivos é descritiva, ao passo que buscará delinear, explicar, classificar e esclarecer o problema apresentado; e exploratória, à medida que busca aprimorar ideias através de informações sobre o tema em foco e da análise das fontes a serem apreciadas.

II. LEGISLAÇÃO BRASILEIRA E A TUTELA DO CIBERESPAÇO

A doutrina em geral classifica os cibercrimes em duas grandes modalidades, os impróprios e os próprios. Os impróprios são os "tradicionais", são os crimes comuns (à exemplo do furto, estelionato etc.) que utilizam a rede de computadores como meio para praticar outros

crimes. Já os delitos próprios, são aqueles nos quais a informática não é simplesmente objeto do crime, são os delitos contra as próprias redes de computadores (VINÍCIUS, 2013, *online*).

Prejuízos com cibercrimes no Brasil já alcançam, no ano de 2016, US$10,3 bilhões segundo uma pesquisa anual intitulada Norton Cyber Security Insights Report (NORTON, 2016, *online*). Isso, portanto, deixa o Brasil como quinto país com maior número de vítimas dos crimes pela internet. De acordo com o relatório anual, o número de ataques virtuais cresceu 10% no Brasil em relação a 2015. No mesmo ano, um total de 42,4 milhões de pessoas no Brasil foram afetadas pelo cibercrime no país, o que representa 39% do total de internautas nacionais.

O ordenamento jurídico brasileiro, entretanto, carece de leis que regulem de forma eficaz as questões envolvendo proteção de dados pessoais, cibercrimes e demandas gerais sobre segurança na internet. Há, portanto, um grande atraso legislativo combinado com uma falta de interesse dos legisladores pátrios em resolver tais questões.

O Brasil está em uma situação delicada perante a comunidade internacional, pelo fato de que, apesar de ter forte inclusão digital, a contra senso carecede normas eficazes que regulem as demandas envolvendo a rede mundial de computadores. De certo, sabe-se que a tarefa de legislar sobre um plano pouco conhecido e que envolve tecnologia de ponta e soberanias estatais é tarefa extremamente complexa. Existem muitas variáveis a serem observadas, lacunas técnicas que devem ser preenchidas e interesses dos mais diversos setores da sociedade que devem ser contrapostos.

As duas principais leis brasileiras (lei nº 12.737/12 e lei nº 12.965/14) que regulam o assunto foram frutos de acontecimentos casuísticos, isto é, sem ter tido um debate adequado acerca da temática. Dessa forma, tem-se a elaboração de leis frágeis, inócuas erepletas de lacunas jurídicas e técnicas que propiciam a insegurança jurídica.

II.1 Lei Carolina Dieckmann (Lei 12.737/2012)

A Lei 12.737/2012, que dispõe sobre a tipificação criminal dos delitos informáticos e que ao mesmo tempo altera o Código Penal (doravante chamado CP), ficou popularmente conhecida como Lei Carolina Dieckmann, tendo em vista que sua edição decorreu diretamente do fato de que a atriz nacionalmente conhecida, Carolina Dieckmann, ter sido vítima de *crackers* que invadiram seu computador e tiveram acesso a 36 fotos íntimas, tendo as publicado na internet. O fato teria, segundo especialistas, sensibilizado os parlamentares que teriam aprovado em regime de urgência as alterações no CP.

Pela urgência da aprovação é sabido que não houve tempo hábil para um amplo debate acercada temática em pauta, tendo em vista que o projeto fora apresentado em Novembro de 2011 e a transformação em Lei Ordinária deu-se em Dezembro do ano seguinte. O resultado foi apublicação de uma lei frágil, cheia de lacunas, ineficaz e que não tutela, de forma satisfatória, os cibercrimes.

A Lei 12.737 de 2012 recebe inúmeras críticas da doutrina especializada, que aponta para a ausência de definição de diversos termos técnicos, normas abertas que facilitam interpretações conflitantes, ressaltando que faltou suporte técnico-jurídico aos legisladores na redação dos dispositivos. Neste sentido, há uma grande incongruência entre a referida lei com a lei de interceptações (Lei nº 9.296, de 24 de Julho de 1996), a saber, para a elucidação da maioria dos casos de cibercrimes, necessário se faz a quebra de sigilo de dados telemáticos de um equipamento informático. Contudo, o artigo 2º aduz que:

> Art. 2°Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
> I - não houver indícios razoáveis da autoria ou participação em infração penal;
> II - a prova puder ser feita por outros meios disponíveis;
> III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção (BRASIL, 1996, *online*).

Os crimes previstos nos artigos 154-A §§ 1º e 2º, 266 §§ 1º e 2º na Lei 12.737/2012 são apenados com detenção, o que não preenche o requisito legal exigido no inciso III do artigo 2º da Lei de interceptações, que só contempla tão somente os crimes punidos com reclusão. Desta forma, a desatenção do legislador restringe o campo de atuação da polícia judiciária, tendo em vista que esta deverá se valer de outros meios de investigação na busca de provas concretas.

Acontece que, na prática, há um grande impasse, qual seja, nos delitos informáticos, a maioria das provas se encontra em meio virtual e, para sua produção, o delegado necessita solicitar ao juiz o acesso aos equipamentos envolvidos com o crime em comento. Contudo, a Lei de Interceptações em seu Art. 2º III, como visto, não permite a realização de quebra de sigilo de dados telemáticos para os crimes cuja pena é de detenção, assim os crimes punidos por detenção (que são a maiorias dos delitos da Lei Carolina Dieckmann) ficam impossibilitados de sofrer quebra de sigilo de dados ou qualquer tipo de interceptação, o que dificulta consideravelmente a produção de prova e por consequente punir o infrator.

Além disso, outra agravante deve ser levada em consideração. Os cibercrimes, punidos por reclusão, mesmo que pudessem sofrer interceptação, quando envolvem empresas multinacionais, cujo armazenamento de dados encontra-se em outro país, a lei brasileira se mostra incompetente para realização de tal diligência, cabendo, portanto, ao Poder Judiciário utilizar os recursos oferecidos no Direito Internacional para a produção de provas.

II.2 Lei do Marco Civil da Internet (lei 12.965/2014)

Outra importante lei que regula as relações jurídicas presentes na rede mundial de computadores é o Marco Civil da Internet, que garante o direito à inviolabilidade da intimidade e da vida privada do cidadão e ao sigilo de suas comunicações pela internet, comunicações privadamente armazenadas, bem como o não fornecimento a terceiros de dados pessoais, inclusive registros de conexão e de acesso a aplicações de internet.

Os incidentes de espionagem envolvendo o Governo norte-americano e outros chefes de estado, dentre eles a ex-presidente Dilma Rousseff, desencadearam uma forte pressão no Congresso Nacional para aprovação da Lei 12.965/2014 (Marco Civil da Internet). Sendo este mais um episódio clássico em que leis brasileiras são calcadas em casos concretos ao invés de se estabelecerem pelas regras gerais do direito (Atheniense, 2014, *online*).

O Marco Civil da Internet, aprovado em 24 de abril de 2014, apesar da existência muitos pontos controversos dentro do seu texto, boa parte dele da lei já havia sido discutido (o que de certa forma mostra um avanço com relação à aprovação da Lei Carolina Dieckmann). Contudo, a espionagem da agência nacional de segurança norte americana, denunciada pelo ex-funcionário Edward Snowden, terminou por catalisar a aprovação da lei e questões sensíveis tiveram que ser resolvidas sem aprofundar o debate.

Quanto o sigilo de dados, cumpre-nos destacar que a existência de elementos perniciosos no bojo do texto da nova lei é deveras preocupante, ressaltamos aqui a guarda de registro de acesso contemplada no artigo 15, vejamos:

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos **deverá manter os respectivos registros de acesso a aplicações de internet**, sob sigilo, em ambiente controlado e de segurança, **pelo prazo de 6 (seis) meses**, nos termos do regulamento. (grifo nosso) (BRASIL, 2014, *online*).

Desta feita, tal dispositivo legal roga que os usuários brasileiros terão guardados seus registros de acesso à internet por 6 (seis) meses independente de terem ou não cometido um ilícito penal na esfera cibernética, com o fulcro de facilitar investigações futuras. No entanto, esse artigo pode ser considerado uma flagrante violação ao principio da privacidade pelo fato de exigir um monitoramento integral e generalizado da população. Isso demonstra que o Estado é seriamente limitado no que diz respeito ao controle do crime na pós-modernidade. Isto é, como não consegue prover segurança para seus cidadãos, passa a marcar a política criminal com negação e gestos expressivos (GARLAND, 2008, p.430).

Outra discussão recorrente sobre privacidade na internet é a questão do direito ao "esquecimento digital", uma garantia jurídica para solicitar a exclusão de dados pessoais disponíveis na internet, tais como informações sensíveis (questões políticas e econômicas, dados médicos, religião, sexualidade) e dados individuais (perfil de compra, circulação geográfica, imagens, salário etc).

Ações isoladas por meio de legislações nacionais, ainda que juridicamente perfeitas (que não é o caso do Brasil), não conseguem eficácia no ambiente digital. À exemplo disso, os Estados Unidos da América possuem um vasto arcabouço jurídico sobre os cibercrimes, mas ainda sim, são uns dos principais alvos dos cibercriminosos.

Diante de todo o exposto podemos constatar que diversos problemas técnicos e jurídicos permeiam a seara do espaço digital dificultando a determinação da autoria dos crimes na internet. São leis frágeis e incompletas para tutelar um ambiente onde os elementos possuem características efêmeras e são dotados de complexidades tecnológicas.

Neste contexto, o Brasil sempre tratou a matéria com desídia e morosidade, beirando à irresponsabilidade. Atualmente as autoridades buscam meios de ajustar e atualizar os mecanismos legais para obter uma tutela jurídica satisfatória, criando leis que tipificam e penalizem as demandas ilegais do ciberespaço.

Conforme já observado, soluções isoladas não têm eficácia no plano do ciberespaço, sendo necessárias medidas de atuação regionalizadas objetivando a harmonização legislativa respeitando as diferenças jurídicas e tecnológicas entre os países. Urge, portanto, que a cooperação internacional se faça presente objetivando tutelar de forma satisfatória as demandas oriundas dos cibercrimes.

III. DIREITO INTERNACIONAL COMO SOLUÇÃO PARA OS CIBERCRIMES

III.1 O cenário internacional

Cientes da relevância do tema, alguns países saíram à frente e promoveram o devido alinhamento das demandas oriundas do ciberespaço. Legisladores de países como Japão, Estados Unidos, Canadá, Suécia, Argentina, bem como vários países da União Europeia não titubearam em face do problema e desde cedo adequaram suas leis internas.

Nesse sentido, Silva (2000, p. 14-17) compilou o panorama geral das legislações internacionais relacionada aos cibercrimes, que remonta ao ano de 2000, o que relata a preocupação pretérita desses países, *verbis*:

ARGENTINA - Projeto de Lei sobre Delitos Informáticos, tratando do acesso ilegítimo a dados, dano informático e fraude informática, entre outros tipos. Arts. 183 e 184 do Código Penal; Decreto 165/94, relacionado ao software;Lei 11.723, Direito Intelectual;
ALEMANHA - Código Penal, Seção 202 a, Seção 263 a, Seção 269, Seção 270 a 273, Seção 303 a, Seção 303b; - Lei contra Criminalidade Econômica de 15/05/86;
AUSTRÁLIA - Possui Legislação Federal e os Estados têm independência para legislarem sobre o assunto;
ÁUSTRIA - Lei de reforma do Código Penal de 22/12/87, que contempla os delitos de destruição de dados (art. 126) e fraude informática (art. 148);
CANADA - Código Criminal, Seção 183, Seção 242.2, Seção 326, Seção 342, Seção 342.1, Seção 430,Seção 487;
CINGAPURA - Ato de Abuso do Computador, Seção 3;
CHILE - Lei 19.223 de 07/06/93, sobre Delitos Informáticos.
CHINA - possui regulamentos para proteção da segurança de informações de computadores. Dec. 147 do Conselho Estatal da República Popular da China;
CUBA - Regulamento de Segurança da Informática em vigor desde novembro de 1996, emitido pelo Ministério do Interior; Regulamento sobre a Proteção e Segurança Técnica dos Sistemas Informáticos, de novembro de 1996, emitido pelo Ministério da Indústria Mecânica e Eletrônica; O vigente Código Penal – Lei nº 62 de 29/12/87, em vigor desde 30/04/88, modificado pelo Decreto Lei 150 de junho de 1994, traz um conjunto de figuras aplicáveis aos delitos cometidos contra sistemas informáticos.
DINAMARCA - Código Penal, Seção 263;
EGITO - Nenhuma legislação penal específica;
ESPANHA - Novo Código Penal, aprovado pela Lei Orgânica 10/1995 de 23/11/95, traz vários artigos intimamente relacionados com os crimes da informática. Ex. arts.197 a 201, arts.211/ 212, art.248, arts. 255/256, art.279, art.278, art.400, art. 536;
ESTADOS UNIDOS - Ato Federal de Abuso do Computador (18 USC. Sec. 1030), que modificou o Ato de Fraude e Abuso do Computador de 1986; Ato de Decência de Comunicações de 1995; Ato de Espionagem Econômico de 1996; Seção 502 do Código Penal relativo aos crimes da informática; Os Estados têm independência para legislar sobre o assunto;
FINLANDIA - Código Penal, Capítulo III, art.323.1, art.323.2, art.323.3, art. 323.4;
FRANÇA - Novo Código Penal, Seção 202 a, Seção 303 a, Seção 303 b; - Projeto de Lei relativo a criminalidade informática. - Lei 88-19 de 05/01/88 sobre Fraude Informática;
GRÉCIA - Código Criminal, art. 370c, par. 2;
HONG KONG - Ordenação de Telecomunicação, Seção 27 a, Seção 161;
IRLANDA - Ato de Dano Criminal de 1991, Seção 5;
ISRAEL - Possui Lei de 1979 relacionada a crimes informáticos;
ITÁLIA - Código Penal, art.491, art.615, art.616, art.617, art.621, art.623, art. 635. Lei 547 de 23/12/93 (modifica e integra norma ao Código Penal e ao Código de Processo Penal em tema de criminalidade informática); Lei 675 de 31/12/96 sobre a Tutela da Privacidade;
JAPÃO - Tem legislação penal relacionada a crime de computadores;
LUXEMBURGO - Ato de 15/07/93, art. 509.1;
MALASIA - Ato de Crimes do Computador de 1997; Ato de Assinatura Digital de 1997;
NORUEGA - Código Penal, par. 145, par.151b, par. 261, par. 291;
PAÍSES BAIXOS - Código Criminal, art. 138a;
PORTUGAL - Lei de Informação Criminal nº 109 de 17/08/91. Lei de Proteção de Dados Pessoais, 67/98 de 26/10/98; Constituição Portuguesa, art. 35; Código Penal, arts. 193 e 221;
REINO UNIDO - Ato de Abuso do Computador de 1990, Cap. 18;
SUÉCIA - Lei de Dados de 1973, com emendas em 1986 e 1990, par. 21;
SUIÇA - Código Penal, art. 143.

Apesar de todos esses países terem promovido uma evolução de seus ordenamentos jurídicos internos, o combate eficaz ao cibercrime não pode permanecer circunscrito a uma

nação, ou seja, a um sistema jurídico isolado, pois o próprio princípio explícito do ciberespaço permite que o cibercriminoso transponha fronteiras com extrema facilidade e velocidade. É por isso que a filiação à Convenção de Budapeste, que será vista mais a frente, devido o seu caráter internacional, acertadamente propõe uma harmonização das normas jurídicas referentes aos cibercrimes dos países signatários, o que ajudará efetivamente a combater tais delitos na internet.

III.2 Tratados e Convenções que se sobrepõem à insuficiência do Direito interno brasileiro

Em vários aspectos, a vida passou a ser cada vez mais dependente da internet, porém autilização maldosa da rede mundial de computadores pode incentivar a pratica de atos de violação de direitos de personalidade, direito de propriedade intelectual e delitos criminais, todos estes com efeitos transnacionais e multiterritoriais.

> Marcos jurídicos têm sido aprovados com a ambição de estabelecer parâmetros, princípios, garantias, direitos e deveres no mundo digital. Se os avanços da tecnologia da informação e das comunicações podem ameaçar e violar direitos, também têm a potencialidade de promover e fortalecer esses mesmos direitos (ONU, 2018, *online*).

A formação de redes entre poderosas organizações criminosas e seus associados, com atividades compartilhadas em todo o planeta, constitui um novo fenômeno que afeta profundamente a economia no âmbito internacional e nacional, a política, a segurança e, em última análise, as sociedades em geral (CASTELLS, 2007, p. 203).

É notório que, com o fenômeno da globalização e da popularização da internet, as fronteiras indelimitáveis do ciberespaço infelizmente não abrigaram somente as criações em prol da cidadania e da participação universal. Mais uma vez se retoma Castells, quando este afirma, por exemplo, que a "internacionalização das atividades criminosas faz com que o crime organizado [...] estabeleça alianças estratégicas para cooperar com as transações pertinentes a cada organização, em vez de lutar entre si" (CASTELLS, 2007, p. 205).

É importante salientar a discussão acerca da dificuldadede se definir o tempo e o lugar de determinada conduta cibernética criminosa. A dificuldade está no fato de estarem correlacionados com o local em que se consumam, e, por consequência, podendo englobar a jurisdição de vários países distintos. É imprescindível que esses crimes sejam investigados e identificados em escala *mundi*, mas qual o país competente para processar, julgar e penalizar os infratores?

Nesse caso, Tratados e/ou Convenções internacionais poderiam ser mias efetivos quando da soluçãodo problema, tendo em vista que, em sendo a internet um meio de comunicação que

ultrapassa limites e fronteiras de qualquer país, seria pouco provável que somente leis nacionais de cada Estado conseguissem definir como, quando, onde e qual legislação seria responsável por determinada conduta delituosa de um indivíduo.

Assim, nas discussões e elaborações legislativas internacionais sobre delitos na internet vem se concluindo que não há mais como cogitar soluções nacionais para eles, devendo o assunto ser debatido em âmbito internacional, já que estes fenômenos são influenciados diretamente pela globalização, sendo praticados de forma célere e com ultrapassagem de fronteiras geográficas dos países, com interdependência de ações praticadas em diversos locais (BOITEUX, 2004, p. 170).

Um bom exemplo dessa problemática é referente à suspensão judicial do aplicativo "WhatsApp" por desobedecer as de decisões da Justiça brasileira, fato esse que prejudicou milhões de brasileiros. As organizações criminosas se utilizam do aplicativo para cometer delitos, sabendo disso, o Poder Judiciário requereu inúmeras vezes à empresa responsável pelo aplicativo os dados das conversas dos criminosos envolvidos, pedido esse que foi negado pela empresa. De acordo com o Marco Civil da Internet os dados são protegidos e só podem ser revelados por decisão judicial. A empresa, no entanto, alegou que os dados criptografados não podem ser fornecidos, visto que tais informações exigidas pela Justiça estão armazenadas em banco de dados localizado nos Estados Unidos, ou seja, em regime jurídico distinto do brasileiro. Como dirimir o conflito?

Os tratados e/ou convenções internacionais têm a função de "universalizar" (pelo menos dentre os signatários) algumas leis para que todos os países membros tenham maior facilidade em resolver algumas questões nessas horas (BOITEUX, 2004, p. 166). Portanto, há urgente necessidade de se facilitar a cooperação internacional como meio eficaz de combate a esse tipo de criminalidade bem como os demais problemas envolvendo o mau uso da rede mundial de computadores. Os programas de computadores utilizados por usuários do mundo todo são praticamente os mesmos. Nessa medida, frente à importância dada a esse assunto e as características globais próprias da internet, a existência de várias leis nacionais com o intuito de legislar sobre eles poderia levar à criação de paraísos criminais e não resolveria os conflitos no meio cibernético (BOITEUX, 2004, p. 166-167).

III.3 A Convenção de Budapeste

A Convenção de Budapeste (também conhecida como Convenção sobre o Cibercrime - CETS nº 185) foi elaborada em 21 de setembro de 2001 com mais de quarenta países-membros

signatários, dentre os quais Estados Unidos da América, Canadá, Japão e África do Sul, postula a produção de uma política criminal comum para fornecer proteção à sociedade contra a criminalidade no espaço virtual, enfatizando a necessidade de se ter uma legislação adequada com o desenvolvimento tecnológico atual.

A Convenção de Budapeste em geral propiciou a realização de um tratado internacional que buscava harmonizar as legislações penais e processuais sobre cibercrimes. É o mais amplo instrumento jurídico que busca na cooperação internacional meios para se combater os cibercrimes, tratando ainda especificamente da segurança de redes de computadores, das violações de direitos autorais, da fraude por meio de computadores e da pornografia infantil. O respectivo acordo entrou em vigor em 01 de julho de 2004 e conta hoje com 5 países signatários e 55 adesões com ratificações (COUNCIL OF EUROPE, 2017, *online*).

Cientes da potencialidade dos cibercrimes e "Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation" (COUNCIL OF EUROPE, 2001, *online*), o Conselho Europeu se debruçou sobre a temática buscando equacionar a tutela jurídica em consonância com a soberania dos países membros. Nessa convenção, o espaço cibernético foi definido como um tipo de espaço comum que é usufruído por todos aqueles que trafegam na internet ao se conectarem aos serviços de comunicação e informação (BOITEUX, 2004, p. 170).

Os redatores da Convenção de Budapeste debateram aspectos importantes como o direito material, processual e a competência. Diante disso, tal convenção foi elaborada não somente para criar novos tipos penais, mas também para estipular normas de processo penal, conciliando procedimentos de direito penal internacional e estabelecendo acordos referentes à tecnologia da informação (BOITEUX, 2004, p. 170).

Com relação ao direito material, a mencionada Convenção definiu e tipificou os cibercrimes quanto ao acesso e interceptação ilegítima, interferência de dados e de sistema, uso abusivo de dispositivos, falsidade informática, fraude informática, como também a pornografia infantil virtual e violação de direitos autorais. Outras condutas delituosas controvertidas, tais como o jogo ilegal pela internet e o terrorismo cibernético, foram deixadas de fora da Convenção para que cada Estado pudesse decidir criminalizá-las ou não. Já em relação à responsabilidade de pessoa jurídica, a Convenção se restringe apenas a dizer que ela poderá ser responsabilizada criminal, civil ou administrativamente. É interessante destacar que todos os crimes definidos na referida Convenção são dolosos, ou seja, não se admite a possibilidade de

conduta delituosa perpetrada por meio de computador sem que tenha havido a verdadeira intenção de fazê-la (BOITEUX, 2004, p. 171).

Além do mais, no que tangeria à modificação da legislação nacional, tal Convenção dispõe de alguns roteiros que têm como objetivo maior fazer com que os países signatários se comprometam a adotá-los em seus sistemas jurídicos, não sendo exigido, entretanto, que estes venham a copiá-los podendo somente utilizar definições equivalentes.

A Convenção de Budapeste é atualmente o único instrumento jurídico de caráter global para o combate hábil aos cibercrimes. Contudo, acredita-se que a Convenção peca por tratar todos Estados signatários de forma idêntica não levando em consideração as discrepâncias e os hiatos tecnológicos de cada país.

Destaca-se que o Brasil não é signatário da Convenção de Budapeste sobre cibercrimes. Fato este que merece atenção, pois, ainda que se aponte lacunas na respectiva Convenção, vislumbra-se total capacidade técnica e jurídica nacional para recepcionar o Tratado. A importância desta análise para o direito brasileiro refere-se ao fato de que os crimes praticados pela Internet, sejam eles tradicionais ou não, estão em conflito direto com a competência e atuação territorial das autoridades nacionais, uma vez que as leis nacionais têm sua aplicação limitada a um território específico e são totalmente ineficientes no que tange à violação aos direitos humanos e às liberdades individuais. Desse modo, somente um instrumento internacional poderia ter eficácia na luta contra estes crimes.

Além da compatibilidade entre o ordenamento brasileiro e a referida convenção, a escassez de leis específicas sobre o tema dentro do Brasil tem dificultado a aplicação da justiça nos casos concretos. Possivelmente, essa realidade seria alterada caso o Brasil se tornasse signatário, já que a cooperação internacional estaria a seu favor.

IV. CONCLUSÃO

Atualmente a sociedade globalizada busca regularizar o uso da internet de forma a preservar o direito à liberdade, à privacidade e à segurança jurídica. Questões como comércio eletrônico internacional, proteção propriedade intelectual, espionagem, infrações penais e a cooperação internacional são temas discutidos mundialmente. Mas, devido ao corte epistemológico do presente estudo, o foco foi direcionado mais para a doutrina brasileira (ou a insuficiência dela) e seu papel na resolução dos cibercrimes. Apesar de ser um tema discutido, como dito anteriormente, as legislações nacionais e estrangeiras ainda estão ganhando força e tomando seu espaço dentro do direito internacional.

A internet ainda não apresenta exatamente um sistema de centros decisórios e de convergência normativa que permitam uma regulação uniforme pelo Direito. As tecnologias ali existentes não podem ser comparadas com as formas tradicionais de comunicação, o que evidencia, em larga medida, o caráter inédito das relações privadas e públicas, quando comparadas com aquelas tradicionalmente concebidas no domínio do Direito.

As atividades delituosas no mundo cibernético cresceram e ganharam proporções juntamente com a força e evolução das tecnologias, dados pesquisados revelaram que os cibercrimes se tornaram uma epidemia global silenciosa afetando milhões de pessoas. Pela complexidade estrutural e ubiquidade da internet, pelas frágeis leis que regulam o ciberespaço e pela ineficácia (em termos práticos) das leis internas de um país somada à dificuldade de identificar e processar criminosos virtuais, os cibercriminosos atuam quase livremente certos da impunidade.

Alguns países desenvolvidos já se debruçaram em busca da solução para a tutela eficaz do ciberespaço, no entanto, no âmbito internacional alguns poucos se tornaram signatários da Convenção de Budapeste (CETS nº 185), sendo até hoje o mais amplo instrumento jurídico que busca na cooperação internacional meios para se combater os cibercrimes. O Brasil não tratou de assinar a Convenção de Budapeste, cabendo apenas ao Marco Civil e a lei Carolina Dieckmann resolverem demandas virtuais, o que na pratica restou insuficiente devido a suas lacunas jurídicas.

Acredita-se que a tutela isolada não consegue ser efetiva para o combate aos cibercrimes, haja vista a sua ubiquidade e as diferenças de desenvolvimento tecnológico e jurídico dos países. É por esse motivo que os tratados internacionais são um importante instrumento no combate aos cibercrimes, pois permitem a cooperação entre diferentes soberanias.

Em uma breve análise asseveramos que a solução para a problemática apresentada é bastante sensível, posto que elementos de controle podem atingir o seio do ambiente virtual acabando definitivamente com o elemento mais fundamental da internet: a liberdade. Se faz necessário, portanto, um esforço global, atuando em vários segmentos sociais. Leis bem elaboradas, homogêneas e atualizadas com as demandas inerentes ao ciberespaço e processos céleres que se amoldem à dinâmica dos cibercrimes são imprescindíveis para uma tutela eficaz.

REFERÊNCIAS BIBLIOGRÁFICAS

1° SEMINÁRIO CIBERCRIME E COOPERAÇÃO PENAL INTERNACIONAL, 2009, Paraíba. Anais. UFPB e Association Internacionale de Lutte Contra La Cyber criminalite (França), 2009.

ATHENIENSE, Alexandre. Direito sem Papel: Aprovação do Marco Civil foi pautada por evento internacional. **Conjur**, 2 mai. 2014. Disponível em: <https://www.conjur.com.br/2014-mai-02/direito-papel-aprovacao-marco-civil-foi-pautada-evento-internacional>. Acesso em: 23 abr 2018.

BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. **Revista Brasileira de Ciências Criminais**. São Paulo: Revista dos Tribunais, 2004.

BRASIL. Lei 12.737 de 30 de Novembro de 2012. **Diário Oficial da União**, Brasília, DF, 13 ago. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato20112014/2012/lei/l12737>. Acesso em: 17 jan. 2017.

BRASIL. Lei 9.296 de 24 de Julho de 1996**. Vade Mecum Acadêmico de Direito Rideel**. 24ª ed. São Paulo: Rideel, p. 1020.

BRASIL. Lei nº 12.965, de 23 abril de 2014. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2011/2014/lei/l12965.htm>. Acesso em: 30 abr. 2017.

CASTELLS, Manuel. **Fim do Milênio**: A Era da informação: economia, sociedade e cultura; v. 3, 4ª ed. Trad.: Klauss Brandini Gerhardt e Ronei de Venancio Majer. São Paulo: Paz e Terra, 2007.

COUNCIL OF EUROPE. Chart of signatures and ratifications of Treaty 185. 16 jun. 2017. Disponível em: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=44BgUu5q>. Acesso em 16 jun. 2017.

COUNCIL OF EUROPE. Convention on Cybercrime. 23 nov. 2001. Disponível em: <https://rm.coe.int/1680081561>. Acesso em: 16 jun. 2017.

GARLAND, David. **A cultura do Controle:** Crime e ordem social na sociedade contemporânea. Rio de Janeiro: Revan, 2008.

NORTON. Norton Cyber Security Insights Report 2016: Comparação Global. Disponível em:<https://www.symantec.com/content/dam/symantec/br/docs/reports/2016-norton-cyber-security-insights-comparisons-brazil-pt.pdf>. Acesso em: 28 jun. 2017.

ONU. **Internet e direitos humanos**. Disponível em: <https://nacoesunidas.org/artigo-internet-direitos-humanos/>. Acesso em: 23 abr. 2018

PINHEIRO, Patrícia P. **Direito Digital**. 2. ed. São Paulo: Saraiva, 2007.

SILVA, Remy Gama. **Crimes da Informática.** Editora: Copy Market, 2000.

VINÍCIUS, Marcus. **O lado sombrio da internet**. Revista Exame. Disponível em: <http://info.abril.com.br/noticias/internet/2013/09/lado-sombrioweb.shtml>. Acesso em 10 jan. 2017.

Recebido em: julho/2017

Aprovado em: maio/2018.