Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito / Relações Internacionais

IARA VENÂNCIO FERREIRA

CRIMES INFORMÁTICOS: Legislação Penal Brasileira e a Cooperação Jurídica Internacional em Matéria Penal.

TAGUATINGA
2020

IARA VENÂNCIO FERREIRA

CRIMES INFORMÁTICOS: Legislação Penal Brasileira e a Cooperação Jurídica Internacional em Matéria Penal.

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Me. Victor Minervino Quintiere

TAGUATINGA
2020

IARA VENÂNCIO FERREIRA

CRIMES INFORMÁTICOS: Legislação Penal Brasileira e a Cooperação Jurídica Internacional em Matéria Penal.

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Me. Victor Minervino Quintiere

TAGUATINGA, DIA MÊS 2020

BANCA AVALIADORA

_____

Professor(a) Orientador(a)

_____

Professor(a) Avaliador(a)

Título do artigo: CRIMES INFORMÁTICOS: Legislação Penal Brasileira e a Cooperação Jurídica Internacional em Matéria Penal.

Autor: Iara Venâncio Ferreira

Resumo: O presente artigo tem como objetivo analisar a legislação penal brasileira no tocante aos crimes informáticos à luz da Convenção de Budapeste. E também identificar a relevância jurídica da Convenção de Budapeste. Além disso, foi necessário verificar o interesse do Brasil em aderir ao referido tratado, bem como as possibilidades de adesão do Brasil. A partir disto, foi possível observar as implicações jurídicas no âmbito da legislação brasileira. O presente estudo se mostrou necessário dado a grande quantidade de delitos dessa modalidade ocorridos na sociedade atual. O método utilizado foi o método dedutivo, pois a pesquisa iniciará analisando o geral sobre os crimes cibernéticos e terminará relacionando a cooperação jurídica e a Convenção de Budapeste. A metodologia utilizada foi a revisão bibliográfica, pois a forma mais eficaz encontrada para alcançar as respostas foi a análise de leis e doutrinas jurídicas.

Palavras-chave: Direito Penal. Crimes Informáticos. Convenção de Budapeste.

Sumário:

INTRODUÇÃO

O advento da globalização, por meio do avanço da tecnologia permitiu o surgimento da sociedade do conhecimento, considerada por muitos doutrinadores como a sociedade da informação. É preciso atentar-se que a sociedade não é estática, mas sim uma estrutura em constante mudança, sendo a tecnologia um dos fatores que influenciam a mudança de uma sociedade, inclusive chegando a ditar comportamentos e criar costumes. (JESUS; MILAGRE, 2016)

Não há dúvidas que os meios digitais integram a sociedade atual, e que cada vez mais os indivíduos buscam utilizar desse conforto para realizar suas atividades do cotidiano, entretanto, o grande problema é o uso dessa tecnologia para má finalidade.

Ademais, seria utopia imaginar que esse ambiente digital, somente seria utilizado para trazer benefícios a sociedade. O espaço da internet permite que as pessoas possam estar conectadas em qualquer lugar do mundo, oferecendo serviços e produtos que ultrapassam o limite das fronteiras. (GUIDI; REZEK, 2018)

Para Damásio de Jesus e José Antônio Milagre (2016. p.14), “ A Internet é rica, e onde há riqueza, existe crime. ”

Por isso, tema abordado nesse artigo é de extrema relevância, tendo em vista o grande avanço da tecnologia na sociedade brasileira, segundo o IBGE, o Brasil tem aproximadamente 126 milhões de pessoas conectadas à internet, segundo pesquisa realizada no ano de 2017. Dada essa informação, é notório que cada vez mais as pessoas utilizam da tecnologia em seu dia-dia. (IBGE,2018)

Além disso, segundo dados da Fortinet, em 2020, o Brasil sofreu mais de 1,6 bilhão de tentativas de ataques cibernéticos apenas nos 3 primeiros meses do ano. (Rolfini, 2020)

No Brasil, a primeira notícia que se obteve sobre crimes informáticos, foi no ano de 1999. Ainda nesse mesmo ano, um caso que ganhou notoriedade no país foi o do empresário e ex-controlador de uma rede de varejos, que foi acusado de ter enviado, de Londres, e-mail’s contendo informações falsas para o mercado financeiro

informando sobre o risco de quebra de um banco. Em decorrência disso, criou-se o debate sobre os problemas que envolviam a investigação de crimes informático, eis que eles poderiam ser praticados em qualquer lugar do mundo. (JESUS; MILAGRE, 2016. p.21).

Logo, o surgimento dessa nova pratica criminosa faz com que o direito penal tenha uma expansão no tocante aos seus bens jurídicos tutelados, sendo bem explicado pela dogmática do direito penal.

A partir do reconhecimento da existência de condutas lesivas aos bens jurídicos protegidos pelo direito penal, cabe ao direito, por meio de seus operadores, definir o que é um crime informático e como eles são cometidos, afim de buscar a solução mais inteligente para garantir o convívio social pacífico no ciberespaço.

Após essa definição jurídica, abre-se a possibilidade de analisar a legislação brasileira em relação a estes delitos, o Brasil possui a Lei nº 12.737/2012, conhecida popularmente com Lei Carolina Dieckmann e a Lei nº 12.965/2014 que dispõe sobre o Marco Civil da Internet.

Ocorre que devido falta de limites de jurisdição no ciberespaço é possível perceber os Estados devem recorrer a mecanismos de cooperação internacional, principalmente quanto a persecução penal, pois esta modalidade criminosa é complexa por dificultar a identificação de autoria e materialidade, uma vez que por meio do ciberespaço as pessoas conseguem ser anônimas e atingir locais a milhares de distância, por muitas vezes sem deixar nenhum rastro.

Acerca dos mecanismos de cooperação internacional relacionados aos crimes informáticos, tem se a Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrimes, que foi o primeiro Tratado Internacional a versar sobre a criminalidade virtual, entretanto, o Brasil ainda não é signatário desta Convenção.

Diante disso, faz se necessário analisar esse referido tratado, uma vez que a legislação nacional somente tem abrangência em seu território e como já foi citado os crimes cometidos na internet não possuem fronteiras. Dessa forma, somente

instrumentos de caráter internacional poderiam ter eficácia na luta contra esses delitos. (MAZONI, 2009)

Desta forma, a problemática tratada neste artigo versa sobre: em que medida o Brasil possibilitaria a adesão a Convenção de Budapeste em seu ordenamento jurídico?

1. ASPECTOS HISTÓRICOS

1.1 DOGMÁTICA PENAL CLÁSSICA AO DIREITO CONTEMPORÂNEO

O surgimento da sociedade de informação, faz com que a dogmática penal clássica deixe de ser capaz de alcançar fenômenos, cuja natureza, gravidade e repercussão na sociedade ultrapassam a esfera da proteção de bens jurídicos individuais, ou seja, surgem novas condutas que atingem toda a coletividade. (OLIVEIRA, 2012, p.360)

As práticas delituosas, segundo a dogmática penal clássica, eram tratadas como fatos individuais, como mera infração à lei e, por consequência, às cláusulas do “contrato social” (ALENCAR, 2019).

Para Jesus Maria Silva Sánchez (2002, p.93), “O paradigma do direito penal clássico é o homicídio de um autor individual. Não parece desarrazoado sustentar que a maior parte das garantias clássicas do Direito Penal adquire seu fundamento nessa constatação”.

Uma vez que o direito penal clássico está pautado na ideia da proteção do bem jurídico individual e nas garantias do cidadão contra medidas autoritárias.

O cenário vivido pela sociedade atual é caracterizado, basicamente, por um âmbito econômico variante e pelos avanços tecnológicos sem paralelo com toda a história da humanidade, dando ao direito contemporâneo um novo paradigma a ser tutelado pelo direito penal, qual seja: a coletividade. (SÁNCHEZ, 2002)

Segundo Silva Sánchez, é nesse aspecto que se observa a expansão do Direito Penal, pois a mudança do modelo de delito que serve de referência a construção dogmática: em lugar do homicídio do autor individual, trata-se, por exemplo, de abordar atos de corrupção realizados por uma empresa que, por sua vez, comete delitos econômicos. (SÁNCHEZ,2002. p 84).

Por isso, Sánchez propõem um modelo de Direito Penal de duas velocidades, primeiramente, sob uma perspectiva minimalista, propõe uma preservação dos esquemas clássicos da dogmática penal para a proteção dos bens jurídicos clássicos

e das garantias fundamentais dos acusados, uma vez que a primeira velocidade representaria o modelo de política criminal pautado na aplicação de penas restritivas de liberdade. Enquanto, a segunda velocidade representa a flexibilização dos princípios e regras do direito para aplicação de medidas com menor intensidade da sanção, tal como: penas restritivas de direitos e multas pecuniárias. (SILVA, 2019)

Isso faz com que as características expansionistas enxerguem mais os riscos e menos a lesividade das condutas. Dessa forma, quando defende a proteção dos bens jurídicos surgidos na complexidade social acredita-se na necessidade da criminalização de condutas, mesmo que o fundamento esteja nos riscos gerados e não nos danos efetivamente causados. (SILVA, 2019)

A sociedade da informação, ou pós-industrial, tem, sim, seus riscos, por isso também é conhecida como sociedade do risco, visto que é inegável que práticas de crimes com novas técnicas ainda desconhecidas pela sociedade provoquem incertezas na vida social. (SÁNCHEZ, 2002)

A criminalidade, associada aos meios informáticos e à internet (a chamada ciberdelinqüência), é, seguramente, o maior exemplo de tal evolução. (Sánchez,2002). Pois, é possível inferir que com o fenômeno da globalização e da popularização da internet, as fronteiras ilimitáveis do ciberespaço hospedaram, não apenas criações em favor da cidadania e da participação universal, como também colaboraram para que crimes, comumente praticados no “mundo real”, também fizessem parte do ciberespaço. (MUNIZ; CIDRÃO; ALVES, 2018)

A partir disto, é possível fazer a análise desse novo tipo de delito, tal como: seu conceito, sua classificação e sua legislação a luz de mecanismos de cooperação internacional.

2. CRIMES INFORMÁTICOS

2.1 CONCEITO

Em decorrência das inovações tecnológicas, é comum deparar-se com diversos termos relacionados aos crimes digitais, dentre os quais “ crimes de computador”, “crimes cibernéticos”, “fraude informática”, “cybercrimes”, “delinquência informática”, “delitos informáticos”, “crimes virtuais”. (CRESPO, 2011, p. 39)

Marcelo Crespo, ainda acredita que isso se dá por dois motivos: a) a evolução tecnológica que faz surgir novas técnicas e mecanismos para as práticas desses delitos. b) devido a presença de neologismos, vistos que os termos são marcados pela língua inglesa, e depois, inserido em nosso vocabulário. (CRESPO, 2011, p. 39)

No Brasil, escolheu-se nomear os crimes cometidos contra a informática de “delitos informáticos”, termo usual em países de língua espanhola que se relaciona à ideia de proteção do objeto jurídico informática e informação. (JESUS; MILAGRE, 2016. p. 50) .

Embora, no Brasil, jurista e doutrinadores ainda utilizam outras denominações distintas, mas, que, no fundo, acabam por significar basicamente a mesma coisa” (ROZA, 2007, p. 53 apud JESUS, 2016)

Segundo Mário Antônio Lobato de Paiva (apud, Spinieli,2018), os crimes informáticos são definidos como

> [...]conjunto de normas e instituições jurídicas que pretendem regular aquele uso dos sistemas de computador – como meio e como fim – que podem incidir nos bens jurídicos dos membros da sociedade; as relações derivadas da criação, uso, modificação, alteração e reprodução do software; o comércio eletrônico, e as relações humanas realizadas de maneira sui generis nas redes, em redes ou via internet (PAIVA, 2003)

Valdir Sznich (apud COSTA, 2001, on-line) define Crime de Informática “como qualquer ato ilegal onde o conhecimento especial de tecnologia de informática é essencial para a sua execução, investigação e acusação.

Para Emanuel Alberto Sperandio Garcia Gimenes

> “O crime virtual é qualquer ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão em que um computador conectado à rede mundial de computadores (Internet) seja o instrumento ou o objeto do delito”. (CITAÇÃO)

Nesse mesmo sentido, a OECD – Organização para Cooperação Econômica e Desenvolvimento define o Crime Informático como “ qualquer conduta ilegal, não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados” (NETO, Apud Reis, 2003).

A partir disso, pode-se inferir que, nos crimes informáticos, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal. (JESUS; MILAGRE, 2016, p.49)

2.2 CLASSIFICAÇÃO

Tulio Viana, dividiu os delitos informáticos em crimes informáticos próprios, impróprios, mistos e mediatos ou diretos. (VIANA; MACHADO, 2013)

Os crimes cibernéticos próprios, são aqueles em que o indivíduo utiliza o sistema informático como meio e fim almejado para pratica de delitos, como por exemplo: a invasão de um dispositivo causando modificação e destruição ao sistema software do dispositivo. (MAZONI, 2009)

Já em relação aos impróprios, também chamado de impuros, podem ser classificados como: utilização do sistema para prática de delitos já previstos em legislação vigente, ou seja, o sistema informático é utilizado como meio para cometimento do crime, podendo ser exemplificado como: postar mensagens nas redes sociais caluniando outro indivíduo. (MAZONI, 2009)

No tocante aos crimes informáticos mistos, Tulio Vianna, define que são aqueles em que há inviolabilidade da proteção de dados, embora a finalidade da norma seja proteger outro bem jurídico, como a invasão ao sistema informático eleitoral, afim de alterar os votos de uma urna. Neste caso, o bem jurídico tutelado

seria apenas o sistema eleitoral, uma vez que a invasão ao sistema informático seria um elementar do tipo penal. (VIANA; MACHADO, 2013)

Ademais, crimes informáticos próprios que são utilizados como crime meio de pratica delitiva são classificados como mediato ou indireto, como por exemplo: invadir dispositivo com o intuito de furtar dinheiro de conta bancária. Desta forma, ainda que o agente tenha cometido 2 crimes autônomos, o ele só será punido pelo furto, aplicando-se ao caso o princípio da consunção, uma vez que a invasão ao dispositivo foi apenas crime-meio. (VIANA; MACHADO, 2013)

A partir dessa da conceituação e classificação dos crimes informáticos, é possível analisar a legislação brasileira acerca dessa nova pratica delituosa.

3. LEGISLAÇÃO BRASILEIRA À LUZ DA CONVENÇÃO DE BUDAPESTE

3.1 LEGISLAÇÃO BRASILEIRA

No Brasil, o uso da internet com fulcro de gerar danos a terceiros tem gerado muitos conflitos internos, principalmente no tocante à dificuldade de se aplicar normas e controles judiciais efetivos. No Ordenamento jurídico brasileiro, 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. (Muniz; Cidrão; Alves, 2018)

A Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, tipificou no ordenamento jurídico brasileiro o delito de invasão de dispositivo ao inserir o artigo 154-A e 154-B no Código Penal Brasileiro, bem como alterou a redação dos artigos 266 e 298 também do Código Penal Brasileiro. (BRASIL, 2012)

A referida lei foi criada após a atriz Carolina Dieckmann ter seu computador pessoal invadido por *crackers* e ter sido chantageada pelos criminosos, que obtiveram e divulgaram fotos intimas da atriz. O caso ganhou grande repercussão por se tratar de uma figura pública e por não ter na época dos fatos nenhuma legislação especifica para a conduta dos criminosos. (G1, 2013)

O artigo 154-A do Código Penal traz em seu texto a criminalização da conduta de invasão a dispositivos com finalidade de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita ou ainda instalar vulnerabilidades para obter vantagem ilícita, tutelando assim o direito ao sigilo de dados presentes nos dispositivos informáticos. (BRASIL, 2012)

Além disso, o artigo 154-A, §1º do Código Penal, ainda criminaliza a conduta de quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador, com a finalidade de assegurar a prática da conduta de invasão dispositivos.

Há ainda previsão nos parágrafos seguintes deste artigo de causas de aumento de pena, quando a invasão de dispositivo resultar em prejuízo econômico ou

ainda quando houver divulgação, comercialização ou transmissão a terceiros, bem como nos casos em que o crime for praticado contra: Presidente da República, governadores e prefeitos; Presidente do Supremo Tribunal Federal; Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.” (BRASIL, 2012)

A referida lei também deixa claro no artigo 154-B do Código Penal Brasileiro que a ação penal para este delito somente se procede mediante representação, exceto quando o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (BRASIL, 2012)

A lei ainda acrescentou aos arts. 266 e 298 do Código Penal Brasileiro os seguintes parágrafos, respectivamente, “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, com aumento de pena se ocorrido em período de calamidade pública e a equiparação de cartão de crédito ou débito a documento particular, tipificando a falsificação de cartão. (BRASIL, 2012)

No entanto, a Lei 12.737 de 2012, foi duramente criticada pela doutrina especializada, que apontou a ausência de definição de diversos termos técnicos, normas abertas que permitem interpretações divergentes.

Neste seguimento, há uma grande divergência entre a referida lei com a lei de interceptações, Lei nº 9.296/1996, a saber, para a resolução da maioria dos casos de cibercrimes, necessário se faz a quebra de sigilo de dados telemáticos de um equipamento informático, entretanto, o art. 2º, inciso III da lei de interceptações veda a quebra do sigilo telemático em crimes puníveis com pena de detenção. (MUNIZ; CIDRÃO; ALVES, 2018)

Ocorre que os delitos previstos no art.154-A, §§1º e 2º e 266 §§ 1º e 2º da Lei 12.737/2012 são puníveis apenas com pena de detenção, não preenchendo assim os

requisitos da lei de interceptações, por consequência restringido o trabalho da polícia investigativa e facilitando a impunidade. (MUNIZ; CIDRÃO; ALVES, 2018)

Outra legislação importante é a Lei 12.965/2014, o Marco Civil da Internet, que apesar de não tratar de legislação penal desempenha função complementar no combate aos crimes informáticos. A principal finalidade desta lei é prevenir e evitar o mau uso da Internet no Brasil. Dessa forma, ela estabelece princípios, garantias e deveres dos usuários dessa ferramenta. (CUSNIR, 2018)

Ademais, a referida legislação garante o direito à inviolabilidade da intimidade e da vida privada do cidadão e ao sigilo de suas comunicações pela internet, bem como o não fornecimento a terceiros de dados pessoais, e também os registros de conexão e de acesso a aplicações de internet. (BRASIL, 2014)

O Marco Civil da Internet, ainda prevê em seu ordenamento jurídico brasileiro a soberania nacional, em termo de jurisdição, em relação aos dados coletados em território brasileiro, independe de local do planeta onde eles estejam armazenados, desde que o serviço atrelado a esses dados estejam sendo ofertado ao público brasileiro. (MPF, 2020)

Após observar a legislação pátria e as formas como esses delitos são cometidos, é possível perceber que soluções isoladas não têm eficácia no plano do ciberespaço, tornando-se necessárias medidas de atuação regionalizadas, cujo o objetivo é a harmonização legislativa e o respeito as diferenças jurídicas e tecnológicas entre os países. (MUNIZ; CIDRÃO; ALVES, 2018)

Portanto, nota-se a importância que a cooperação internacional detém quando objetiva-se tutelar de forma satisfatória as demandas oriundas dos cibercrimes. (MUNIZ; CIDRÃO; ALVES, 2018)

3.2 COOPERAÇÃO INTERNACIONAL

Uma das grandes discussões que envolvem a utilização da internet como meio para prática de delitos informáticos é a dificuldade em definir o tempo e o lugar de determinada conduta criminosa, visto que, na internet, inexistem fronteiras impeditivas que barrem criminosos de realizarem qualquer delito dentro do seu território. (MUNIZ; CIDRÃO; ALVES, 2018)

Isso faz com que as questões que rodeiam a internet sejam de alta complexidade, devido ao fato de estarem relacionadas a várias jurisdições distintas, atingindo diferentes países, o que dificulta o entendimento de qual o país seria realmente competente para processar, julgar e penalizar esses criminosos informáticos. Por isso, surge como alternativa para resolver esse conflito o direito internacional, por meio de tradados e cooperação jurídica. (MUNIZ; CIDRÃO; ALVES, 2018)

A cooperação jurídica internacional é um modo formal de solicitar a outro país alguma medida judicial, investigativa ou administrativa necessária para um caso concreto em andamento, sendo exercida pelos Estados com base em acordos bilaterais, tratados regionais e multilaterais e com base na promessa de reciprocidade. (MINISTÉRIO DA JUSTIÇA, 2020)

O Brasil possui uma ampla lista de acordos e tratados e também coopera mediante promessa de reciprocidade em casos análogos por parte do Estado estrangeiro. Por meio desses instrumentos internacionais, o Brasil não apenas adquire o direito de solicitar cooperação jurídica aos outros Estados Partes, como também se compromete a cumprir os pedidos que recebe desses países. (MINISTÉRIO DA JUSTIÇA, 2020)

No tocante a matéria penal, os pedidos de cooperação jurídica internacional – Carta Rogatória e Auxílio Direto – são recebidos de forma exclusiva de Autoridades Públicas – Juízes, membros dos Ministérios Públicos, Delegados de Polícia, Defensores Públicos – com a finalidade de cumprir atos de comunicação processual tais como: citações, intimações e notificações, além de atos de investigação ou instrução, como: oitivas, obtenção de documentos, quebra de sigilo bancário, quebra

de sigilo telemático, etc. Além de algumas medidas de constritivas de ativos, como bloqueio de bens ou valores no exterior. (MINISTÉRIO DA JUSTIÇA, 2020)

É nesse contexto que os tratados internacionais se mostram sendo um importante instrumento para o combate aos cibercrimes, visto que não resta dúvidas quanto ao alcance sem fronteiras dessa modalidade criminosa. Ademais, o tratado internacional relacionado aos crimes informáticos é a Convenção de Budapeste, ou também conhecida como Convenção sobre Cibercrime.

3.3 CONVENÇÃO DE BUDAPESTE

A Convenção de Budapeste de 2001, foi o primeiro tratado internacional que diz respeito aos crimes informáticos, dada a grande necessidade de criar mecanismos de uniformização para defender a sociedade desses delitos, ademais, a Convenção determinou que o espaço cibernético é determinado como uma espécie de espaço comum que é usufruído por todos aqueles que trafegam na internet ao se conectarem aos serviços de comunicação e informação. (MAZONI,2009)

A Convenção de Budapeste tem como objetivo harmonizar os elementos relativos ao Direito Penal fundamental dos países que aderiram, bem como também busca definir poderes e ações que ajudem a persecução penal, além de que pretende estabelecer um regime eficaz de cooperação internacional. (CRESPO, 2011)

Segundo o preambulo da própria Convenção de Budapeste, é de caráter prioritários intensificar a cooperação entres os Estados Partes da presente Convenção, pois com uma política criminal comum, juntamente com a legislação adequada e de uma eficiente cooperação internacional, estaria cumprindo seu objetivo principal de proteger a sociedade da criminalidade presente no ciberespaço. (CONVENÇÃO DE BUDAPESTE, 2001)

A necessidade de padronização dos procedimentos de cooperação é mais que um benefício de forma, eis que garante que a pretensão executória do Estado requerente não viole preceitos fundamentais do Estado requerido, uma vez que a

padronização exclui a possibilidade de atos investigatórios e de instrução processual serem considerados ilegais e abusivos. (GUIDO; REZEK, 2018, p. 284)

Ademais, é de fácil constatação que a legislação brasileira não está de acordo com a referida Convenção. Embora o Brasil ainda não seja signatário, no ano de 2019, o Comitê de Ministros do Conselho da Europa convidou o Brasil a aderir a Convenção de Budapeste, celebrada em 2001. Sendo o processo de adesão iniciado em julho de 2019, quando o Governo brasileiro manifestou sua intenção de aderir ao acordo internacional. (ITAMARATY, 2019)

A referida convenção conta hoje com mais de 62 Estados Partes, sendo a maioria da União Europeia e ainda conta com países como Estados Unidos, Chile e Argentina. Além disso, ainda tem a presença de 10 países observadores. (Brasil,2020)

Ao evidenciar que a legislação brasileira ainda encontra-se rasa em relação ao combate à criminalidade cibernética, o governo federal traçou uma estratégia para tornar o Brasil um país mais seguro em relação a essa modalidade criminosa.

Em 05 de fevereiro de 2020, foi a publicada pelo governo brasileiro a Estratégia Nacional de Segurança Cibernética - E-Ciber, cuja finalidade é a orientação do Governo federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e terá validade no quadriênio 2020-2023. (Brasil,2020)

Os objetivos da referida estratégia é 1. Tornar o Brasil mais próspero e confiável no ambiente digital; 2. Aumentar a resiliência brasileira às ameaças cibernéticas; e 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional. Sendo que uma das ações pretendidas pelo governo é Ampliar a cooperação internacional do Brasil em Segurança cibernética. (Brasil,2020)

Diante disso, pode-se inferir que o Brasil de fato possui interesse em aderir a referida convenção, bem como a adesão seria um grande passo ao combate à criminalidade informática no país, uma vez que o Brasil estaria em cooperação com uma gama de países do mundo, facilitando principalmente a investigação criminal. Além de cumprir com um de seus objetivos da estratégia publicada.

CONSIDERAÇÕES FINAIS

O presente artigo mostrou-se necessário devido ao grande número de crimes informáticos na sociedade brasileira, nos últimos tempos, levantando assim diversos questionamentos sobre como a tecnologia foi capaz de impactar a vida dos seres humanos, principalmente, quando impactou também de maneira negativa, chamando assim atenção do Direito para essa análise.

No cenário atual, é notório que a internet integra a sociedade, pois o grande alcance da internet permite que as pessoas possam estar conectadas umas às outras, mesmo estando a quilômetros de distância, bem como a comodidade proporcionada pela tecnologia faz com que cada dia mais a pessoas estejam utilizando desse ambiente, sejam em seus trabalhos, na comunicação, para aprender ou para se relacionar. (GUIDI; REZEK, 2018)

Dessa forma, o avanço da tecnologia impôs um grande desafio para os Estados, visto que surgiu uma nova modalidade criminosa. Com isso, os crimes informáticos desafiam os Estados no que tange a investigação, julgamento e punição, uma vez que autoria, materialidade e as provas podem encontrar-se a milhões de distância do local que foi sofrido o dano ou de onde será seu julgamento. (GUIDI; REZEK, 2018)

Assim, por se tratar de novos crimes, cabe ao direito penal, por meio de sua ciência jurídica observar e atuar perante essa modalidade delituosa, bem como auxiliar nas formas e procedimentos do processo penal, afim de não gerar impunidade e garantir que sejam respeitados os diretos e garantias fundamentais.

Vale salientar que o presente artigo não tem como objetivo esgotar a discussão acerca desta temática, uma vez que é possível perceber que trata-se de um assunto ainda recente no ordenamento jurídico brasileiro, porém mostrou-se necessário observar como o Brasil está se comportando juridicamente acerca dos crimes cometidos dentro e por meio do ciberespaço.

No tocante ao combate à criminalidade informática, é perceptível que dado o caráter transnacional e a complexidade dos crimes cibernéticos, não adianta o Estado

ter uma vasta legislação interna para ser eficiente no combate a estes tipos de crime. Ou seja, além da legislação interna os Estados devem recorrer aos tratados e acordos de cooperação internacional.

Em termos de cooperação internacional, a Convenção de Budapeste surge como uma resposta rápida ao combate na criminalidade informática, eis que trata-se um tratado multilateral. Ou seja, o Brasil consegue ter cooperação com um número maior de países em um único tratado ratificado. Caso o Brasil optasse por tratados bilaterais, tornaria o processo de elaboração e cooperação moroso e até ineficiente devido à grande quantidade de acordos e tratados penais que deveria realizar para atingir o mesmo objetivo que a Convenção de Budapeste propõe.

Ademais, o texto previsto na Convenção de Budapeste não fere nenhum princípio constitucional previsto no ordenamento jurídico brasileiro. Logo, não há nenhum empecilho para que o tratado seja ratificado pelo Congresso Nacional e sancionado pelo Presidente da República.

Portanto, a publicação da Estratégia Nacional de Segurança Cibernética - E-Ciber, reafirma o interesse do Brasil em combater à criminalidade cibernética por meio de cooperação internacional, sendo uma das possibilidades para pressionar o Brasil a ratificar a referida convenção, embora o Brasil já esteja em processo de adesão à Convenção de Budapeste, é importante perceber que o Brasil se propõe a cumprir os objetivos da convenção com a aprovação da estratégia, que tem validade até 2023.

Entretanto o prazo de validade da estratégia não implica em uma desobrigação do Brasil em combater a criminalidade informática, a expectativa é que até 2023, ano fim da estratégia, o Brasil seja exemplo de eficiência na batalha contra os crimes informáticos.

Além de que, uma vez ratificada a Convenção de Budapeste em nosso ordenamento jurídico, o Brasil se tornará um Estado Parte da Convenção. Dessa forma, possuirá obrigação legal de cumprir os preceitos de cooperação internacional, mas também deverá o Brasil cumprir sua parte por uma questão moral diante da comunidade internacional.

Por isso, o Procurador Geral da República, Augusto Aras, tem cobrado do Presidente da Câmara dos Deputados e do Presidente do Senado Federal uma rápida tramitação da ratificação desta convenção, afim de garantir que o Brasil possa usufruir o mais rápido possível dos benefícios que o instrumento trará. (ARAS, 2020)

Diante disso, a Convenção de Budapeste ratificada no ordenamento jurídico brasileiro, possibilitaria agilidade nas investigações criminais e garantiria segurança jurídica.

REFERÊNCIAS:

ALENCAR, Leonardo de Araújo. **Alternativas à criminalização ou à penalização do crime de furto: à luz de uma abordagem crítica do Direito Penal**. 2019. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2019.

BARBOSA, Thaís Graziella Souza. **Crimes Virtuais**. 74.f. Trabalho de Conclusão de curso. Pontifícia Universidade Católica de Campinas. Campinas-SP, 2016.

BRASIL. **Estratégia Nacional de Segurança Cibernética - E-Ciber**. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato20192022/2020/decreto/D10222.htm>. Acesso em: 03/05/2020

BRASIL. **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012**. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 13/06/2020

BRASIL. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 13/06/2020

BRASIL. Ministério da Justiça. **Cooperação Jurídica**. Disponível em: < https://www.justica.gov.br/sua-protecao/cooperacao-internacional/Cooperacao-juridica-internacional> acesso em: 22/05/2020

BRASIL. Ministério da Justiça. **Cooperação Jurídica Internacional em Matéria Penal.** Disponível em: < https://www.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal >acesso em: 22/05/2020

BRASIL. Ministério Público Federal. **Câmara de Coordenação e Revisão, 2.Crimes cibernéticos / 2a Câmara de Coordenação e Revisão, Criminal**. – Brasília: MPF,

2018.275 p. – (Coletânea de artigos; v. 3). Disponível também em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes> Acesso em: 19/04/2020

CRESPO, Marcelo. **Crimes Digitais**. São Paulo: Saraiva, 2011.

CUSNIR, Danielle. **A Problemática Dos Ciberataques em um Contexto De Cooperação Jurídica Internacional.** 66 f. Trabalho de Conclusão de Curso. Universidade Federal do Rio De Janeiro - UFRJ, Rio de Janeiro-RJ, 2018.

GIMENES, Emanuel Alberto Sperandio Garcia. **Crimes virtuais**. Revista de Doutrina da 4ª Região, Porto Alegre, n. 55, ago. 2013. Disponível em: https://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html Acesso em: 18/04/2020.

GUIDI, Guilherme Berti de Campos; REZEK, Francisco. **Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos**. Rev. Bras. Polít. Públicas, Brasília, v. 8, no 1,2018 p.276-288.

ITAMARATY. **Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública.** Disponível em:http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 18/03/2020.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual De Crimes Informáticos**. São Paulo: Saraiva, 2016.

Lei 'Carolina Dieckmann', que pune invasão de PCs, entra em vigor. G1.Disponível em: < http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html > Acesso em: 09/06/2020.

MAZONI, Ana Carolina. **Crimes na Internet e a Convenção de Budapeste**. 2009. 65 f. Trabalho de Conclusão de Curso. Faculdade de Ciências Jurídicas e Sociais-FAJS, Brasília-DF, 2009.

MINISTÉRIO PÚBLICO FEDERAL**. Convenção de Budapeste**.< http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em: 27/08/2020

MINISTÉRIO PÚBLICO FEDERAL. **MPF pede celeridade ao Congresso na ratificação do Brasil como parte da Convenção de Budapeste**.< http://www.mpf.mp.br/pgr/noticias-pgr/mpf-pede-celeridade-ao-congresso-na-ratificacao-do-brasil-como-parte-da-convencao-de-budapeste>. Acesso em: 12/09/2020

MUNIZ, Antônio Walber; CIDRÃO, Taís Vasconcelos; 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.

NETO, Eduardo Diniz**. Sociedade de risco, direito penal e política criminal**. Revista de Direito Público, Londrina, v. 5, n. 2, p. 202-220, ago. 2010

NETO, João Araújo Monteiro. **Crimes informáticos uma abordagem dinâmica ao direito penal informático.** Pensar, Fortaleza, v. 8, n. 8, p. 39-54, fev. 2003.

OLIVEIRA, Natália Silva Teixeira Rodrigues de. **Insider trading: uma realidade à luz do direito penal**. Rev. Fac. Direito UFMG, Belo Horizonte, n. 60, p. 365 a 390, jan./jun. 2012.

PNAD Contínua TIC 2017: Internet chega a três em cada quatro domicílios do país. IBGE. disponível em:< https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais>. Acesso em: 30/08/2019.

ROLFINI, Fabiana, **Brasil teve mais de 1,6 bilhão de ataques cibernéticos em três meses**< https://olhardigital.com.br/fique_seguro/noticia/brasil-teve-mais-de-1-6-bilhao-de-ataques-ciberneticos-em-tres-meses/100420> Acesso em: 28/08/2020

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

SILVA, Ana Laura Rossi. **Cibercrimes: Uma Análise Sob a Perspectiva da Aplicação do Direito Internacional**.30.f. Trabalho de Conclusão de Curso. Universidade Federal de Uberlândia-UFU, Uberlândia-MG, 2019.

SPINIELI, André Luiz Pereira. **CRIMES INFORMÁTICOS: Comentários ao Projeto dd Lei nº 5.555/2013**. Disponível em: < http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos>. Acesso em: 19/04/2020

VIANNA, Túlio; MACHADO, Felipe**. Crimes informáticos**. Belo Horizonte: Fórum.2013.