Revista da Faculdade de DIREITO da Universidade Federal de Uberlândia

Os aspectos gerais dos tratados internacionais e a Convenção de Budapeste sobre Crimes Cibernéticos

General aspects of international treaties and the Budapest Convention on Cybercrime

Clayton Vinicius Pegoraro de Araujo[1]

Resumo: O objetivo deste artigo é verificar aspectos gerais dos tratados internacionais e os níveis similares de desenvolvimento para aplicação das disposições relativas ao crime cibernético na União Europeia. Utilizando como metodologia a análise documental dos textos legais de domínio público, bem como textos doutrinários que embasam as considerações finais neste trabalho. Durante a análise da Convenção sobre crimes cibernéticos do Conselho da Europa, que foi aberta para assinatura em Budapeste, em novembro de 2001, observou-se que a adesão de membros continua crescendo, bem como a qualidade da cooperação para enfrentar novos desafios no campo da informática, das relações em redes e duro combate ao crime.
Palavras-chave: Cooperação regional. Cibernético.Crimes. Convenção. Acordo.

Abstract: The objective of this paper is to verify general aspects of the international treaties and the similar levels of development for the application of the provisions regarding cybercrime in the European Union. Using as methodology the documentary analysis of legal texts from the public domain, as well as doctrinal texts that support the final considerations in this study. During the analysis of the Council of Europe Convention on Cybercrime, which was opened for signature in Budapest in November 2001, it was observed that the membership continues to grow, as well as the quality of cooperation to face new challenges in the field of information technology, network relations and hard crime fighting.
Keywords: Regionalcooperation. Cybercrime. Convention. Agreement.

1. Introdução

Os acordos de cooperação regional envolvem, via de regra, membros com semelhante desenvolvimento, cultura e tradição jurídica e situados em um bloco econômico, como é o caso do Mercado Comum do Sul (MERCOSUL)

[1] Advogado, Pós-Doutor em Economia Política, Doutor em Direito das Relações Econômicas Internacionais, Mestre em Direito (área de concentração em Direito Internacional), Especialista em Direito Público. Professor do Programa de Mestrado Profissional em Economia e Mercados e Graduação da Universidade Presbiteriana Mackenzie, professor titular na Universidade Municipal de São Caetano do Sul - USCS. Professor convidado na FIA/USP para cursos de MBA.

DOI: https://doi.org/10.14393/RFADIR-50.1.2022.65259.145-165

e do *North American Free Trade Agreement* (NAFTA) e da União Europeia. Por conta desta proximidade geográfica entre os países-membros de um bloco regional, trona-se mais fácil promover a cooperação e o desenvolvimento de um sistema único por meio da harmonização e convergência de políticas de combate ao crime cibernético.

Em análise sore os aspectos da defesa da concorrência, por analogia, tema os lição de (OLIVEIRA, 2002, p. 308), na qual traz reflexão sobre a importância da harmonização dos preceitos:

> [...] o desenvolvimento no âmbito dos blocos regionais envolve, em um primeiro momento, a harmonização das legislações nacionais de defesa da concorrência. Um passo seguinte importante é a transformação da defesa comercial (com ações *antidumping*, por exemplo), articulando-a com a defesa da concorrência. Em um estágio mais avançado, em que já se consolidou um mercado comum, como aquele obtido pela União Europeia, é possível conceber um órgão supranacional, como a DE-IV, da Comissão Europeia.

Neste sentido, a União Europeia é considerada o bloco comercial mais evoluído na atualidade, possuindo uma eficiente forma de defesa dos sistemas internos, por intermédio do Conselho Europeu de modo supranacional e responsável pela política de defesa contra crimes cibernéticos no âmbito da Comunidade. A título de exemplo e comparação, no Mercosul ainda não temos um avançado estágio de integração alcançado pela União Europeia, entretanto, podemos citar o Conselho do Mercado Comum, reconhecendo a cooperação entre os Estados-Partes da localidade.

A questão da formação dos protocolos intrabloco e sua importância no sistema internacional está definida nos ensinamentos de (GUIMARÃES, 2009, p. 47) como sendo a termologia utilizada de modo indistinto, seja para tratados bilaterais, mas também para tratados multilaterais importantes e traz como exemplo o Protocolo de Kyoto, na esfera multilateral em matéria ambiental. Explica, ainda, que alguns se valem do vocábulo para indicar o termo final de uma reunião ou conferência internacional.

É importante frisar que, ainda resta um logo caminho para a efetiva proteção dos dados e um esquema maior de repressão do crime cibernético, já se trata de uma excelente iniciativa dos membros, com as perspectivas de, no futuro, incrementar as políticas de defesa cibernética, além de instituir um órgão supranacional com vistas a dirimir questões relativas a atos que possam vir a prejudicar o trefego das informações em rede digital.

Em uma análise sobre os pressupostos interpretativos dos tratados e convenções internacionais e seu alcance, esclarece (FERRAZ JÚNIOR, 2011, p. 239):

> Os tratados são fontes cujo centro irradiador é o acordo entre as vontades soberanas dos Estados. As convenções são celebradas no âmbito dos organismos internacionais que, reconhecidos, veem seus atos normativos repercutirem no âmbito interno dos Estados. Este é o caso, por exemplo, da OIT, Organização Internacional do Trabalho, cujas convenções aprovadas são submetidas às autoridades competentes dos Estados participantes (por exemplo, devem ser ratificadas pelo Congresso), passando a ter força legal.

A experiência obtida nos acordos de cooperação tem sido benéfica, tanto no sentido de evitar conflitos de jurisdições na aplicação extraterritorial de leis, quanto para servir de exemplo em um eventual acordo de cooperação multilateral, neste sentido afirma (NUSDEO, 2002, p. 170):

> [...] os principais deveres assumidos pelas partes referem-se à informação recíproca a respeito de atividades potencialmente anticompetitivas realizadas em seu território de que tenham conhecimento e sejam do interesse da contraparte; à informação sobre investigações ou medidas tomadas que possam afetar os interesses da outra parte, podendo requisitar documentos, inquirir testemunhas, realizar buscas, etc. Costuma-se estabelecer também as cláusulas de cortesia, através das quais as partes se comprometem a levar em consideração os interesses da contratante no desempenho de suas funções.

Outro exemplo para contextualizar a situação de cooperação profícua foi a celebração entre o governo dos Estados Unidos e a Comissão Europeia em 1991, cuja principal proposta era a coordenação e diminuição da possibilidade de impacto resultante das diferenças entre as partes na

aplicação de suas leis sobre concorrência e outras medidas. Havia previsão para que cada uma das partes notificasse a outra quando for aplicar sua legislação e afetação dos interesses da outra, bem como reuniões periódicas entre ambas as autoridades com o fim de promover maior convergência legal.

2. Os Aspectos Jurídicos dos Tratados Internacionais

Nas lições de (FRANCO FILHO, 1999, p. 127), ao organizar o tema sobre a Convenção sobre os Direitos dos Tratados, ocorrida em Viena, no ano de 1969, destaca que:

> 1. Um tratado entra em vigor na forma e na data previstas no tratado ou acordadas pelas partes; 2. Na ausência de tal disposição ou acordo, um tratado entra em vigor tão logo o consentimento em obrigar-se por um tratado seja manifestado por todos os Estados negociadores [...]

A Convenção de Viena sobre Direito dos Tratados, em seu artigo 2°, alínea *"a",* define tratado: "Tratado' significa um acordo internacional celebrado por escrito entre Estados e regido pelo direito internacional, quer conste de um instrumento único, quer de dois ou mais instrumentos conexos, qualquer que seja sua denominação particular".

Entretanto, embora haja uma definição da expressão 'tratado' nessa Convenção, na verdade, a denominação dos tratados internacionais é irrelevante para que sejam determinados tanto os seus efeitos, isto é, sendo válida uma norma a mesma gera uma série de consequências; quanto a sua eficácia, ou seja, se a norma válida está verdadeiramente gerando consequências, surtindo efeitos. É irrelevante, porque se pode verificar, pela prática, que não há atribuição de nenhuma consequência (Soares, 2002, p. 59). Assim, tratados, por definição histórica de (SOARES, 2002, p. 58) ao observar a solenidade dos atos internacionais, destaca como sendo:

> [...] atos solenes entre os Estados, tão antigos quanto as relações amistosas ou litigiosas entre grupos políticos autônomos. A notícia

> de sua prática entre os povos pode ser datada dos primeiros registros escritos ou gravados em monumentos de pedra, os quais procuravam tornar claros, e em especial, com vista em sua perpetuação no tempo, tal como os valores religiosos fundamentais das grandes civilizações, os direitos e deveres entre aquelas unidades políticas autônomas. [...]

Como já mencionado no corpo deste trabalho, em nosso sistema podemos utilizar várias nomenclaturas para definir o tratado, como, por exemplo: acordos, convenções, ajustes, ligas, entre outros que são utilizados como sinônimos de atos bilaterais ou multilaterais internacionais, às vezes sem qualquer critério.

Nesse sentido, entende (PIOVESAN, 1997, p. 73/74) que "os tratados internacionais, enquanto acordos internacionais juridicamente obrigatórios e vinculantes (*pacta sunt servanda*) constituem a principal fonte de obrigação do Direito Internacional". E segue explicando que 'tratado' é um termo genérico, usado para incluir tantas outras denominações semelhantes, tais como: convenções, pactos, protocolos, cartas e demais acordos internacionais.

Na verdade, os adeptos dessa corrente defendem a existência de uma diversidade das fontes de produção das normas jurídicas, como também a existência de um limite de validade dessas normas, ou seja, a norma internacional só teria validade e geraria efeitos internacionalmente, mas não teria validade no interior dos Estados, a não ser que este, aceitando-a, promovesse sua internalização (por meio de um procedimento próprio, estabelecido por lei interna).

Eventualmente, na questão do dano econômico, o Estado vitimado de alguma forma em seu território, seu patrimônio, seus serviços ou mesmo sobre a pessoa ou bens de particulares a ele subordinado, tem legitimidade para invocar a responsabilidade internacional do Estado faltoso. Neste sentido, em matéria de complexidade, pode ser observada a lição de (MELLO, 2004, p. 1684-1685):

> No século XIX, tendo em vista as consequências da revolução industrial, os Estados começam a estabelecer restrições às importações. A dificuldade para se estabelecer uma regulamentação internacional no setor econômico é explicada, citando a jurisprudência norte-americana [...] no sentido de que as possibilidades são tão grandes que se trona impossível fazer uma regulamentação geral. [...]

É fato que as soluções de controvérsias que envolvem os Estados devem ser resolvidas pelo modo pacífico. Neste sentido é a fala de (TRINDADE, 2002, p. 788):

> [...] tendências atuais na solução pacífica das controvérsias internacionais mas também de áreas emergentes do direito internacional contemporâneo (tais como as das organizações internacionais, proteção dos direitos humanos, direito do meio ambiente) assim como de novas transformações ou desenvolvimentos em algumas de suas áreas mais tradicionais (tais como território, jurisdição, tratados, responsabilidade dos Estados) revela um sensível declínio da concepção voluntarista do direito internacional, segundo a qual este último dependeria inteiramente da vontade dos Estados.

3. Os Tratados Internacionais e seus Limites de Aplicação

Sem dúvida, temos uma inovação para os chamados *positive comity* e *negative comity principles*, traduzidos como princípios de cortesia positiva e de cortesia negativa. Pela cortesia negativa, uma das partes leva em consideração os interesses da outra, antes de aplicar sua legislação contra atos praticados em seus próprios limites territoriais, podendo, inclusive, não iniciar uma investigação, que deixaria a cargo do parceiro no acordo. Neste sentido, inclusive, é a própria redação da Convenção de Budapeste:

> Artigo 26.º – Informação espontânea 1. Qualquer Parte pode, nos limites previstos no seu Direito interno e não e sem pedido prévio, transmitir a uma outra Parte informações obtidas no âmbito das suas próprias investigações, sempre que considerar que a transmissão dessas informações pode ajudar a Parte destinatária a iniciar ou a efetuar investigações ou procedimentos relativos a infracções penais previstas na presente Convenção, ou sempre que considerar que ela pode dar origem a um pedido de cooperação formulado por essa Parte nos termos do presente Capítulo.

Por outro lado, o *positive comity principle*, ou princípio de cortesia positiva, consiste em atos positivos de cooperação e assistência recíproca entre autoridades nacionais localizadas em diferentes países, ao contrário da *negative comity,* que implica, simplesmente, a decisão de não iniciar uma investigação. Mediante a cortesia positiva, uma das partes, sentindo-se prejudicada por práticas que ocorram no território da outra, pode notificá-la para que tome as medidas cabíveis em cada caso. Neste sentido também pode ser observado o texto da Convenção de Budapeste:

> Artigo 27.º - Procedimentos relativos aos pedidos de auxílio mútuo na falta de acordos internacionais aplicáveis 1. Na falta de um tratado de auxílio mútuo ou de um acordo assente em legislação uniforme ou recíproca em vigor entre a Parte requerente e a Parte requerida, aplica-se o disposto nos números 2 a 9 do presente artigo. Existindo esse tratado, acordo ou legislação, só se aplica o disposto no presente artigo se, em vez deles, as Partes envolvidas decidirem aplicar o presente artigo, no todo ou em parte.

É importante frisar que as disposições do acordo, principalmente no que concerne aos princípios de cortesia, não têm caráter vinculativo para as partes, ou seja, trata-se de mecanismos de aplicação voluntária com o intuito de dirimir os conflitos e tensões causados por aplicações unilaterais de leis antitruste nacionais.Além disso, cabe distinguir, como complemento, a diferenciação entre os conceitos de integração regional e regionalismo, com apoio nos estudos de (CREUZ, 2010, p. 61):

> Com isso, vale pontuar breve distinção entre o conceito de integração regional e regionalismo. O regionalismo pode ser visto como um programa ou como uma política de Estado, enquanto a integração regional consubstancia-se efetivamente em um processo do qual Estados lançam mão de suas autonomias absolutas para a formação de um bloco econômico regional. Logo, o regionalismo integra o campo das políticas públicas, que pode envolver a instituição de um projeto [...]

Do ponto de vista histórico das relações internacionais, não se trata de algo novo, pois como exemplo, os Estados Unidos e a União Europeia já estabeleceram acordos de cooperação, ampliando os termos do acordo de 1991, em momento após a dissolução da União Soviética e, principalmente,

tornando mais abrangente o conceito de cortesia positiva. A versão aprimorada do princípio da cortesia positiva estabelece que qualquer das partes tem o dever de abrir uma investigação contra atos praticados em seu território, sempre que isso for solicitado pela outra parte. Não obstante, uma parte deve atender ao pedido da outra, mesmo que não haja qualquer violação de sua legislação antitruste interna.

Os Estados Unidos também firmaram acordos de cooperação com a Alemanha, Austrália, Canadá e Brasil. Nota-se que há grande interesse, por parte dos estadunidenses, em ampliar a cooperação com seus parceiros comerciais, que começou a se manifestar principalmente a partir de 1994, quando o Congresso americano aprovou uma lei que permite a troca de informações confidenciais com outros países; trata-se da *International Enforcement Assistance Act* (IAEAA), que confere poderes às agências para celebrarem acordos de cooperação não apenas no âmbito das trocas de informações sigilosas, mas também no que concerne às modalidades de assistência técnica (NUSDEO, 2002, p. 171).

Cabe ressaltar que há diferenças em relação aos acordos celebrados pelos Estados Unidos com seus diversos parceiros, pois isso ocorre em virtude da similaridade entre os níveis de desenvolvimento dos sistemas jurídicos desses países, diferentes, por sua vez, dos sistemas de países emergentes, que muitas vezes nem possuem legislação apropriada ao tema do crime cibernético, como é o caso deste estudo. O acordo celebrado entre os Estados Unidos e o Brasil, em 1999, difere do acordo celebrado entre os Estados Unidos e a União Europeia em 1998, por exemplo, principalmente no que se refere ao conceito de cortesia positiva, mais extenso no acordo com a União Europeia. Nesse diapasão, serve como esclarecimento o escólio de (FINKELSTEIN, 2003,p. 39) sobre a formação de blocos econômicos e seu contexto mundial:

> Não existe um órgão internacional ou uma agência encarregada de fiscalizar ou autorizar a criação e o funcionamento dos mercados de bloco ou acordos de integração regional. Estes são negociados

> diretamente pelos Estados interessados versando desagravar parte ou a totalidade da pauta comercial existente ou, em outros casos, ampliar a integração ora alcançada, evoluindo a forma adotada àquela posterior, que implica em maior integração.

Dessa forma, aumenta-se a expectativa da comunidade internacional para que se tornem viáveis acordos de cooperação multilaterais com vistas a um maior desenvolvimento dos sistemas de defesa para o crime cibernético em diferentes países, promovendo convergência de procedimentos e harmonização de leis progressivamente.

Neste sentido, é a percepção de (CELLI JÚNIOR, 1999, p. 61), ao expressar suas considerações a respeito das funções da regulação jurídica no âmbito internacional "[...] até certo ponto paradoxal regulamentação jurídica, das tensões, inconsistências e contradições entre os diversos sistemas de proteção à livre concorrência [...] As regras de concorrência podem ainda ser utilizadas como instrumento de outras políticas".

Assim, nos envolve o tema da recepção dos tratados, que deve ser compreendida, mesmo no âmbito da União Europeia, sob dois prismas: Direito Internacional Público e direto interno, conforme ensina (DALLARI ,2003, p. 7):

> O tema da recepção – e eventual integração – do direito, à luz dos propósitos desta obra, compreende duas dimensões distintas: a da recepção do Direito Internacional Público no direito interno e, mas particularmente, a da recepção dos tratados internacionais pelo sistema de normas de direito positivo do Estado. Quanto á dimensão mais geral, que serve de pano de fundo para aquela que, mas específica [...]

Portanto, as relações entre o Direito Internacional e o Direito Interno geram inúmeros problemas não só doutrinários, mas também práticos a respeito de se saber qual o tipo de relação que eles mantêm entre si. O ponto principal dessa questão consiste em saber qual das normas deverá prevalecer em havendo conflito entre a norma internacional e a norma interna. A problemática envolvendo as teorias monista e dualista reside no ponto da incorporação dos tratados internacionais ao direito interno, uma

vez que os monistas defendem a existência de um só ordenamento com prevalência (ou não) de uma norma sobre a outra, enquanto os dualistas defendem a existência de dois ordenamentos distintos e normas de sobreposição.

4. Os Crimes Cibernéticos e a Comunidade Global

Com o crescimento da conectividade global, a vida social e política mudou imensamente. O papel amplamente citado que a internet desempenhou durante a primavera árabe na promoção da liberdade de discurso afirma que as redes de computadores estão na linha de frente da defesa da liberdade, fundamental direitos e Estado de direito. No entanto, a liberdade on-line, assim como off-line, também exige segurança. De fato, a internet pode igualmente ser usada como um instrumento eficiente para vigiar e atacar adversários ou cometer danos e crimes de qualquer forma possível. O grau em que o ciberespaço trouxe liberdade aos usuários, da mesma forma, deram origem a ameaças à segurança que podem ser usadas contra o mesmo cidadão. Neste sentido é a lição de (NUNZI, 2012, p. 4):

> As ameaças à segurança em nossas sociedades estão crescendo em escala e sofisticação e o desafio que representam é cada vez mais transfronteiriço e intersetorial. O crime cibernético, que ocupa um lugar de destaque entre as preocupações dos cidadãos e dos governos, corresponde perfeitamente a este perfil, uma vez que se baseia e visa as infraestruturas da Internet e seus usuários. Cidadãos, empresas, governos e infraestruturas críticas precisam de proteção contra os criminosos que exploram as tecnologias modernas.[2]

Entre os pontos do direito à liberdade e a garantia de segurança, a segurança cibernética é desafiada a garantir, de algum modo, a democracia, o Estado de Direito e dos direitos fundamentais aos cidadãos e, ao mesmo

[2] *Security threats to our societies are growing in scale and sophistication and the challenge they pose is increasingly cross-border and cross-sectoral. Cybercrime, which ranks high among the concerns of citizens and governments, perfectly matches this profile as it relies upon and targets internet infrastructures and their users. Citizens, businesses, governments and critical infrastructures need protection from criminals who exploit modern technologies.*

tempo, controlar o abuso da liberdade que pode, em tese, prejudicar vidas alheias. Consequentemente, a segurança cibernética e o crime cibernético estão ganhando crescente atenção no discurso público. No entanto, noções divergentes dos conceitos são que está colocando desafios quando se trata de abordar a questão de forma sistêmica.

Para obter certeza sobre os conceitos trazidos na Convenção de Budapeste partimos da premissa que o crime cibernético é definido, como os ataques cibernéticos que são conduzidos com potenciais ameaças para os serviços essenciais da União Europeia. Portanto, além disso está a noção de segurança cibernética, ou seja, a infraestrutura para defender computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados de ataques maliciosos.

Assim, o conceito de segurança cibernética e Infraestrutura crítica possuem várias definições e são usadas dentro de discussão acadêmica sobre o tema. Enquanto alguns estudiosos se referem à defesa cibernética e resiliência como componentes de uma estratégia global de segurança cibernética, outros usam o termo o que já indica discordância na abordagem do tema. Em geral, segurança cibernética concentra-se na proteção de computadores, redes e dados de forma não intencional ou acesso não autorizado, mudança ou destruição. Desta forma, de modo técnico, cabe a definição de (ROSSINI *et al*., 2015, p. 10)[3]

> Na verdade, um grande exemplo é o próprio termo segurança cibernética, que a União Europeia define como "salvaguardas e ações que podem ser usadas para proteger o domínio cibernético", tanto no campo civil como militar, das ameaças que estão associadas a ou que possam prejudicar suas redes interdependentes e infraestrutura de informação. A UIT define segurança cibernética como "a coleta de ferramentas, políticas, segurança conceitos, salvaguardas de segurança, diretrizes,

[3] *In fact, a great example is the term cybersecurity itself, which the European Union defines as "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure". The ITU defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets"*

> abordagens de gerenciamento de risco, ações, treinamento, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético e os ativos da organização e do usuário".

Portanto, o alcance, a severidade e a natureza transnacional da Comissão Europeia, induzem a aplicação da lei e organizações de segurança internacional, juntamente com governos e o setor privado para definir e abordar a questão da segurança de dados. Desta feita, busca-se garantir a segurança cibernética como uma prioridade máxima na política da União Europeia, de onde existe uma noção de trincheira como uma primeira linha de defesa contra o crime cibernético.

Além disso, a Comissão estabelece princípios que devem realmente orientar a política de alcançar segurança cibernética como a proteção dos direitos fundamentais, a liberdade de expressão, dados pessoais e privacidade, acesso para todos, governança democrática e eficiente de múltiplas partes interessadas e uma responsabilidade compartilhada para garantir, claramente, na direção da sustentação de um direito que deve protegido por meio de uma abordagem de segurança comum a todos.

A prevenção de crimes cibernéticos é parte integrante de uma segurança cibernética transnacional e de informações críticas estratégia de proteção. Isto inclui a adoção de uma legislação apropriada tanto no âmbito nacional como a nível internacional. Neste contexto, deve ser avaliado como determinante a relação entre crimes cibernéticos e relacionados, pois crimes cibernéticos têm um significado mais restrito em comparação com os crimes relacionados aos computadores de modo geral. Para elucidar esta questão interpretativa e conceitual, cabe o escolio de (FIGUEIREDO, 2014, p.90), com apoio no Direito Penal, de onde extrai:

> Logo, o Direito Penal desempenha um importante papel não somente de repressão, mas também de prevenção geral negativa ao criminalizar determinadas condutas que ameacem ou quebrem os princípios básicos do ciberespaço que são a confidencialidade, integridade e disponibilidade. Neste aspecto, a Convenção do Cibercrime possibilitou uma repressão e prevenção uniforme aos perigos causados pelo uso indevido do sistema de informática entre

> os Estados europeus e também serve de inspiração aos demais países para legislarem acerca do tema, contribuindo desta forma para delimitar os parâmetros de um conceito operativo de cibercriminalidade de âmbito global.

Com isso, as legislações definem o crime responsabilidades por qualquer ação possível. O potencial ilimitado das tecnologias de computação aponta ao fato de que a situação atual é um começo deste problema que hoje se torna perigoso e ameaçador. No mais, quando as tecnologias estão se desenvolvendo tão rapidamente e há tantos cientistas e progresso técnico, a criminalidade informática, está se transformando em um dos crimes mais perigosos entre todos. Os crimes informáticos causam ameaças particulares ao campo das finanças, escolas, serviços, governos etc. Grupos criminosos roubam milhões de Reais por meio do uso ilegal de novas metodologias ilegais, sem falar no crime cibernético em nível internacional, que tem claramente uma dificultosa prevenção dada a velocidade de cometimento e possibilidade de escapatória dos delinquentes.

Como já dito anteriormente, o crime cibernético consiste em atos criminosos cometidos on-line através do uso de redes de comunicação eletrônica e sistemas de informação. A União Europeia implementou leis e apoia a cooperação operacional através de ações não-legislativas e financiamento de estruturas de combate. A colaboração entre países é essencial para o bom funcionalmente do sistema repressivo. Neste sentido comenta (DELGADO, 2007. p.57/58):

> [...] atendendo à diversidade dos sistemas jurídicos dos Estados envolvidos nos procedimentos de cooperação, pode-se admitir sob a rubrica de cooperação judicial penal internacional aqueles atos de colaboração praticados não só entre juízes, mas também entre as autoridades do Ministério Público158, razão pela qual – admite o autor – apesar de se utilizar do termo cooperação judicial penal internacional, considera que, sob este ponto de vista, seria tecnicamente mais adequado fazer uso da expressão, mais compreensiva, "cooperação jurisdicional penal internacional.

Portanto, o crime cibernético ou cibercrime é uma questão sem fronteiras que pode ser de vários maneiras classificado, que vão desde ataques contra sistemas de informação ou *phishing* (por exemplo, falsos

sites bancários para solicitar senhas que permitam o acesso às contas bancárias das vítimas), fraude e falsificação on-line, com instrumentos para o roubo de identidade, *phishing*, spam e código malicioso para conteúdo ilegal, incluindo material sobre abuso sexual infantil, incitação ao ódio racial, incitação a atos terroristas e glorificação da violência, terrorismo, racismo e xenofobia.

É sabido que, muitos destes tipos de crimes, têm se movimentado on-line ou são facilitados on-line. Como consequência, a maioria das investigações criminais tem um componente digital muito importante e uma necessidade especialização dos investigadores.

5. A Convenção de Budapeste e o Crime cibernético

A Convenção sobre crimes cibernéticos, discutida e aprovada no âmbito do Conselho da Europa foi aberta para assinatura em Budapeste, em novembro de 2001. Quinze anos depois, ela continua sendo o acordo internacional de suma relevância que versa sobre crimes cibernéticos e provas eletrônicas. A adesão continua crescendo, enquanto tanto a qualidade da implementação quanto o nível de cooperação entre as Partes continuam melhorando, e o próprio tratado está evoluindo para enfrentar novos desafios. Parte disso é a complementação por meio de um mecanismo de acompanhamento eficaz e por programas de capacitação, que são alimentados pelo comitê responsável, fato que, sobremaneira, vem contribuindo para a evolução da Convenção. Inclusive, no dia 15/12/21, o Senado brasileiro aprovou a adesão do Brasil à Convenção de Budapeste (APROVADA..., 2021), o que se trata de um grande avanço em nosso sistema de proteção e combate aos crimes cibernéticos.

Oficialmente conhecida como a Convenção do Conselho da Europa sobre Cibercriminalidade, a Convenção de Budapeste - aberta para assinaturas em 2001 e que entrou em vigor em 2004 - foi o primeiro tratado

internacional a focar explicitamente o crime cibernético. Desde a redação deste artigo, 64 países ratificaram a Convenção de Budapeste - incluindo os Estados Unidos, que ratificaram o tratado em 2006. Vários outros países também estão em processo de aderir ao tratado.

Os objetivos do tratado são três: I- harmonizar as leis nacionais relacionadas aos crimes cibernéticos; II- apoiar a investigação desses crimes; e III- aumentar a cooperação internacional na luta contra os crimes cibernéticos. Entre outras coisas, o tratado obriga os países participantes a adotar legislação que proíba os crimes cibernéticos especificados. Ele também exige que os países participantes adotem certas regras de coleta de provas, tais como mecanismos para apoiar a preservação rápida de dados armazenados, além de servir como um limite ao Tratado de Assistência Jurídica Mútua (M-LAT) quando os países envolvidos em um pedido não possuem tais tratativas.

Conforme discutido, o tratado foi escrito antes do surgimento da computação em nuvem, quando a grande maioria das provas digitais (e outras) críticas para as investigações criminais foi mantida dentro das próprias fronteiras territoriais. Assim, pressupunha-se a jurisdição sobre a localização dos dados - operando sob a suposição de que os interesses nacionais relevantes e a localização dos dados subjacentes eram concomitantes. Este não é mais o caso. Com uma mudança na interpretação da regra, a partir 2018, concluiu-se que mais da metade de todas as investigações envolve um pedido transfronteiriço de acesso a provas eletrônicas.

A desconexão entre a jurisdição territorial dos Estados e as formas pelas quais os dados se movimentam e são mantidos além das fronteiras nacionais representa desafios significativos para a aplicação da lei. Mesmo em situações nas quais os países têm relações amigáveis, as múltiplas etapas necessárias para acessar os dados muitas vezes levam a longos atrasos. E em outras situações, a aplicação da lei pode nem mesmo ter a

certeza de localização dos dados ou sede da entidade com posse e controle dos dados e, portanto, nenhuma ideia de jurisdição para decisão do pedido. Ao analisar esta questão, nota-se a complexidade da extraterritorialidade e a internet nas palavras de (CIDRÃO *et. al*., 2018, p.69/70):

> 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.

Em reconhecimento a esses desafios postos, o Comitê da Convenção sobre Crime Cibernético criou um grupo de trabalho para considerar as questões em 2012, que se transformou no Grupo de Evidência da Nuvem e, por fim, recomendou a adoção de uma atualização do tratado na forma de um Segundo Protocolo Adicional. As negociações começaram em setembro de 2017, que resultaram na elaboração de cinco textos provisórios destinados a abordar alguns dos desafios. Além disso, a União Europeia está atenta aos perigos reais inseridos no ciberespaço, conforme preleciona (CAMPOS, 2018, p.2):

> Devido não só ao perigo da ameaça transnacional, que é nos tempos correntes mais real do que nunca, mas também devido a evolução tecnológica que trouxe consigo novos desafios para estes atores, as Organizações Internacionais que agora se exploram começaram então a contar com o ciberespaço, espaço onde a delimitação espacial desta dissertação se cingirá, no ambiente securitário prioritário dos seus documentos estratégicos. A UE viria a aumentar o foco na segurança cibernética equipando-se e ajudando os Estados-membros a protegerem-se contra as ameaças cibernéticas, mantendo simultaneamente um ciberespaço aberto, livre e seguro.

O cibercrime existe há mais de 40 anos e o Conselho da Europa vinha lidando com este tema do ponto de vista do direito penal desde meados dos anos 80. Em 2001, a questão tornou-se suficientemente importante para

justificar um tratado internacional vinculativo. Então foi negociado pelos Estados membros do Conselho da Europa juntamente com o Canadá, Japão, África do Sul e Estados Unidos da América, a Convenção sobre Crimes Cibernéticos, ocorrida na cidade de Budapeste, Hungria, em novembro de 2001.

Desde então, as Tecnologias da Informação e Comunicação (TIC's) transformaram as sociedades em todo o mundo. Elas também as tornaram altamente vulneráveis aos riscos de segurança, com o advento dos crimes cibernéticos. Tudo isso aliado aos desenvolvimentos de células criminosas atuantes de forma organizada que, nas palavras de Carrapiço (2005, p. 181) colaboram entre si dentro do ciberespaço para:

> O desenvolvimento em áreas como as comunicações, os transportes e o ciberespaço aumentaram de forma exponencial o campo em que estes grupos podem operar: "the spread of e-business and the possibility of creating so-called virtual identities facilitates and obscures criminal activities and actors by providing anonymity". Outra consequência relevante é a constituição de parcerias e a cooperação entre grupos de crime organizado de diferentes regiões do globo.

Embora haja o reconhecimento da necessidade de fortalecer a segurança, a confiança nas TIC's e de reforçar o Estado de Direito e a proteção dos direitos humanos no ciberespaço, todas as coisas "cibernéticas" se tornaram agora muito importantes. medida que eles tocam os direitos fundamentais dos indivíduos, bem como os interesses nacionais (de segurança) dos Estados, é cada vez mais difícil chegar a um consenso internacional sobre soluções comuns.

Para superar este dilema, a abordagem mais sensata é focar em padrões comuns que já estão em vigor e funcionando, como a Convenção de Budapeste sobre aspectos do crime cibernético, e em abordagens nas quais há um amplo consenso, em particular, o desenvolvimento de capacidades.

Além disso, a repressão dos crimes cibernéticos continua desafiando os governos e a própria legislação constituída no tocante à aplicação devido à inerente interconectividade global das pessoas e das coisas. Os cibercrimes

desafiam os tudo que se tem como convencional até hoje em matéria de soberania estatal, pois podem originar-se de quase qualquer computador do mundo e passar por múltiplas fronteiras nacionais em questão de segundos. No mais, também são problemáticos os níveis nacionais de legislação que, eventualmente, facilite a atuação de criminosos.

6. Considerações Finais

Do ponto de vista legislativo, duas alternativas existem para o tratamento dos atos ou comportamentos antijurídicos, quais sejam, a ilegalidade intrínseca e a ilegalidade condicionada. A ilegalidade intrínseca é a aproximação adotada pelos Estados Unidos da América e pela Alemanha, na qual se supõe a proibição geral de certos comportamentos sem necessidade de avaliar o impacto, considerando com isso que só sua existência deveria ser demonstrada para ativar os procedimentos dedicados para impor as sanções correspondentes então.

Por outro lado, a ilegalidade condicionada é considerada para que os atos ou comportamentos constituam práticas restritivas que possam ser prejudiciais ao interesse geral ou outros objetivos que são estabelecidos pela legislação. Desse modo, a autoridade competente deveria enfrentar um caso de avaliação para estabelecer a existência de ato lesivo ao interesse individual.

É importante frisar que as interpretações estão conferindo habilidades discricionárias aos órgãos de aplicação (em medida menor quando eles são comportamentos definidos de proibição absoluta), mas com a diferença que em um caso a discricionariedadeé usada para determinar se um ato ou comportamento ilegal é autorizado (ilegalidade intrínseca), enquanto no outro esse império é exercitado para determinar se ele é proibido (ilegalidade condicional).

Assim, no denominado ciberespaço, por estar em constante evolução, assim como as políticas preventivas e reativas relacionadas, uma grande quantidade de perguntas não respondidas permanece para os futuros pesquisadores abordarem, tais como o envolvimento dos direitos fundamentais e as disposições relacionadas com a análise de segurança dos dados no ciberespaço. Esta avaliação pode, inclusive, versar sobre o direito à proteção de dados pessoais, liberdade de expressão, liberdade de informação contidos na Carta dos Direitos Fundamentais Digitais da União Europeia.

Tomando como base a Convenção de Budapeste e as novas pesquisas sobre o possível envolvimento das normas de proteção de dados e aspectos da segurança cibernética a União Europeia ainda terá muito espaço para encontrar soluções de governança para os novos emergentes desafios técnicos e de segurança neste novel campo do conhecimento.

A política de segurança cibernética inclui algumas das principais prioridades, entre as quais se destacam necessário para cumprir os objetivos estabelecidos no documento internacional firmado. Assim, umas das prioridades centrais da política estão definindo a principal estratégia em termos da provisão de segurança cibernética, bem como o fornecimento de uma visão geral dos princípios que podem possivelmente criar a infraestrutura e as estratégias para que se venha a ter uma proteção segura dos sistemas e redes de informação (públicas e privadas).

Portanto, a ausência de harmonização internacional pode criar abrigos para criminosos, semelhantes aos criados em paraísos fiscais pelo mundo afora. Urge, desta feita, impor limites legais dentro de um regime de direito internacional no ciberespaço para que se evitem dilemas jurisdicionais, pois os Estados não podem tratar do assunto individualmente e necessitam buscar, de modo contínuo, a cooperação transnacional ou global para combater eficazmente o crime cibernético.

Referências

APROVADA adesão do Brasil à Convenção sobre crime cibernético.**Senado Notícias**, 15 dez. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico. Acesso em: 27 mar. 2022.

CAMPOS, Hélio Samuel Farinha. **A Luta Contra o Cibercrime**: Os Casos da União Europeia e da NATO. Dissertação (mestrado em Relações Internacionais). Universidade do Minho - Escola de Economia e Gestão, 110p., 2018.

CARRAPIÇO, Helena. O Crime Organizado e as Novas Tecnologias: uma Faca de Dois Gumes.**Revista Nação e Defesa**,n. 111, 3ª série, p. 175-192, 2005.

CELLI JUNIOR, Umberto. **Regras de Concorrência no Direito Internacional Moderno**. Porto Alegre: Livraria do Advogado, 1999.

CIDRÃO, Taís Vasconcelos; MUNIZ, Antônio Walber; ALVES, Ana Abigail Costa Vasconcelos. A oportuna e necessária aplicação do Direito Internacional nos ciberespaços: da convenção de Budapeste à legislação brasileira.**Brazilian Journal of International Relations**, Marília, v. 7, n. 1, p. 66-82, jan./abr. 2018.

COUNCIL OF EUROPE. **Convention on Cybercrime**. Budapest, 23 nov. 2001. Disponível em: https://rm.coe.int/1680081561. Acesso em: 10 mar. 2022.

CREUZ, Luís Rodolfo Cruz e. **A construção da defesa da concorrência no Mercosul**: uma perspectiva construtiva – cooperação e interesses nas relações internacionais. Dissertação (Mestrado Programa San Tiago Dantas de Pós-Graduação em Relações Internacionais). Universidade Estadual de Campinas, 215p., 2010.

DALLARI, Pedro B. A. **Constituição e tratados internacionais**. São Paulo: Saraiva, 2003.

DELGADO, Vladimir Chaves. **Cooperação internacional em matéria penal na Convenção sobre o Cibercrime**. Dissertação (mestrado em Direito das Relações Internacionais). Centro Universitário de Brasília, 315p., 2007.

FERRAZ JÚNIOR, Tércio Sampaio. **Introdução ao estudo do Direito**: técnica, decisão, dominação. São Paulo: Atlas, 2011.

FIGUEIREDO, Herivelton Rezende de. Cibercrime.**Revista Jurídica UNIGRAN**, Dourados, MS, v. 16, n. 32,jul./dez. 2014.

FINKELSTEIN, Cláudio. **O processo de formação de mercado em blocos**. São Paulo: Thomson, 2003.

FRANCO FILHO, Georgenor de Sousa (Org.). **Tratados internacionais**. São Paulo: Ltr, 1999.

GUIMARÃES, Antônio Márcio da Cunha. **Contratos internacionais de seguros**. São Paulo: Revista dos Tribunais, 2002.

GUIMARÃES, Antônio Márcio da Cunha. **Tratados internacionais**. São Paulo: Aduaneiras, 2009.

MELLO, Celso D. de Albuquerque. **Curso de Direito Internacional Público**. v. II. Rio de Janeiro: Renovar, 2004.

NUNZI, Alfredo. Cybercrime: A new challenge for the European Union.**Revue Internationale de Droit Penal**, v. 83, 2012. Disponível em: https://www.cairn.info/revue-internationale-de-droit-penal-2012-1-page-289.htm. Acesso em: 17 mar. 2022.

NUSDEO, Ana Maria de Oliveira. **Defesa da concorrência e globalização econômica**: o controle dos atos de concentração no Brasil. São Paulo: Malheiros, 2002.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. São Paulo: Max Limonad, 1997.

REZEK, José Francisco. **Direito internacional público**: curso elementar. São Paulo: Saraiva, 2018.

ROSSINI, Carolina; GREEN, Natalie. **Cybersecurity and Human Rights**.GCCS - Webinar Series Training Summaries, 2015. Disponível em: https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf. Acesso: 17 mar. 2022.

SOARES, Guido Fernando Silva. **Curso de Direito Internacional Público**. v. I. São Paulo: Atlas, 2002.

TRINDADE, Antônio Augusto Cançado. **O direito internacional em um mundo em transformação** (Ensaios, 1976-2001). Rio de Janeiro: Renovar, 2002.

Artigo recebido em: 30/03/2022.
Aceito para publicação em: 09/11/2022.