

A CONVENÇÃO DE BUDAPESTE É UM MODELO DE ALTERNATIVA PARA SOLUÇÃO DOS CONFLITOS NO MUNDO VIRTUAL?

Francisca da Glória Menezes de Oliveira*

Bernardo de Oliveira Neto**

RESUMO

As novas tecnologias mudaram as formas das pessoas se inter-relacionarem, criando duas realidades: uma virtual e outra física. A conexão virtual vem gerando benefícios e prejuízos incontáveis para a comunidade internacional. O uso doloso da internet tem violado direitos humanos, direitos de personalidade, direitos civis (propriedade intelectual) e sobretudo causado delitos penais. A rapidez da comunicação vem contribuindo para a multiplicação de condutas criminosas na rede mundial de computadores. Combatê-las tem sido um desafio para o Judiciário. Essas condutas delituosas atravessam fronteiras em questão de segundo. Os conflitos de competência para aplicação da justiça são constantes. Como julgar, processar e condenar um infrator que está do outro lado do globo, causando dano em vários continentes simultaneamente? A Convenção de Budapeste é um modelo que sinaliza para uma possível resolução de conflitos supranacionais. É urgente que a sociedade global compreenda que somente por meio de Convenções e Tratados Internacionais é que haverá a criação de legislações comuns capazes de combater crimes virtuais de natureza internacional.

Palavras-chave: CONDUCTAS VIRTUAIS CRIMINOSAS, VIOLAÇÃO DE DIREITOS, CONVENÇÕES E TRATADOS INTERNACIONAIS.

ABSTRACT

New technologies have changed people's ways of interrelating, creating two realities: one virtual and one physical. The virtual connection has been generating countless benefits and losses for the international community. The malicious use of the internet has violated human rights, personality rights, civil rights (intellectual property) and above all caused criminal offenses. The speed of communication has contributed to the proliferation of criminal conduct in the world wide web. Fighting them has been a challenge for the judiciary. These

*Mestranda em Direito Internacional dos Direitos Humanos na Unisantos. E-mail: franciscamenezes@bol.com.br

** Mestrando em Direito Internacional dos Direitos Humanos na Unisantos. E-mail: adv.bernardo@gmail.com

criminal conduct cross borders in a matter of seconds. Conflicts of jurisdiction for the application of justice are constant. How to prosecute and convict an offender on the other side of the globe, causing damage to several continents simultaneously? The Budapest Convention is a model that signals a possible resolution of supranational conflicts. It is urgent that global society understands that only through international conventions and treaties will it be possible to create common laws capable of combating virtual crimes of an international nature.

Keywords: CRIMINAL VIRTUAL CONDUCT, VIOLATION OF INTERNATIONAL RIGHTS, CONVENTIONS AND TREATIES.

1 INTRODUÇÃO

O modo como as pessoas se relacionam na presente década sofreu bastante alteração. O mundo virtual se tornou palco dos mais diversos conflitos (civis, criminais, etc). A rede mundial de computadores proporcionou os mais relevantes ganhos, como também os mais inesperados conflitos e problemas. Ocorre que essa interligação informática não retroagirá, pelo contrário, gradativamente alcançará mais pessoas e regiões.

O processo de globalização se acentuou após a segunda guerra mundial em decorrência do avanço tecnológico. A partir da concretização da interligação não só das máquinas, mas sobretudo dos indivíduos, todas as relações humanas foram respingadas. O que se flagram são grandes transformações no mundo jurídico, comercial, nas relações afetivas, etc. Com tantas divergências nos mais variados pilares da vida, o que desponta é encontrar alternativas novas para resolução dos mais diversificados fenômenos sociais postos em evidência no mundo virtual.

A nova maneira dos indivíduos se relacionarem com os demais (Estado, Organizações, pessoas) via rede mundial de computadores necessita urgentemente de regras claras e práticas para coibir todas as formas de abusos/crimes. O mundo jurídico já não consegue solucionar os conflitos atuais, utilizando conceitos e regras antigas. O novo ambiente de litígios surgidos pelo uso da internet no ciberespaço requer proteção jurídica do Estado da mesma forma que os decorrentes do tempo/lugar/espacos delimitados geograficamente.

A Convenção de Budapeste surge como a melhor alternativa para solucionar os mais diversos conflitos do mundo virtual. A importância jurídica desse instrumento internacional ganha relevo no mundo acadêmico/jurídico. Os principais desafios para punir as

transgressões do mundo virtual é exatamente como determinar o tempo e o lugar das infrações. As ações delituosas não são delimitadas por fronteiras físicas, já que os homens e as máquinas estão interligados globalmente. Somente se valendo de Tratados e Acordos Internacionais é que será possível evitar a colisão do Direito interno com o Direito alienígena.

Desse modo, arrimado na complexidade de o Estado responder com eficácia às instabilidades desses novos modelos de relações sociais surgidos no ciberespaço, é que o presente trabalho se propõe a analisar a aplicabilidade da Convenção de Budapeste. Imerso nessa temática, será verificada a questão da relatividade com que os conceitos tradicionais jurídicos (Estado, Jurisdição, Soberania, territórios) estão sendo compreendidos pelos aplicadores do direito. Pretende-se ainda identificar alguns casos concretos de conflitos de jurisdição/competência de ordem internacional, pesquisar sobre a importância da Criação da Convenção de Budapeste e verificar os objetivos do documento.

A estratégia de investigação para abordagem da temática sugerida será através de consultas a fontes bibliográficas: livros, legislações, artigos científicos, revistas acadêmicas. Com o resultado da pesquisa, almeja-se poder contribuir com o mundo acadêmico para o entendimento da problemática em questão. Incentivar e provocar os interessados a pensarem sobre as crises levantadas, possibilitando o surgimento de novas ideias, e quem sabe novas resoluções para os dilemas jurídicos do campo cibernético.

2. OS CONCEITOS TRADICIONAIS DE ESTADO, JURISDIÇÃO, NACIONALIDADE X A APLICABILIDADE NO CIBERESPAÇO

Convém lembrar os ensinamentos de Rezek (2011, p.193s) que conceituam Estado como sendo uma personalidade originária de direito internacional público. A esse ente jurídico estão vinculados os seguintes elementos: território, povo e uma forma de governo. No tocante à definição de Jurisdição (competência), afirma que o Estado detém autoridade perante seu território, o qual é delimitado fisicamente por aspectos geográficos (espaços terrestres, hídricos, aéreos). Leciona ainda que essa soberania do Estado o legitima a exercer jurisdição geral e exclusiva. A primeira permite abarcar competências legislativa, jurisdicional e administrativa. A segunda, competência exclusiva, o Estado não concorrerá com outra soberania.

A maneira como o estado se manifesta em sua dimensão pessoal é por meio da nacionalidade. Esse vínculo jurídico existente entre os cidadãos e o Estado é que permite este

legislar sobre aqueles, tendo competência para julgar todas as ações referentes aos respectivos nacionais¹.

A partir dessas definições tradicionais de Jurisdição, Estado, Nacionalidade, de há muito surgiram controvérsias para aplicação da “Justiça”. Algumas situações das relações sociais ficavam impunes. Como o Estado estava adstrito a exercer jurisdição para seus nacionais, o que fazer para solucionar conflitos envolvendo estrangeiros já que a máxima era a regra costumeira: *par in parem non habet iudicium*: O Estado não pode ser submetido contra sua vontade a qualquer foro doméstico.² Entretanto, essa ideia absoluta de soberania passa a se tornar mais flexível. Veja-se o que afirma Rezec (2011, p. 207):

A ideia da imunidade absoluta do Estado estrangeiro à jurisdição local começou a desgastar-se já pela segunda metade do século XX nos grandes centros internacionais de negócios, onde era natural que as autoridades reagissem à presença cada vez mais intensa de agentes de soberanias estrangeiras atuando não em funções diplomáticas ou consulares, mas no mercado, nos investimentos, não raro na especulação. Não havia por que estranhar que ingleses, suíços e norte-americanos, entre outros, hesitassem em reconhecer imunidade ao Estado estrangeiro envolvido, nos seus territórios, em atividades de todo estranhas.

No século XXI, em virtude do fenômeno da globalização, as formas de se estabelecerem relações pessoais, econômicas, sociais vêm permitindo reconfigurações nos modos de controle já existentes. Assim, pode-se afirmar que o ciberespaço estabelece um elo concomitante entre o que é físico e virtual. Entretanto, a disputa entre esses dois mundos é um desafio para o Direito. Como implementar normas que sejam comuns nesse novo contexto? Essa realidade causa temor e o sentimento de impossibilidade de controle jurídico ou político, nesse sentido escreveu ANTAS, (2005, P.65):

Diante das gigantescas mutações introduzidas pela globalização e pelo nascimento de novos poderes, que escapam do tradicional controle político e jurídico, e perante a possibilidade de uma revolução permanente, como parece o progresso telemático em ação, é difícil ter certeza quanto ao futuro da democracia e se a história humana se encaminha para o aumento da desigualdade e marginalização, ou, então, para uma democracia internacional, baseada na garantia dos direitos do homem em relação aos Estados e aos velhos e novos poderes.

Convém refletir acerca das definições de ciberespaço. As literaturas que tratam do assunto noticiam que o responsável pela criação da expressão foi o escritor californiano, William Ford Gibson, o qual é autor do livro *Neuromancer* escrito em 1984.³ A obra prospera em torno de uma narrativa sobre um hacker que visualiza a possibilidade de cometimento de

¹ REZEC, Francisco. Direito Internacional Público – Curso Elementar -13ª edição revista, aumentada e atualizada 2011 - SARAIVA

² REZEC, (2011, p. 213)

³ GIBSON, W. *Neuromancer*. Trad. de Alex Antunes (baseada na tradução da 1ª ed. de Maya Sangawa e Silvio Alexandre). 3. ed. São Paulo: Aleph, 2003

infrações no ambiente virtual. Essa descoberta o faz perceber que esse mundo desmaterializado é mais seguro para o anonimato. Essa publicação representou um marco histórico porque abordou conceitos inovadores sobre ações/omissões na internet.

Para Levy, Albuquerque (1995, P.157) ciberespaço é a conexão mundial de computadores e equipamentos eletrônicos que resultou na desterritorialização da realidade. Os espaços que outrora foram definidos geograficamente migraram para a dimensão virtual.

Infere-se então que todos os aparatos tecnológicos fizeram surgir duas realidades: a virtual e a física. Com isso, não se admite delimitação territorial, pois as pessoas estão inter-relacionadas eletronicamente sem qualquer empecilho, limite geográfico. Desse modo, os conceitos tradicionais de fronteiras, a exigência de presença física, distâncias são totalmente irrelevantes para que se ocorram crimes virtuais. A teor dessa ideia, Albuquerque (2006) menciona que crianças norte-americanas (New York) invadiram virtualmente bancos de dados canadenses, os quais detinham informações de caráter nacional. Do mesmo modo, relata que a National Aeronautics and Soarce Administration (NASA) foi atacada em seus bancos de dados informáticos.

O mundo virtual gera dificuldades tais como identificar qual seria o lugar do crime ou qual seria a autoria em situações delineadas como nos exemplos anteriores. Nesse diapasão, ensina Albuquerque (2006), que nos crimes cibernéticos o lugar do crime pode variar do seguinte modo: praticável entre um país e outro, entre vários países. De modo sintético, o iter criminis tanto poderá ocorrer em um só local ou em várias localidades. Também será dificultoso identificar as autórias de tais crimes em face da rapidez com que as informações se multiplicam em razão da transmissão via protocolos TCP/IP.⁴

A partir dessa realidade, diante de situações semelhantes às delineadas acima, surgem os seguintes questionamentos: Se um fato delituoso percorre dois ou mais países, quem seria a nação competente para julgamento?⁵ Em face da ausência de fronteiras é que se multiplicam as condutas delituosas no ciberespaço, dificultando também a identificação dos infratores. Uma possibilidade de resolução desses conflitos é relativizar os conceitos já firmados de jurisdição e competência.

Dentre os princípios que regem a ideia de jurisdição, vale destacar os seguintes: princípio da proteção ou protetivo e o princípio da jurisdição universal. O primeiro assegura que uma conduta delituosa fora dos limites da jurisdição do país vitimado, possa ser

⁴ CASTRO, Carla Rodrigues Araújo de. Crimes de informática e seus aspectos processuais. 2. ed. Rio de Janeiro: Lumen Juris, 2003. 230 p.

⁵ CORRÊA, Gustavo Testa. Aspectos jurídicos da internet. São Paulo: Saraiva, 2000. 135 p

adjudicada a esse Estado. Assim, os interesses públicos de uma nação estariam efetivamente protegidos.⁶ Quanto ao segundo princípio, Bitencourt (2009, P.176) nomeia-o como o princípio da universalidade ou cosmopolita. Esse princípio deriva-se da cooperação internacional, permitindo que todos os países signatários de determinados tratados e convenções internacionais julguem os transgressores independentes do local do crime e da nacionalidade do infrator. Até o momento, os crimes que estão albergados para aplicação do princípio da universalidade são os que causam maior ojeriza a todos os seres humanos: a pirataria, o genocídio, os crimes de guerra e os crimes contra a humanidade.

Em que pese haver instrumentos jurídicos internacionais para penalizar os crimes transnacionais, a aplicabilidade das penas nos planos nacionais tem sido praticamente anulada. Essa dificuldade é oriunda da falta de harmonização do direito penal internacional nos países envolvidos no conflito.⁷

O pós-modernismo do ordenamento jurídico relacionados ao cibercrime encontra-se desafiado por várias questões como por exemplo: abuso e violações às liberdades de expressão, a natureza oculta de várias espécies de violações virtuais, bancos de dados inconfiáveis, natureza transnacional das infrações (vítimas e infratores em lugares adversos), carência de uniformização das leis nacionais referentes a condutas delituosas nos sistemas de informática.⁸

Diante da realidade imposta no espaço digital, verifica-se que a aplicação dos conceitos tradicionais de jurisdição, competência, já é inadequada para efetividade da justiça. A tutela desse mais novo ambiente de relações sociais há de ser derivada de cooperações internacionais que produzam documentos (tratados e convenções) de caráter universal. Caso contrário, o trabalho do judiciário, da polícia será inócuo.

2.1 CASOS CONCRETOS DE CRIMES VIRTUAIS ENVOLVENDO CONFLITOS DE JURISDIÇÃO E COMPETÊNCIA NA ORDEM INTERNACIONAL

É cediço que a popularização da internet não serviu apenas para universalizar ações positivas em prol das liberdades individuais e cidadania, mas também para causar inúmeros

⁶ SHAW, Malcolm. International Law, cit., p.667

⁷PAIVA, Bruno Teixeira de. Ampliação da competência do Tribunal Penal Internacional para o julgamento de crimes ambientais transfronteiriços. 2008. 112p. Dissertação. (Mestrado em Ciências Jurídicas) - Universidade Federal da Paraíba, João Pessoa, 2008. p. 63.

⁸ NETO, Arnaldo Sobrinho de Moraes – Cibercrime e Cooperação Penal internacional.: Um enfoque à luz da Convenção de Budapeste. 2009, p. 99. Dissertação. (Área de concentração em Direito Econômico) Universidade Federal da Paraíba

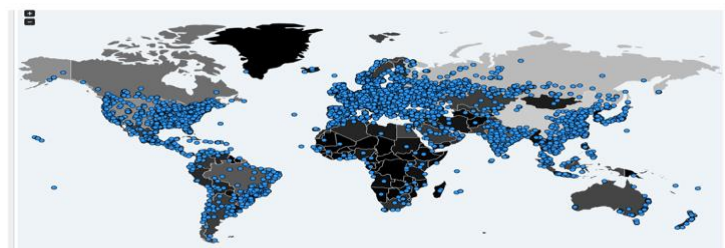
prejuízos á sociedade. Conforme leciona Cstells (2007, p. 205), As atividades criminosas possuem caráter transnacional e estabelecem conexão e alianças que cooperam entre si para a perpetuação de suas infrações. Alguns crimes virtuais foram de bastante notoriedade nos últimos anos. A seguir abordaremos alguns exemplos.

2.1.1- Os ataques virtuais nominados WannaCry e Petya

O mundo está conectado. Entretanto, essa interatividade não contribuiu apenas para benefícios. A gestão das organizações, os negócios, as relações sociais, todos têm se tornado dependentes da conexão pela internet. Essa inter-relação também tem sido alvo de grandes vulnerabilidades. É salutar lembrar o ataque cibernético ocorrido em 12 de maio de 2017. O acontecimento estremeceu todo o planeta: a infecção do ransomware WannaCry que instantaneamente se espalhou por mais de 200 países, com mais de 200.000 casos registrados.⁹

Segundo a Cartilha de Segurança, define-se ransomware da seguinte forma: “Ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.” A seguir, o mapa referenciando a dimensão do ataque cibernético por todos os continentes.

Figura 1- Países invadidos pelo WannaCry



Fonte: TUPINAMBÁ, 2017

Uma falha detectada no sistema operacional Microsoft Windows permitiu a agressão do malware, o qual provocou um cenário de terror pelo mundo. O malware infectava o equipamento e rapidamente se propagava pela rede. O início da invasão ocorreu na Espanha. Pouco tempo depois já havia sequestrado informações de vários órgãos públicos, empresas,

⁹ ROCHA, Márcio Antônio da. Cibersecurity: o foco da proteção é só tecnológico? Fonte, Ed. 18, dezembro 2017

hospitais no mundo inteiro, inclusive no Brasil. Naquela data, vários órgãos públicos no Brasil desligaram seus computadores, suspenderam atendimento ao público, excluíram seus sites da rede mundial de computadores. Dentre eles podemos citar: Petrobrás, Instituto Nacional do Seguro Social (INSS) em todo o Brasil, Tribunais da Justiça de São Paulo, Sergipe, Roraima, Amapá, Mato Grosso do Sul, Minas Gerais, Rio Grande do Norte, Piauí, Bahia e Santa Catarina, Ministério Público de São Paulo, Itamaraty, Instituto Brasileiro de Geografia e Estatística (IBGE).¹⁰

Ao se resgatarem as informações dos computadores alvos, o(s) infrator(es) exigiam das vítimas um resgate de US\$ 300 em bitcoin (moeda virtual) que deveria ser repassado a um endereço/conta dos cibercriminosos.

Posteriormente, na data de 27 de junho do mesmo ano, outro ransomware nominado como PETYA realizou ataque idêntico no mundo inteiro. Em ambos os ataques foram exigidas as mesmas moedas. Entretanto, mesmo que as vítimas se dispusessem a pagar, não teriam a garantia do retorno de suas informações virtuais.

Ações delituosas como as explicitadas anteriormente, podem ocorrer de modo anônimo e silencioso, sendo bastante complexa a identificação de suas autorias. Nesses casos, frise-se, com vítimas globais, com prejuízos ímpares, não foi identificada a autoria. A gravidade e a forma de atuação desses crimes preocupam toda a comunidade internacional. Nesse sentido registra Rocha (2017):

As fontes de ameaças em potencial e as motivações para tais atos são muitas, e o rastreamento preciso dos autores de ataques cibernéticos normalmente não é uma tarefa simples. Em cenários mais críticos, os ataques podem até mesmo colocar vidas humanas em risco (desativação de plantas de energia e ataques em outras infraestruturas críticas). De fato, existe uma preocupação cada vez maior com o uso do espaço cibernético para ações terroristas.

O espaço cibernético vem sendo um lugar apropriado para execução de quaisquer atos ignóbeis. De fato, o mundo deve temer ações terroristas diferentes das tradicionais: explosão de bombas, explosão de aviões, envenenamento de pessoas etc. A possibilidade dos furtos de informações de bancos de dados públicos ou privados, pode gerar as mais diversas

¹⁰ G1. Ciberataques em larga escala atingem empresas no mundo e afetam Brasil – Maio.2017. Disponível em: < <https://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml> >. Acesso em 14/03/2019

consequências negativas. Desse modo, é urgente que Leis e Acordos/Tratados Internacionais relativos à segurança da informação sejam regulados.

Por derradeiro, ressalte-se que caso a autoria dessas ações tivesse sido identificada, estar-se-ia diante de um conflito de competência para aplicações das penalidades, uma vez que houve violações em vários países. Que nação iria realizar a execução das penas?

2.1.2- Caso dos processos apensos eDate Advertising GmbH v. X e Olivier Martinez e Robert Martinez v. MGN Limited

O caso em epígrafe é oriundo do Tribunal de Justiça da União Europeia. O conflito envolve dois países. A narração dos fatos ocorre da seguinte maneira: A Justiça Alemã condena X (com seu irmão) em 1993 a uma prisão perpétua, em razão de um homicídio de um autor famigerado. Em 2008 ocorreu uma liberdade condicional. Um portal na Internet «www.rainbow.at» com o endereço «Info-News» gerado pela eDate Advertising localizada na Áustria, dispôs até 18 de Junho de 2007, informação fazendo referência a 23 de Agosto de 1999. A notícia fazia menção ao indivíduo X e ao seu irmão. Afirmava que os réus teriam ingressado com recurso para o Tribunal Constitucional Federal em Karlsruhe (Alemanha). Abordava ainda uma sucinta descrição do fato criminoso e declarava que o advogado de defesa pretendia provar que as testemunhas haviam faltado com a verdade no período do julgamento.¹¹

O réu X intimou a eDate Advertising para que fizesse cessar as referidas publicações e se comprometesse com isso. Apesar de a empresa não responder a intimação, excluiu a notícia afrontosa em 18 de Junho de 2007. A eDate Advertising contesta a procedência da ação, alegando a competência dos órgãos jurisdicionais alemães.

No segundo caso, o ator francês Oliver Martinez juntamente com seu pai ingressa com ação no tribunal de grande instance de Paris. Suas alegações versaram sobre a violação ao seu direito de imagem quando divulgaram em um sítio na internet «www.sundaymirror.co.uk» a seguinte notícia data de 03 de fevereiro de 2008: “Kylie Minogue está de novo com Olivier Martinez”, narrando, inclusive detalhes do encontro. Com base no art. 9º do Código Civil

¹¹UNIÃO EUROPEIA. eDate Advertising GmbH v. X e Olivier Martinez e Robert Martinez v. MGN Limited, Acórdão do Tribunal de Justiça, Quarta Seção, ECLI:EU:C:2011:685, 3 de outubro de 2013. Disponível em: <goo.gl/AFMWtp>. Acesso em: 15.03.2019.

francês que assegura a todos o respeito a sua vida privada, postularam a ação em desfavor da MGN, editora do Jornal Britânico Sunday Mirror.

Tanto no primeiro caso quanto no segundo, a jurisdição das ações foi julgada incompetente, tendo sido encaminhados para o Tribunal de Justiça da União Europeia para definição de competência. Com fundamento no art. 5º do Regulamento do Conselho da União Europeia (CE) 44/2001, o Tribunal frisou que as decisões judiciais em matérias civis e comercial deveriam tramitar no local onde ocorra o fato danoso (devendo interpretar como sendo o lugar que se materializou e o local do dano). Aquele tribunal ressaltou que diferentemente das notícias divulgadas por meio da imprensa física, aquilo que é publicado pela internet ganha relevo de universalidade, transnacionalidade. Dessa forma, os critérios de conexão devem ser adaptados, podendo a vítima escolher o foro pelo centro de seus interesses (local de trabalho, local de sua residência).

Compreendeu-se então, que nos casos de violações aos direitos de personalidade por meio da rede mundial de computadores, o lugar em que se materializa o dano seria o local em que melhor pudesse ser apreciado pelo órgão jurisdicional. Decidiu ainda que em todos os Estados nos quais a vítima pudesse acessar o conteúdo agressivo a sua imagem poderia acionar o judiciário.¹²

Verifica-se que o Tribunal de Justiça da União Europeia em ambos os casos relatados, decidiu por relativizar o conceito de tradição de competência. O lugar de competência para julgamento das ações foi o de melhor interesse para a vítima.

2.1.3. A IMPORTÂNCIA DA CONVENÇÃO DE BUDAPESTE PARA OS PAÍSES SIGNATÁRIOS

Em 23 de Novembro de 2001, a Convenção de Budapeste estava com seu texto produzido em definitivo para assinatura dos países interessados. Esse foi o primeiro documento internacional público sobre o cibercrime. Os autores responsáveis por sua elaboração foram peritos do Conselho da Europa, bem como outros países como Estados Unidos da América, Canadá, Japão e África do Sul. A pretensão da propositura dessa

¹² UNIÃO EUROPEIA. eDate Advertising GmbH v. X e Olivier Martinez e Robert Martinez v. MGN Limited. Acesso em: 15.03.2019.

legislação é que venha ser ratificada e aderida pela generalidade dos países.¹³

O objetivo principal da Convenção é criar uma legislação penal e processual penal comum entre os países membros. Essa unicidade de leis propiciaria um combate real aos crimes perpetrados na rede mundial de computadores. Veja o que preconiza o preâmbulo da Convenção de Budapeste:

Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objectivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adopção de legislação adequada e da melhoria da cooperação internacional;

Conforme preconiza a transcrição do fragmento acima, se os países dispusessem de uma legislação comum, facilitaria a cooperação internacional a fim de realizar as investigações e execuções criminais. A teor, seu texto delimitou o direito penal material com os crimes relativos à confidencialidade, integridade, disponibilidade dos sistemas de computadores, bem como crime referidos aos conteúdos e crimes cometidos por meio da informática. O protocolo adicional à Convenção aprovado pela Resolução da Assembleia da República n.º 91/2009 disciplinou também os crimes de natureza racista e xenófobo praticados através do sistema de informática.

Importante ressaltar, conforme observou Boiteux (2004, p.170), que nesse documento a definição de espaço cibernético foi dada como sendo o lugar comum visitado por aqueles que se conectam por intermédio das tecnologias da informação. Uma preocupação importante dos peritos que elaboraram esse texto, além de criar novas tipificações penais, de definir regras processuais, foi conciliá-las com o direito penal internacional. Acrescente-se ainda que todos os crimes tipificados são dolosos, não havendo como idealizá-lo na forma culposa, já que não há como ter as referidas condutas delineadas sem que seja de modo intencional.

A convenção de Budapeste em seu art. 22 resolve uma controvérsia importante: A questão da competência e da jurisdição para apuração dos fatos delituosos no mundo virtual. Estabelece ali que os países signatários deverão adotar os critérios mais convenientes à aplicação dos procedimentos legais.

É importante mencionar que apesar do carácter de transnacionalidade da Convenção, visto que são signatários países de todos os continentes, há o cuidado de resguardar as

¹³ BRAVO, Rogério; ROCHA, Manuel Lopes; VEIGA, Paula (Org). **Leis do cibercrime vol. I**. Portugal: Rolo & Filhos 1ª edição. Julho de 2003

legislações nacionais dos países envolvidos. Nesse sentido cabe destacar o que dispõe o art. 15 do documento em referência:

Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos previstos na presente Secção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do Pacto Internacional das Nações Unidas sobre os Direitos Civis e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade.

O artigo retromencionado demonstra que a Convenção de Budapeste reafirma as soberanias dos países signatários. Com isso, revela uma garantia para que as nações não sintam temor de aderi-la. Também o estímulo à cooperação jurídica é de salutar importância para o combate dos ataques virtuais.

Destaque-se que atualmente são 72 (setenta e dois países) que ratificaram a Convenção, dentre os quais estão nações que não são da União Europeia: Panamá, Paraguai, Peru, Filipinas, Senegal, África do Sul, Tunísia e Estados Unidos, Cabo Verde, Canadá, Chile, Colômbia, Austrália, Costa Rica, República Dominicana, Gana, Israel, Japão, Ilhas Maurício, Nigéria, Sri Lanka, Tonga, México, Marrocos, Argentina.

Como se ver, O Brasil não a aderiu até o momento. Isso não parece conveniente diante de todo cenário de cibercrimes a que todos os países estão expostos. Ademais, sabendo que as condutas delituosas praticadas no universo virtual estarão sempre em conflito com a competência/jurisdição, pois as leis nacionais só terão aplicabilidade também em um território delimitado e nacional, seria prudente que o Brasil também recepcionasse e ratificasse a Convenção.

A convenção em estudo é o único documento de caráter global. Entretanto, sofre algumas críticas por tratar de forma idêntica todos os países que a ratificaram no tocante à consideração dos avanços tecnológicos.

Pois bem, a grande quantidade de países que ratificou a Convenção demonstra êxito dessa legislação. Diante da complexidade das ações criminosas no ambiente virtual internacional, insistir na aplicação de conceitos tradicionais implica denegar efetivamente o acesso à justiça. Ao se imaginar por exemplo que o domicílio de um réu (praticante de crime informático) seja critério fixo e absoluto de competência para que alguém seja julgado e

condenado, certamente várias vítimas ficariam sem a garantia de seus direitos. Pois, em se tratando de cibercrimes, às vezes o autor está há milhões de quilômetros de suas vítimas.¹⁴

O novel da elaboração da Convenção de Budapeste é extremamente relevante para aplicação da justiça diante dos crimes cibernéticos ocorridos constantemente nesse novo ambiente paralelo ao mundo físico. A regulamentação de leis penais e processuais trará resultados positivos para comunidade internacional.

A falta de adesão de alguns países à Convenção pode favorecer surgimento de Paraísos Jurisdicionais (mercados de sentenças). Investidores econômicos do mercado online podem ser estimulados a oferecer seus negócios e serviços somente onde as legislações sejam falhas. A exemplo, as empresas que exploram os jogos de azar pela internet têm se utilizado desse artifício. Alguns países/ regiões como a cidade de Gibraltar, a Ilha de Man (territórios do Reino Unido) têm favorecido empresas que realocam seus bens e serviços para aquela região. Isso é realizado com o enfraquecimento das legislações domésticas. A dificuldade para a execução de decisões de outras nações também é outro motivo que contribui para o surgimento desses mercados de sentença.¹⁵

A finalidade da Convenção de Budapeste nos remete a coadunar com a obra de Joanna Kulesza (International Internet Law) na qual defende a criação de um Direito Internacional da Internet por meio de tratados e Convenções. A autora sugere que da mesma maneira que foi possível a criação de um Direito Ambiental Internacional com ramo do Direito Internacional Público, deve-se buscar convencionar aquele.

O acesso à rede mundial de computadores permitiu que se avolumem cotidianamente questões envolvendo violações dos direitos humanos, de propriedade intelectual e também do comércio eletrônico. A questão é que na perspectiva virtual os problemas transmutam as fronteiras, carecendo de um direito que também alcance essas fronteiras.

Para Kulesza (2012), a ideia de um Direito Internacional da Internet não pode se desvencilhar dos princípios da diversidade cultural, da liberdade de acesso e da adoção de padrões abertos, os quais estão previstos na Declaração de Princípios de Genebra. Isso somente será viável caso haja uma conscientização mundial dos governantes, de modo que ocorra uma cooperação entre os Estados.

¹⁴ BASSO, Maristela e POLIDO, Fabrício Bertini Pasquot. "**Jurisdição e lei aplicável na Internet: Adjudicando litígios de violação de direitos da personalidade e as redes de relacionamento social**". In: LUCCA, Newton de e SIMÃO FILHO, Adalberto (eds.). Direito & Internet – Aspectos Jurídicos Relevantes, São Paulo: Quartier Latin, 2008, v.02, p. 442-490, p.443.

¹⁵ ESTADOS UNIDOS. Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997). Disponível em: <<https://goo.gl/LpT5T2>>. Acesso em:18/03/2019

3. CONCLUSÃO

Nosso cenário internacional de globalização das relações sociais, econômicas exige que se regulamente de forma mundial o uso da internet. Caso não se materialize essa positivação internacional, vamos testemunhar flagrantes desrespeitos às liberdades individuais, aos direitos humanos, à privacidade, bem como uma intensa insegurança jurídica. As infrações nos cibercrimes com conflitos internacionais ficarão sem resolução. Certamente seus autores serão motivados a provocarem os danos que desejarem por terem a certeza da impunidade. Pode-se observar que as atitudes delituosas dos cibercriminosos estão prejudicando as pessoas com a mesma intensidade com que se evoluíram todas as tecnologias telemáticas. Isso é alarmante. Os juristas necessitam encontrar alternativas que acompanhem tais transformações e que possam tutelar o direito das pessoas.

Essa realidade mostra que legislações isoladas, como por exemplo a Lei Carolina Dieckman e a Lei do marco Civil da Internet adotada no Brasil, são frágeis para resolução de crimes com caráter universal. O Brasil foi literalmente prejudicado com os ataques cibernéticos nominados como WannaCry e Petya, entretanto essas legislações domésticas não puderam ser invocadas por terem caráter apenas nacional.

É urgente que se implementem programas/legislações a fim de garantir a segurança da informática, bem como que se combata os crimes cometidos no ambiente virtual. Instituições públicas e privadas estão sujeitas aos mais vis ataques. Esse contexto de insegurança no mundo virtual poderá trazer prejuízos de todas as ordens para a comunidade internacional. O mais preocupante ainda é saber da dificuldade para identificação e autoria dos criminosos cibernéticos, os quais vêm ficando impunes algumas vezes.

Os Estados necessitam compreender que jurisdição e competência devem ser relativizados em prol de se proteger o mundo. A homogeneização de leis materiais e processuais que regulem o ciberespaço deve ser perseguida por todos os povos.

É salutar afirmar que a Convenção de Budapeste propõe uma possibilidade importante de resolução de litígios decorrentes do espaço virtual. A harmonização das legislações entre países parece ser o direcionamento mais adequado para gerar equidade e justiça. A importância desse tratado é de natureza relevante e ímpar. Se ele não é a solução para o fim de todos os conflitos cibernéticos, poder-se-ia considerar como uma sinalização mais adequada que já foi idealizada para cuidar dos problemas surgidos nas fronteiras online.

REFERÊNCIAS

- ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo, SP: Juarez de Oliveira, 2006. 241 p
- ANTAS Jr., Ricardo Mendes. **Território e regulação: espaço geográfico, fonte material e não-formal do direito**. São Paulo: Associação Editorial Humanistas – Fapesp, 2005. Acesso em 09/ 03 /2019 Disponível em: <<http://ricardoantasjr.org/wp-content/uploads/2012/03/livro.pdf>>. Acesso em: 09/03/2019. livro.pdf
- 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.
- BRAVO, Rogério; ROCHA, Manuel Lopes; VEIGA , Paula (Org). **Leis do cibercrime vol. I** . Portugal: Rolo & Filhos 1ª edição. Julho de 2003
- Cartilha de Segurança – Ransomware, <https://cartilha.cert.br/ra> <https://cryptoid.com.br/banco-de-noticias/fim-da-linha-para-o-wannacry-nao-alerta-o-jovem-ingles-que-cessou-o-ataque-mundial/>> acesso em 14.03.2019nsomware/
- 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.
- CASTRO, Carla Rodrigues Araújo de. **Crimes de informática e seus aspectos processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003. 230 p.
- CONSELHO DA EUROPA. Convenção sobre o cibercrime. Budapeste: Conselho da Europa, 2001.
- CONVENÇÃO de Budapeste para Crimes Cibernéticos. 23 de novembro de 2001. Disponível em: <<http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> >Acesso em: 19/02/2019.
- CORREIA, Gustavo Testa. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2000. 135 p
- ESTADOS UNIDOS. Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997). Disponível em: <<https://goo.gl/LpT5T2>>. Acesso em:18/03/2019
- G1. **Ciberataques em larga escala atingem empresas no mundo e afetam Brasil** – Maio.2017. Disponível em: < <https://g1.globo.com/tecnologia/noticia/hospitais-publicos-na>

inglaterra-sao-alvo-cyber-ataques -em - larga - escala.ghml >. Acesso em 14/03/2019.

GIBSON, W. **Neuromancer**. Trad. de Alex Antunes (baseada na tradução da 1ª ed. de Maya Sangawa e Silvio Alexandre). 3. ed. São Paulo: Aleph, 2003

HONORATO, Eduardo. **Cibersegurança: qual o risco mundial**. Fonte, Ed. 18, dezembro 2017, pag. 72

KULESKA, Joanna. **International Internet law**, 1ª ed. New York: Routledge, 2012

LÉVY, Pierre, **Qu'est-ce que le virtuel?**. Paris, Éditions La Découverte, coll. Sciences et Société, 1995, p.157

NETO, Arnaldo Sobrinho de Moraes – **Cibercrime e Cooperação Penal internacional.: Um enfoque à luz da Convenção de Budapeste**. 2009, p. 99. Dissertação. (Área de concentração em Direito Econômico) Universidade Federal da Paraíba

PAIVA, Bruno Teixeira de. **Ampliação da competência do Tribunal Penal Internacional para o julgamento de crimes ambientais transfronteiriços**. 2008. 112p. Dissertação. (Mestrado em Ciências Jurídicas) - Universidade Federal da Paraíba, João Pessoa, 2008. p. 63.

PINHEIRO, Patrícia P. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2013.

REZEC, Francisco. **Direito Internacional Público** – Curso Elementar -13ª edição revista, aumentada e atualizada 2011 – SARAIVA

REVISTA FONTE – **tecnologia da informação na Gestão Pública**. ANO 14, Nº18 DEZEMBRO 2017 (Reproduzido do White Paper “Defesa cibernética com os controles críticos de segurança do CISTM (Center for Internet Security)”, item 2, Módulo Security Solutions, junho de 2017, versão 1.2)

ROCHA, Márcio Antônio da. **Cibersecurity: o foco da proteção é só tecnológico?** Fonte, Ed. 18, dezembro 2017.

<https://www.prodemge.gov.br/images/com_arismartbook/download/22/revista_18.pdf >
Acesso em: 14/03/2019

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

SHAW, Malcolm. **International Law**, cit., p.667

TUPINAMBÁ, Regina. **Fim da linha para o WannaCry? Não! Alerta o jovem inglês que cessou o ataque mundial. cryptoid.com.br** 13.05.2017. Disponível em: >13/05/2017<https://cryptoid.com.br/banco-de-noticias/fim-da-linha-para-o-wannacry-nao-alerta-o-jovem-ingles-que-cessou-o-ataque-mundial/>> acesso em 14.03.2019

UNIÃO EUROPEIA. **eDate Advertising GmbH v. X e Olivier Martinez e Robert Martinez v. MGN Limited**, Acórdão do Tribunal de Justiça, Quarta Seção, ECLI:EU:C:2011:685, 3 de outubro de 2013. Disponível em: <goo.gl/AFMWtp>. Acesso em: 15.03.2019.