A ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE E O ENFRENTAMENTO DO CIBERCRIME: ENTRE A COOPERAÇÃO INTERNACIONAL E A EXPANSÃO DO DIREITO PENAL

BRAZIL'S ACCESSION TO THE BUDAPEST CONVENTION AND CONFIGHTING CYBERCRIME: BETWEEN INTERNATIONAL COOPERATION AND THE EXPANSION OF CRIMINAL LAW

Isadora Donza Corrêa[1]

João Araújo Monteiro Neto[2]

RESUMO: O presente artigo científico tem como objetivo analisar a adesão do Brasil à Convenção de Budapeste, tratado internacional sobre Direito Processual Penal e Direito Penal, que foi desenvolvido como uma resposta à crescente ameaça de crimes cibernéticos, pretendendo à proteção da sociedade contra a criminalidade cometida no ambiente virtual. A Convenção de Budapeste foi promulgada no Brasil em 17 de abril de 2023 através do Decreto nº 11.419. Após fimar o tratado, o Brasil se comprometeu a adotar medidas para combater os crimes cibernético, penalizando infrações relacionadas

[1] Graduada em Direito pela Universidade de Fortaleza (2023). Estágio na Defensoria Pública do Estado do Ceará 2022.2 - 2023.1 Conhecimento Office: Excel (confecção de relatórios, gráficos etc.), Word (confecção de manuais, instrumentos contratuais, etc), e Power Point (criação de apresentações). Conhecimentos na Lei Geral de Proteção de Dados (LGPD). Colaboradora no Projeto: Ciências de Dados e Inteligência Artificial para Produtividade na Prestação Jurisdicional de 1 e 2 Grau - 2020 - atual. Colaboradora no projeto: Desenvolvimento Piloto de Soluções para a Automação Processual e Uso de Técnicas de Inteligência Artificial no Poder Judiciário. Aluna especial no mestrado em Informática Aplicada na Universidade de Fortaleza (Unifor). Noção básica em programação (Python). Currículo Lattes: http://lattes.cnpq.br/0547412133956929.

[2] PhD em Direito pela Universidade de Kent no Reino Unido. Curso de Aperfeiçoamento em Resposta a Incidentes pela Organização dos Estados Americanos em parceria com o Instituto de Ciberseguridade da Espanha (INCIBE) e a Universidade de Leon na Espanha. Ex pesquisador da Universidade de Malta e Voluntário no Mandato do Relator Especial da ONU para o Direito a Privacidade. Professor de Direito Digital, Proteção de Dados Pessoais e Engenharia Jurídica no curso de Direito da Universidade de Fortaleza. Advogado especializado em Proteção de Dados e Privacidade, Presidente da Comissão de Direito Digital da OAB/CE. Certified Information Privacy Professional/Europe (CIPP/E) pela International Association of Privacy Professionals (IAPP) e Privacy Fellow pela Onetrust. Coordenador do Grupo e Estudos de Estudos em Tecnologia, Informação e Sociedade - GETIS e com atividades nas áreas de Direito da Tecnologia da Informação, Governança e Regulação da Internet, Digital Human Rights, Privacidade e Proteção de Dados Pessoais, Inteligência Artificial e Cibersegurança.. Currículo Lattes: http://lattes.cnpq.br/4255484163600547.

a computadores e infrações cibernéticas. Para uma melhor compreensão do tema, buscou-se investigá-lo por meio de pesquisa bibliográfica, com o uso de referências teóricas em livros, artigos científicos, teses e monografias. Quanto à utilização dos resultados, a pesquisa é pura, por ter finalidade precípua a ampliação dos conhecimento sobre a temática. A pesquisa classifica-se como descritiva porque busca inicialmente registrar e analisar o tema sem manipulá-lo e explicativa pois aponta as causas que levam à sua adesão. Quanto à abordagem a pesquisa é qualitativa, enfatizando a compreensão e a interpretação do tema. No tocante aos fins, o presente artigo demonstra que a Convenção de Budapeste serve como importante referência para o Brasil no combate aos cibercrimes, incentivando avanços na legislação e na cooperação internacional no combate a essa modalidade criminosa.

Palavras-chave: Cibercrimes; Convenção de Budapeste; Mecanismos de cooperação internacional.

ABSTRACT: The objective of this scholarly article is to examine Brazil's compliance with the Budapest Convention, an international agreement on criminal procedure and criminal law. The convention was created in response to the increasing threat of cybercrimes, with the goal of safeguarding the public from illicit acts carried out in virtual spaces. On April 17, 2023, Brazil ratified the Budapest Convention with Decree No. 11,419. By joining the Budapest Convention, Brazil agreed to enact laws to combat cybercrimes and to make offenses involving computers and cybercrimes punishable by law. The topic was examined through bibliographic research, utilizing theoretical references from books, theses, scientific papers, and monographs in order to gain a deeper understanding of it. In terms of applying the findings, the study is strictly scholarly, with the primary goal being the advancement of knowledge in the field. The study is categorized as explanatory since it identifies the rationale behind the subject's adherence, and as descriptive since its primary goal is to document and examine the subject without altering it. The research employs a qualitative method, prioritizing the comprehension and interpretation of the topic. In terms of objectives, this article demonstrates how Brazil can tackle cybercrimes by using the Budapest Convention as a valuable guide, which promotes improvements in legislation and global collaboration in addressing this kind of illegal activity.

Keywords: international cooperation mechanisms; cybercrimes; Budapest Convention.

1 INTRODUÇÃO

No decorrer deste artigo científico, far-se-á uma análise da Convenção de Budapeste, tratado internacional sobre Direito Processual Penal e Direito Penal, que

objetiva a proteção da sociedade contra os cibercrimes, propondo a adoção de legislação adequada entre os países signatários em busca de uma cooperação internacional entre os membros. Criada em 2001, o tratado internacional foi originalmente estabelecido no Conselho da Europa, contando com mais de 60 países signatários.

O estudo busca esclarecer pontos críticos da adesão do Brasil à Convenção de Budapeste, tratado internacional, que serve de instrumento no combate aos crimes cometidos no ambiente virtual. Considerado um marco importante na cooperação internacional em investigações criminais de cibercrimes, o tratado, requer um esforço em conjunto no combate em escala global devido à dificuldade na identificação da autoria e materialidades nos crimes desta natureza.

O presente artigo tem como objetivos específicos responder a determinados questionamentos, tais quais: O que se entende pela Convenção de Budapeste e quais os crimes previstos no referido tratado internacional? O que são os cibercrimes e quais os mecanismos utilizados para combater esses crimes de tal natureza? E por fim, a promulgação da Convenção de Budapeste na legislação brasileira será vantajosa?

Tais questionamentos serão respondidos no decorrer do presente artigo, que será resumido em três tópicos. O primeiro tem como finalidade analisar o conceito de cibercrimes, com ênfase as classificações e divergências doutrinárias. Far-se-á posteriormente uma análise acerca do combate à cibercriminalidade, em que se mencionam os procedimentos de investigação no combate aos crimes cibernéticos e a problemática envolvida durante a investigação desses crimes.

O segundo tópico explora a Convenção de Budapeste, criada em 2001, na Hungria, pelo Conselho Europeu, que entrou em vigor no ano de 2004, objetivando impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos de redes e dados. A terceira parte, trata da adesão do Brasil à Convenção de Budapeste, promulgada pelo Governo Federal, Decreto nº 11.419/2023, tratado internacional que incluirá novos tipos penais incriminadores com políticas no combate ao cibercrime.

Por fim, serão abordados os mecanismos de cooperação jurídica internacional incluídos pelo Decreto nº. 11.419/2023, no qual órgãos competentes dos estados atuam em conjunto em seus respectivos territórios, realizando atos pré-processuais ou processuais relevantes para a jurisdição estrangeira no âmbito da esfera penal.

2 CRIMES CIBERNÉTICOS

A era da tecnologia da informação teve seu início na segunda metade do século XX, quando ocorreram avanços tecnológicos significativos e uma maior disseminação de informações na sociedade. No século XXI, houve um crescimento da indústria dos computadores, com uma expansão cada vez maior do uso de recursos informáticos, como computadores, redes de fibras ópticas e tecnologia wireless etc. (COLLI, 2010, p. 15).

Dentre as principais novidades tecnológicas, encontra-se a internet. Criada na década de 90, é uma rede global de computadores que permite a transmissão de inúmeras informações com conteúdo diversos, podendo ser acessadas por computadores que ultrapassam as fronteiras geográficas e temporais de maneira imediata, facilitando a comunicação e o relacionamento entre as pessoas (COLLI, 2010, p.15).

Apesar de a tecnologia da informação ser um recurso valioso para a evolução da humanidade, cabe ressaltar que, alguns usuários desviam a sua finalidade para a preparação e consumação de infrações penais. Essa nova modalidade de delitos cometidos pelo ambiente virtual é comumente conhecida pela terminologia de crimes cibernéticos ou cibercrimes, que são crimes cometidos no ambiente computacional (VECCHIA, 2020, p. 52).

O Brasil é o segundo país com maiores prejuízos decorrentes de crimes cibernético. Conforme o Senado Federal, em apenas 3 meses do ano de 2019, o país registrou 15 bilhões de tentativas de ataques cibernéticos, com 59% dos ataques realizados com o fito de obter vantagens financeiras. (NICOLAI; ALVES, 2020).

2.1 Conceito

Os crimes cibernéticos, ou a criminalidade informática, podem ser conceituados como todo ato em que o computador ou meio de tecnologia de informação serve de meio para atingir um ato criminoso, ou ainda que, o objeto de um crime seja um computador ou um meio de tecnologia. (MARQUES; MARTINS, 2006)

Os crimes cibernéticos envolvem mais de um computador ou dispositivo telemático ou eletrônico, assim, devem estar conectados entre si por uma rede material ou imaterial. O instituto do cibercrime é a ligação entre a cibernética, o ciberespaço e os crimes informáticos, no qual esses meios de tecnologia são utilizados por usuários com o fito de cometer condutas delituosas. Portanto, para se ter um modelo de cibercrime, é necessário que o homem ao utilizar um computador, esteja por meio de uma rede de computadores, interligados no ciberespaço, cometendo condutas tipificadas como crimes (COLLI, 2010, p. 44).

Acerca da nomenclatura, os crimes cometidos na internet apresentam diversos termos doutrinários, qual seja: crimes informáticos, crimes digitais, crime informático-digital, *high technology* e *computer related crime*. Vale ressaltar que, esses crimes envolvem divergência quanto à definição, quanto à tipologia, e a classificação, no entanto, o termo cibercrime apresenta especial interesse, vez que a natureza deste é, em geral, de cunho transterritorial e transnacional. (SIMAS, 2014).

Conforme a Comissão Europeia, o cibercrime apresenta três tipos de atividades criminosas. A primeira delas abordam os crimes tradicionais, no qual são cometidos com o auxílio do computador juntamente com as redes informáticas. Em seguida, os crimes relacionados ao conteúdo, em que as publicações dos conteúdos ilícitos são realizadas através de meios de comunicação eletrônico. Por fim, estabelece os crimes exclusivos das redes eletrônicas, cometidos exclusivamente por meios informáticos (SIMAS, 2014).

Diante o exposto, pode-se concluir que a rede de internet apresenta uma grande fragilidade e meios para a perpetuação de cibercrimes, por ser uma rede de grande acesso ao público, bem como não ser regida por um ordenamento jurídico único que a discipline.

A existência de múltiplos ordenamentos jurídicos internacionais dificulta ainda mais a punição dos infratores, em razão da incompatibilidade procedimental e investigativa entre os diferentes países envolvidos em um cibercrime, sujeitando-se a sistemáticas processuais diversas (COLLI, 2010, p.45).

Por fim, pode-se concluir que, as infrações cometidas no espaço cibernético são chamadas de crimes informáticos ou crimes cibernéticos, que correspondem a qualquer ação ou omissão que possa ferir a política de segurança de uma instituição ou, ainda que possa atentar contra a segurança de um sistema informatizado.

2.2 Classificação dos cibercrimes

Na doutrina brasileira, não existe consenso sobre a expressão cibercrime, nem quanto à definição, nem quanto à tipologia e classificação destes crimes. Contudo, prevalece na doutrina a classificações dos cibercrimes entre crimes próprios e impróprios, de natureza formal, motivo pelo qual a consumação desses crimes acontece no momento da prática delitiva, independente do resultado naturalístico.

A primeira classificação aborda os crimes cibernéticos próprios ou exclusivamente cibernéticos, no qual são conceituados como toda atividade criminosa com principal objetivo a utilização de ambiente computacional, por isso, a execução do crime depende da utilização dos recursos tecnológicos como meio e objeto para a prática delituosa, sendo o ambiente computacional o objeto juridicamente tutelado (VECCHIA, 2020, p.53).

Além disso, nos crimes cibernéticos próprios, se referem ao uso da tecnologia da informação como meio necessário para a sua realização, assim, o autor do crime utiliza o sistema informático pertencente ao destinatário do crime, sendo o computador objeto e meio para a execução do crime. A título de exemplificação, pode-se mencionar o acesso não autorizado a sistemas informáticos, a interceptação de comunicações eletrônicas, fraudes eletrônicas, pornografia infantil etc. (VECCHIA, 2020, p.53).

Assim, é possível perceber que todos esses crimes utilizam a tecnologia da informação como meio para a sua realização, sendo importante destacar que essas práticas violam a privacidade, a segurança e a proteção dos dados pessoais das vítimas, gerando prejuízos e danos tanto para pessoas físicas quanto para empresas.

A segunda classificação aborda os crimes cibernéticos impróprios ou abertos, em que o ambiente computacional é o meio pelo qual é realizada a execução da conduta ilícita. Contudo, não necessariamente precisa do uso da tecnologia para se obter o resultado, ou seja, são crimes comuns que podem ser cometidos por meios diversos, como: divulgação de conteúdo ilícito na internet, comércio ilegal na internet, extorsão virtual, difamação online, entre outros (VECCHIA, 2020, p.53).

Ademais, todos esses crimes podem ser realizados sem a necessidade de se utilizar diretamente a tecnologia da informação como meio de ataque, mas, ainda assim, são considerados cibernéticos pelo fato de terem sido cometidos pelo uso de plataformas e sistemas-digitais. Os crimes cibernéticos impróprios utilizam a internet ou outras plataformas digitais como ferramentas para a prática de ilícitos, causando danos substanciais às vítimas.

2.3 Combate à cibercriminalidade

A investigação cibernética realizada no espaço cibernético ou em um dispositivo computacional é o campo de estudo da computação forense. Assim, a computação forense ou também chamada de perícia digital, tem como principal objetivo identificar, coletar, preservar e apresentar vestígios digitais com mais validade probatória em juízo. Os vestígios digitais são considerados informações que são deixadas em sistemas, dispositivos ou redes de computadores após a realização de atividades digitais, podendo ser exemplificado como: fragmentos de arquivos, textos, imagens, vídeos, registro de conexão à internet, bate-papo nas redes sociais, entre outros (NOGUEIRA, 2018).

A criminalística é a área responsável pela Forense Digital, no qual, aplica a ciência da computação e os procedimentos de investigação, no qual fornece evidências técnicas

para solucionar casos criminais, assim, esses métodos e técnicas realizados no objeto de perícia, auxilia na busca da materialidade e autoria dos incidentes de segurança e delitos perpetrados no ambiente cibernético (BRASIL, 2015).

Contudo, a investigação dos cibercrimes enfrenta uma problemática quanto as investigações preliminares desenvolvidas nesse ambiente, quanto à natureza do crime, os sujeitos, o tempo, o lugar de cometimento e as provas obtidas das infrações penais cometidas pela internet. Nesse contexto, devem-se analisar três elementos essenciais para a caracterização de um crime: a tipicidade, a ilicitude e a culpabilidade (BITENCOURT, 2006).

Segundo Bitencourt (2006), a tipicidade decorre do princípio da reserva legal, podendo ser brevemente definida como a conformidade entre o fato praticado pelo agente e a previsão do crime descrito no texto penal. Seguindo a mesma linha de pensamento do referido autor, a ilicitude seria a relação entre a conduta humana voluntária e o ordenamento jurídico, podendo assim ser definida como, um comportamento que contraria a ordem jurídica estabelecida em um território, em um determinado tempo.

A culpabilidade é o juízo que será feito sobre a reprovabilidade da conduta do agente, para deliberar sobre a prática ou não de uma infração penal. No Brasil, prevalece a teoria finalista, que apresenta três categorias na doutrina. A primeira delibera sobre a imputabilidade, em que trata de presunção de culpabilidade, podendo ser excluída pelos casos previstos em Lei. Em seguida, a segunda categoria trata sobre erro de proibição, em que o autor se equivoca acerca da ilicitude ou licitude do seu comportamento. Por fim, a terceira categoria trata sobre a exigibilidade de conduta diversa, sendo assim, é feito juízo de valor sobre o efeito das circunstâncias na conduta do autor (JUNQUEIRA, 2018).

Desta forma, para que ocorra a consumação de um crime cibernético, parte-se do pressuposto que, o fato deve ser típico, ilícito e culpável, e que seja lesivo a um bem jurídico tutelado pelo ordenamento jurídico brasileiro. Contudo, a tipicidade apresenta uma das principais problemáticas, devido ao surgimento diário de *malware* por programadores, *hackers* ou meros usuários, que se aproveitam das novas tecnologias para cometerem condutas danosas ou que ofereçam riscos a bens jurídicos cometidos através

da internet. Assim, ensejam situações que, apesar de serem ilícitas, são consideradas irrelevantes para o Direito Penal, por inexistir tipicidade caracterizadora da infração penal (COLLI, 2010, p.81).

A legislação brasileira, devido ao princípio da soberania, está limitada pela área territorial nacional para a punição dos crimes cibernéticos, o que dificulta as investigações policiais, já que a natureza destes delitos em sua maioria é de cunho transterritorial e transnacional. Neste seguimento, a existência de múltiplos ordenamentos jurídicos internacionais dificulta ainda mais a punição dos infratores, em razão da incompatibilidade procedimental investigativa entre os diferentes países envolvidos em um cibercrime, sendo assim, sujeitos e etapas diferentes estarão diante de sistemáticas processuais igualmente diversas (COLLI, 2010, p.81).

O principal meio para evolução das investigações policiais e a prevenção de cibercrimes deve ser por intermédio da cooperação internacional, necessitando que o Estado busque através de tratados e acordos internacionais sobre o tema, a obtenção da harmonização da legislação material e processual penal entre as nações.

Além disso, é necessário que os países signatários da comunidade internacional adequem a criação de unidades policiais especializadas em crimes informáticos, cibernéticos, e a conjugação de esforços entre autoridades investigadoras e provedores de internet (COLLI, 2010, p.82).

Na tentativa de uma colaboração internacional, o Conselho Europeu, no ano de 2001 firmou a Convenção de Budapeste, objetivando impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos de redes e dados, assim, estabeleceu um extenso rol de diretrizes e regras para a adequação legal (material e processual) para a solução dos crimes cibernéticos nas relações internacionais (BRASIL, 2022).

Por fim, a cooperação internacional em matéria Penal e a internacionalização do Direito Cibernético irão garantir o enfrentamento do cibercrime, permitindo vínculo entre os sistemas judiciais internacionais, punindo e extraditando os responsáveis pela via da assistência jurídica mútua.

3 A CONVENÇÃO DE BUDAPESTE

O terceiro tópico abordará acerca da Convenção de Budapeste, enfatizando o processo histórico de criação, os seus principais elementos e os mecanismos de cooperação internacional implementados pelo tratado internacional.

3.1 Processo histórico da Convenção

Criada em 2001, a Convenção de Budapeste é um tratado internacional sobre direito processual penal e direito penal, no qual foi originalmente estabelecida no Conselho da Europa, englobando mais de 60 países signatários.

O Conselho Europeu criou o referido tratado objetivando realizar uma união mais estreita com os Estados-membros do presente tratado internacional, criando uma política criminal comum, que objetiva a proteção da sociedade contra os cibercrimes, adotando a legislação adequada entre os países signatários em busca de uma cooperação internacional entre os membros (BUDAPESTE, 2001).

A iniciativa para criação da convenção foi liderada pelo Conselho Europeu, com a participação de especialistas de países de todo o mundo e organizações internacionais. O processo envolveu diversas reuniões e audiências públicas para discutir o conteúdo e as questões legais em relação às implicações da criminalidade cibernética. A convenção foi desenvolvida como uma resposta à crescente ameaça de crimes cibernéticos que se tornaram cada vez mais sofisticados, difíceis de detectar e combatidos no âmbito nacional.

Além disso, o tratado internacional objetiva facilitar o intercâmbio de informações e a cooperação entre autoridades nacionais no combate à criminalidade cibernética, através da harmonização das leis nacionais e internacionais.

3.2 Delimitação dos crimes da Convenção de Budapeste

Assim como os crimes reais, os crimes virtuais têm sua jurisdição, a diferença é que os cibercrimes abordam inúmeras jurisdições devido as suas constantes modificações. As condutas criminosas cometidas na internet apresentam dificuldades na definição de tempo e lugar em que ocorreu a consumação do crime, por não haver fronteiras que estabeleçam o local no qual o criminoso realizou o delito. Desta forma, a complexidade de estabelecer o local da consumação do delito abre o questionamento pelo qual será a jurisdição competente para julgar o crime virtual cometido, e em qual país ficaria obrigado a responder pelo fato criminoso.

Diante da dificuldade apresentada em estabelecer a competência para julgar os crimes virtuais, a União Europeia, quando fica evidente que um crime ultrapassou as fronteiras do referido país, estabelece que a competência para julgar o fato criminoso será de todos os países envolvidos, assim, o combate para tal delito será solucionado através de acordos, no qual irão dispor a possibilidade de todos os países-membros de investigar o crime cometido fora de sua jurisdição.

A Convenção Europeia implementou medidas inéditas para o ambiente tecnológico, protegendo dados específicos de computadores, que caso fossem afetados, poderiam atingir diretamente direitos humanos e de liberdades individuais protegidos. Cabe ressaltar que, a Convenção Europeia faz referência expressa ao princípio da ofensividade, com o fito de indicar opções de criminalização de condutas que lesionem ou coloque em perigo um bem juridicamente tutelado que envolvem o abuso no uso de computadores.

Os países signatários da Convenção de Budapeste determinam sua jurisdição quando identificam a consequência real do crime praticado pela internet, assim, ao determinar o local do crime, será possível identificar a jurisdição competente para julgar a autoria do crime e a prova da materialidade. Cabe ressaltar que, alguns países vinculados a Convenção de Budapeste desenvolveram como solução de impasse a adoção da doutrina do efeito potencial do crime, permitindo a persecução penal, assim, caso o país signatário

encontre material hospedado em um servidor de outro país, e seja acessado em território nacional, os efeitos serão produzidos no território do acesso.

Neste seguimento, cabe salientar que existem três níveis de jurisdição na internet: o espaço físico, no qual, as pessoas são vinculadas ao espaço corpóreo que habitam, cabendo os cidadãos respeitar a legislação; os dos provedores de acesso, em que as pessoas se submetem as leis vigentes no país do referido provedor; por fim, os dos domínios e comunidades, que operam sem respeitar fronteiras internacionais ou de outros provedores.

A Convenção de Budapeste tem como objetivo a harmonia entre as legislações penais substantivas, estabelecendo o elemento dos delitos e outras previsões conexas sobre delitos de informática. Além disso, a referida convenção cumpre com o objetivo de alterar as legislações processuais nacionais, concedendo poderes de investigação e de persecução criminal, com o fito de combater delitos praticados com o uso de sistemas de computadores, ou outros delitos que envolvam provas obtidas mediante meios eletrônicos, com regime célere e efetivo de cooperação internacional.

No que consiste aos temas abordados na Convenção de Budapeste, a sua divisão está composta por quatro capítulos. O primeiro trata sobre os crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computadores, no qual está previsto o acesso ilegal à integralidade ou parte de sistema de computadores sem autorização, a interceptação ilegal, interferência ou danos em dados de computador, e por fim, a interferência em sistemas (BUDAPESTE, 2001).

O segundo capítulo da Convenção aborda os crimes já tipificados em legislações comuns, porém, os mesmos crimes sendo praticados por meio de computadores, como os crimes de falsificação eletrônica praticadas por meio de computadores e fraude informática. O terceiro capítulo preconiza as ofensas relacionadas à pornografia infantil. Por fim, no quarto capítulo, aborda os crimes relacionados à violação de direitos de autor em geral, ou condutas delituosas contra a propriedade intelectual (BUDAPESTE, 2001).

3.3 Principais elementos da Convenção de Budapeste

Inicialmente, a Convenção de Budapeste se inicia com a definição de conceitos e crimes cibernéticos até os mecanismos de cooperação entre os Estados-membros. Como dito anteriormente, a inclusão de alguns crimes inseridos pelo referido tratado podem ser estabelecidos como: acesso não autorizado a dispositivo eletrônico, interceptação ilegal a sistemas, interceptação ilegal de comunicações eletrônicas, pornografia infantil e fraude eletrônica.

Em seguida, a jurisdição estabelecida pela Convenção de Budapeste estabelece as bases da extraterritorialidade de lei em relação aos crimes cibernéticos, permitindo a cooperação entre os Estados-membros a operarem conjuntamente nas medidas legais contra os indivíduos ou organizações que cometeram tais delitos.

Cabe mencionar a cooperação internacional, mecanismo primordial da referida Convenção de Budapeste, em que prevê a cooperação entre os países membros na prevenção e investigação de crimes cibernéticos, incluindo a coleta e compartilhamento de informações e a extradição de suspeitos. Ademais, a proteção de dados pessoais também é considerado um elemento importante após a adesão do referido tratado internacional, em que a Convenção define as responsabilidades dos países a proteger os dados pessoais e de privacidade dos indivíduos, inserindo regras para o compartilhamento de informações e medidas de segurança.

Ademais, a proteção de dados pessoais também é considerado um elemento importante após a adesão do referido tratado internacional, em que a Convenção define as responsabilidades dos países a proteger os dados pessoais e de privacidade dos indivíduos, inserindo regras para o compartilhamento de informações e medidas de segurança. Por fim, insta destacar acerca do desenvolvimento de políticas públicas e estratégicas, em que a convenção necessita de políticas e estratégias nacionais para a prevenção e combate aos cibercrimes, devendo incluir medidas legais, técnicas, organizacionais e educacionais.

3.4 Mecanismos de cooperação internacional

A Convenção de Budapeste sobre Cibercrime estabelece vários mecanismos de cooperação internacional para combater a cibercriminalidade e prevenir violações dos direitos humanos no ambiente virtual. Além disso, a Convenção supramencionada também viabiliza a racionalidade do Direito Penal em cooperação internacional, tipificando condutas por meio da harmonização da legislação penal entre os países-membros, assim, garantindo o enfrentamento dos crimes cometidos pelo computador, por serem infrações que ultrapassam fronteiras internacionais, no qual haverá diálogo entre os diversos sistemas jurídicos internacionais (CASTRO, 2018).

O primeiro mecanismo de cooperação internacional estabelecido pela Convenção de Budapeste é o sistema de plantão 24 por 7, em que busca estabelecer e manter uma rede de contato com duração de 24 horas para permitir a rápida troca de informações sobre os crimes cibernéticos. A cooperação Internacional é outro mecanismo estabelecido pela Convenção de Budapeste, em que os Estados-membros devem cooperar entre si nas investigações em combate aos cibercrimes, incluindo o intercâmbio de informações relevantes e a implementação de ações conjuntas. O referido dispositivo está disposto no artigo 23, Capítulo III, Título 1, do Decreto nº 11.491/2023.

Dando seguimento aos mecanismos de cooperação, a extradição prevista pela Convenção de Budapeste prevista no artigo 24 do mesmo Decreto, estabelece regras para a extradição de indivíduos relacionados aos cibercrimes, desde que o tipo penal seja listado na legislação dos Estados-membros e seja possível a prova da materialidade do delito e a autoria.

Diante o exposto, devido os mecanismos de cooperação internacional impostos pela Convenção de Budapeste, pode-se concluir que visa promover a prevenção dos crimes cometidos no ambiente virtual, bem como a proteção dos direitos humanos no ambiente digital.

Ressalta-se ainda que, esses dispositivos são importantes para garantir que as autoridades policiais de diferentes países possam colaborar efetivamente em

investigações de crimes digitais, evitando lacunas no combate à cibercriminalidade decorrentes das fronteiras geográficas.

4 O PROCESSO DE ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE

O processo de adesão do Brasil à Convenção de Budapeste sobre Crimes Cibernéticos começou em 2009, com a assinatura do documento em uma cerimônia realizada em Estrasburgo, na França. Na época, o Brasil foi representado pelo então ministro de Relações Exteriores, Celso Amorim.

Após a assinatura, o Brasil iniciou o processo interno necessário para tornar a convenção parte de sua legislação nacional. Em 2011, foi elaborado um relatório detalhado sobre a adesão, que passou por avaliação de diversas áreas do governo, incluindo as áreas de Justiça, Segurança Pública e Relações Exteriores (BRASIL, 2019).

Ao aderir à convenção, o Brasil se comprometeu a desenvolver e fortalecer seus mecanismos jurídicos, administrativos e técnicos para combater os crimes cibernéticos. Isso inclui o desenvolvimento de leis e políticas nacionais para prevenir e investigar esses crimes, promover a cooperação internacional na área de crimes cibernéticos e reunir evidências para processar aqueles que cometem crimes online.

Datada em 15 de dezembro de 2021, a Convenção de Budapeste foi aprovada pelo Senado e promulgada pelo Governo Federal em 17 de abril de 2023, em Brasília, Decreto nº 11.419, que traz a decisão publicada no Diário Oficial da União (DOU), no dia 12 de abril de 2023.

4.1 Adequação dos mecanismos de criminalização

Inicialmente, cabe ressaltar que a legislação penal brasileira já previa alguns crimes estabelecidos pela Convenção de Budapeste, tais como o acesso não autorizado a dispositivos eletrônicos, interceptação e divulgação não autorizada de informações pessoais, pornografia infantil e fraudes informática. Contudo, a legislação brasileira

precisou adaptar-se para atender a diversos requisitos da convenção, como a implementação da nova definição de crimes cibernéticos e as novas tipificações de delitos listados que devem ser criminalizados pelos Estados-membros.

Dando início ao comparativo entre a Convenção de Budapeste e a lei brasileira, se dará início pela Seção 1, Título 1, artigo 2º, do Decreto nº 11.491/2023, em que se trata do acesso ilegal a um sistema de informação, no qual o acesso doloso a um sistema protegido por senha objetivando obter dados de computador ou outro meio fraudulento é considerado crime, conforme a seguinte redação:

> [...] Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, o acesso doloso e não autorizado à totalidade de um sistema de computador ou a parte dele. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento mediante a violação de medidas de segurança; com o fim de obter dados de computador ou com outro objetivo fraudulento; ou contra um sistema de computador que esteja conectado a outro sistema de computador. (BRASIL, 2023).

Cabe ressaltar que, a legislação brasileira já protegia o acesso ilegal, sendo regulado pela Lei Carolina Dieckmann, em seu artigo 154-A, Lei nº 12.737 de 2012, que ficou conhecida como a Lei dos Crimes Eletrônicos, no qual prevê como conduta ilegal a obtenção não autorizada de dados armazenados em dispositivos eletrônicos, como celulares e computadores, configura o crime de "acesso não autorizado" e é punível com pena de três meses a um ano de detenção, além de multa. O mesmo tipo de punição é aplicável a quem produz, distribui ou comercializa programas de computador voltados para a prática deste crime. Segue redação do dispositivo legal supramencionado:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita. (BRASIL, 2012).

Além disso, a legislação brasileira estipula punição para o acesso não autorizado a um sistema informático ou de telecomunicações. Isso inclui, por exemplo, a obtenção de informações de uma rede ou sistema sem autorização ou permissão expressa do

proprietário ou administrador do sistema. Essa lei é aplicável a qualquer pessoa que obtenha esses dados sem autorização, independentemente do motivo ou finalidade do ato. Essa lei se aplica também a quem pratica essa atividade com o objetivo de obter vantagem econômica ou financeira.

Assim, pode-se concluir que, a legislação brasileira já dispõe de medidas para prevenir, investigar e punir o acesso não autorizado a dispositivos eletrônicos, o que vai ao encontro dos padrões estabelecidos pela Convenção de Budapeste. Contudo, é importante observar que a legislação precisa ser constantemente atualizada e aprimorada para acompanhar as constantes mudanças na tecnologia e nas ameaças dos crimes cibernéticos.

Dando seguimento a análise da legislação brasileira anterior com a nova lei da Convenção de Budapeste, o artigo 3º, Seção 1 do Decreto nº 11.491/2023 aborda a tipificação de interceptação ilícita, em que aborda condutas ilícitas aos indivíduos que interceptam comunicações eletrônicas, com objetivo fraudulento ou praticado contra um sistema de computador que esteja conectado a outro sistema de computador. A título de exemplo, pode-se mencionar o indivíduo que intercepta comunicações eletrônicas, como e-mails ou mensagens criptografadas. Segue a redação do artigo mencionado acima:

> [...] Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime em sua legislação interna a interceptação ilegal e intencional, realizada por meios técnicos, de transmissões não-públicas de dados de computador para um sistema informatizado, a partir dele ou dentro dele, inclusive das emissões eletromagnéticas oriundas de um sistema informatizado que contenham esses dados de computador. Qualquer Parte pode exigir para a tipificação do crime o seu cometimento com objetivo fraudulento ou que seja praticado contra um sistema de computador que esteja conectado a outro sistema de computador. (BRASIL, 2023).

Apesar de a tipificação supramencionada ser incluída pela promulgação da Convenção de Budapeste em 2023, a legislação brasileira tipifica esse delito na Constituição Federal em seu artigo 5º, inciso XII, estabelecendo que é inviolável o sigilo das comunicações telegráficas, de dados e telefônicas, exceto por ordem judicial, para

fins de investigação criminal ou instrução processual penal. Assim segue a redação do dispositivo mencionado acima:

> Art. 5º [...]: XII - e inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. (BRASIL, 1998).

Além disso, a autorização da interceptação telefônica ou telemática é regulada pela Lei 9.296/96, que estabelece os critérios e procedimentos a serem seguidos pelas autoridades encarregadas da aplicação da lei. Assim, para configurar o crime de interceptação ilícita no Brasil, a legislação penal exige que a interceptação tenha ocorrido sem autorização judicial ou em desacordo com as disposições legais. A pena prevista para esse delito é de reclusão, de dois a quatro anos, e multa.

É importante destacar que, no Brasil, a interceptação telefônica ou telemática só pode ser realizada por autorização judicial especificamente solicitada para este fim, com fundamentação adequada e em cumprimento com todos os critérios estabelecidos pela lei. Além disso, a autorização de interceptação deve ter fim específico, não podendo ser utilizada ou mantida após o término do objetivo determinado pela autoridade judicial.

Dessa forma, a legislação brasileira já prevê medidas para prevenir e reprimir a interceptação ilícita de informações eletrônicas, atendendo aos requisitos da Convenção de Budapeste. É importante ressaltar que a proteção da privacidade dos usuários da internet e a manutenção de um ambiente eletrônico seguro são fundamentais para a garantia dos direitos humanos e do Estado Democrático de Direito.

Dando continuação ao Decreto nº 11.491/2023, insta salientar em seu título 2, o artigo 7º, no qual aborda sobre o tema de falsificação informática, consistindo em um ato em que o indivíduo distribui ou utiliza um *malware*, objetivando danificar ou obter informações de um sistema.

> [...] Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, a inserção, alteração, apagamento ou supressão, dolosos e não autorizados, de dados de computador,

> de que resultem dados inautênticos, com o fim de que sejam tidos como legais, ou tenham esse efeito, como se autênticos fossem, independentemente de os dados serem ou não diretamente legíveis e inteligíveis. Qualquer Parte pode exigir, para a tipificação do crime, o seu cometimento com intenção de defraudar ou com outro objetivo fraudulento. (BRASIL, 2023).

O artigo mencionado anteriormente aborda os crimes de falsificação informática cometido por meio eletrônico, contudo, a legislação brasileira já tipificava o crime de falsidade informática em seu artigo 3º da Lei nº 109/2009, preceituando a seguinte redação:

> [...] Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias. (BRASIL, 2009).

O crime de falsidade informática resulta na alteração dos dados inseridos num sistema informático ou do tratamento por via do mesmo sistema, em que resulta na criação de documentos ou dados falsos, gerando insegurança e desconfiança nos documentos no tráfico jurídico-probatório. Diferente do que dispõe o 3º da Lei nº 109/2009, o artigo 7º (Título 2) do Decreto nº 11.491/2023, estabelece que, danificar ou obter informações de um sistema por meio da inserção, alteração, apagamento ou supressão, de forma dolosa e não autorizada, objetivando defraudar ou com outro objetivo fraudulento é tipificado como crime. Dando seguimento ao estudo, o artigo 8º (Título 2) do Decreto nº 11.491/2023 que dispõe sobre fraude informática, dispõe a seguinte redação:

> Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, a conduta de quem causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem por meio de: a. qualquer inserção, alteração, apagamento ou supressão de dados de computador; b. qualquer interferência no funcionamento de um computador ou de um sistema de computadores, realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita. (BRASIL, 2023).

Ocorre que, a legislação brasileira em seu artigo 171, §2º-A do Código Penal trata sobre a fraude eletrônica, que ocorre se for cometida através de informações ditas pela vítima ou terceiro induzido, através de redes sociais ou outros meios fraudulentos análogos. Além disso, em seu §2-B, estabelece aumento de pena para quando o servidor utilizado estiver além do território nacional. Segue a redação do referido dispositivo:

> Art. 171 – [...] § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. [...] § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional [...]. (BRASIL, 1940).

Além disso, cabe mencionar a Lei nº 12.737/12, conhecida como Lei Carolina Dieckmann, prevê sanções penais para os crimes cometidos contra a privacidade na internet, como a exposição de conteúdos de natureza íntima sem consentimento. Outra importante legislação é a Lei Geral de Proteção de Dados (LGPD), que estabelece diretrizes para a proteção e o uso adequado de dados pessoais no Brasil. A LGPD prevê medidas protetivas que buscam evitar a exposição de informações confidenciais na rede, bem como a necessidade de consentimento explícito por parte dos usuários em relação à coleta e tratamento de dados.

Em suma, a legislação brasileira possui disposições que buscam coibir as fraudes eletrônicas e outros tipos de cibercrimes, estando em consonância com as disposições estabelecidas pela Convenção de Budapeste. A proteção da privacidade e segurança dos usuários da internet e o combate à criminalidade digital são fundamentais para a manutenção da confiança na rede e para a garantia dos direitos dos usuários.

Por fim, o artigo 9º (Título 3) do Decreto nº 11.491/2023, aborda sobre os crimes relacionados ao conteúdo da informação, especificamente sobre o crime de pornografia infantil, em que é tipificado condutas, cometidas dolosamente, a produção de pornografia infantil distribuída por meio de sistema de computador.

Fazendo ênfase a esse novo crime inserido pela Convenção de Budapeste, também vale mencionar os artigos 240 e 241 da Lei nº 11.829/2008 (Estatuto da Criança e do Adolescente), em que tipifica o crime de pornografia infantil. O artigo 240 do ECA é classificado como crime comum, assim, pode ser cometido por qualquer pessoa, além de ser considerado como crime formal, que independe de resultado naturalístico. Cabe ressaltar que esse artigo trata de crimes praticados por meio de computadores com acesso à internet, e lidera o número de denúncias, principalmente por lidar com vítimas tão vulneráveis, como crianças e adolescentes.

O Código Penal Brasileiro também prevê a penalização da produção, venda, exposição, distribuição, publicação, divulgação e armazenamento de material pornográfico envolvendo crianças e adolescentes, estipulando pena de reclusão de quatro a oito anos e multa. Além dessas legislações, o Brasil também é signatário da Convenção da Haia sobre os Aspectos Civis do Sequestro Internacional de Crianças, que estabelece a cooperação internacional para a proteção dos direitos da criança, incluindo medidas para prevenção e erradicação da exploração sexual de crianças.

Dessa forma, é possível concluir que a legislação brasileira está em conformidade com as exigências da Convenção de Budapeste no tocante à pornografia infantil, prevendo medidas rigorosas de proteção das crianças e adolescentes contra esse tipo de crime.

4.2 Adequação dos mecanismos de cooperação técnicas

O processo de adequação da Convenção sobre Cibercrime na legislação brasileira exigirá novos poderes e procedimentos para a obtenção de provas eletrônicas e prestação de assistência jurídica mútua entre os Estados-membros, não limitada a crimes cibernéticos. A Convenção de Budapeste foi promulgada no Brasil através do Decreto nº 11.491/2023, assim, segue a análise da introdução da cooperação internacional após a promulgação do referido decreto e a necessidade de harmonização com a legislação brasileira.

A legislação brasileira, estabelece na Constituição Federal de 1988 a competência dos órgãos que tratam acerca dos procedimentos de cooperação jurídica internacional. O Supremo Tribunal Federal é um órgão competente para tal assunto, podendo processar e julgar pedidos de extradição solicitados por Estados estrangeiros, assim segue o dispositivo: "Art. 102. Compete ao Supremo Tribunal Federal, precipuamente, a guarda da Constituição, cabendo-lhe: I - processar e julgar, originariamente:[...] g) a extradição solicitada por Estado estrangeiro [...]" (BRASIL, 1988).

Além disso, o Superior Tribunal de Justiça detém competência para a homologação de sentenças estrangeiras e a concessão de exequatur às cartas rogatórias, conforme artigo 105, inciso I, alínea "i" da Constituição Federal de 1988. Por fim, a Justiça Federal possui competência para a execução das cartas rogatórias após o exequatur, e a sentença estrangeira após homologação, assim dispõe o artigo 109, inciso X da Constituição Federal de 1988.

O artigo 733 do Código de Processo Penal trata dos instrumentos utilizados para comunicação entre autoridades nacionais e estrangeiras para a cooperação jurídica, assim, prevê a necessidade de sua remessa pelo juiz singular ao Ministro da Justiça, com o fito de dar cumprimento por via diplomática às autoridades estrangeiras competentes. Segue o artigo 733 do CPP, com a seguinte redação:

> O juiz, de ofício, ou a requerimento do interessado, do Ministério Público, ou do Conselho Penitenciário, julgará extinta a pena privativa de liberdade, se expirar o prazo do livramento sem revogação, ou na hipótese do artigo anterior, for o liberado absolvido por sentença irrecorrível. (BRASIL, 1941).

A Cooperação Direta entre as polícias é uma cooperação que não necessita da intervenção do Poder Judiciário para sua validade, no qual ocorre através do intercâmbio de informações policiais por meio da Interpol, em que consiste na atuação da autoridade nacional em busca de realizações de diligências investigativas no território nacional de um país estrangeiro, e vice-versa (COAF, 2020).

Vale ressaltar que, essa cooperação é coordenada pelo órgão da Polícia Federal, em que é feita dentro do território brasileiro, através da Coordenação-Geral de

Cooperação Internacional (CGCI), que opera dentro do Departamento de Polícia Federal. A cooperação possui atribuições como de intercâmbio de informações do mesmo gênero e organizações reconhecidas pelo Brasil, em que congregam organismos policiais ou demonstram interesses na investigação de crimes, assim, pode ser mencionado exemplos como a Interpol, Europol, Ameripol etc. (COAF, 2020).

Apesar de o Brasil caminhar no sentido de uma melhoria na cooperação jurídica internacional, o combate aos cribercrimes demonstra uma complexidade maior quando se trata de crimes que não respeitam as fronteiras, sendo necessário um auxílio maior entre os países para uma efetividade no enfrentamento à cibercriminalidade. Diante esse problema, o Brasil tornou-se país membro da Convenção de Budapeste, tratado internacional que uniformiza a forma como os Estados tratam do assunto.

A Convenção de Budapeste inclui mecanismos de cooperação técnica para os países-membros objetivando a prevenção dos crimes cibernéticos, tais quais: o estabelecimento de marcos legais para a prevenção e combate aos cibercrimes, definindo o conceito de cibercrimes e as sanções claras para este crime; a melhoria da capacidade de investigação e processo de crimes cibernéticos incluindo melhorias na capacitação de autoridades encarregadas da aplicação da lei e o desenvolvimento de estratégias para combater esses crimes; a cooperação internacional entre os países-membros em busca da prevenção dos crimes cibernéticos; e o fomento de inovações e tecnologias, para prevenir e reprimir os crimes cibernéticos.

4.3 Os possíveis problemas na adesão do Brasil à Convenção de Budapeste

A legislação brasileira no quesito combate aos cibercrimes e a cooperação internacional apresenta um grande atraso, pois não há lei nacional ou internacional que supra a necessidade no combate dos crimes virtuais, principalmente quando se aborda os temas de investigação e punição dos referidos crimes. A adesão do Brasil à Convenção de Budapeste foi o meio legal mais eficaz na identificação e punição dos cibercriminosos,

necessitando, assim, de algumas adequações legislativas para fazer parte dos países signatários desse tratado.

Inicialmente, a adesão do tratado internacional no ordenamento jurídico brasileiro foi considerada pelas autoridades governamentais uma grande conquista na luta contra os crimes virtuais, contudo, o processo de adesão também gerou grandes preocupações, qual seja: a celeridade no processo de adesão; a adesão total e irrestrita à Convenção de Budapeste; e por fim, a falta de uma lei geral de proteção de dados pessoais que aborde os temas de persecução penal e segurança pública.

Apesar da celeridade da adesão do tratado internacional na legislação brasileira, o tema foi discutido anteriormente por uma parcela da população, delimitando preocupações e falhas recorrentes no combate aos cribercrimes que deveriam ser consertadas. A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira necessárias na prevenção do vazamento de dados pessoais, consequentemente podendo ser considerada como um meio de prevenção de crimes virtuais (DUARTE, 2022).

Apesar de as leis vigentes na legislação brasileiras demonstrarem ineficácia quanto aos crimes que ultrapassam as fronteiras internacionais, ressalta-se que estas estão dentro dos padrões internacionais criados pela Convenção de Budapeste, pois o referido tratado foi utilizado como guia na criação destas normas. Ademais, tendo em vista as poucas discussão e debates acerca do tratado internacional supramencionado, enfatizando as leis brasileiras e a adequação dos novos tipos penais inseridos pela Convenção, ainda poderá ser alvo de discussão mesmo após a promulgação do Decreto nº 11.491/2023, principalmente pelas autoridades nacionais como o Ministério Público em um processo democrático (DUARTE, 2022).

O segundo tema de pauta de discursão, aborda acerca da adesão total e irrestrita à Convenção de Budapeste no Brasil, no qual, o novo Decreto 11.491/2023 após a sua entrada em vigor necessitaria de adequações na legislação brasileira já vigente, ocasionando, consequentemente conflitos para as devidas mudanças. Contudo, o tratado internacional supramencionado busca harmonizar e estabelecer normas comuns para a

prevenção de crimes cibernéticos em todo o mundo, incluindo a proteção de dados pessoais.

Para evitar conflitos entre a Convenção de Budapeste e as leis nacionais, é importante que o Brasil adote medidas legais e institucionais após implementação da Convenção. Essas medidas incluem a criação de leis nacionais que estejam em conformidade com as normas estabelecidas na Convenção, a capacitação dos órgãos de fiscalização para lidar com questões relativas a crimes cibernéticos, e a adaptação de instâncias administrativas e judiciárias para tratar com os novos desafios provenientes do ambiente virtual.

Assim, a implementação da Convenção pode gerar conflitos de leis, contudo, esse conflito pode ser minimizado e controlado por meio de adoção de medidas legais e institucionais adequadas através da cooperação internacional. Apesar das preocupações acerca da adequação total e sem restrições ao tratado internacional, vale ressaltar que, durante o processo de adequação não ocorreu nenhum tipo de conflito significante entre a legislação brasileira e a Convenção de Budapeste, ou outro instrumento internacional de direitos humanos.

O terceiro tema causador de preocupação na adesão da Convenção de Budapeste à legislação brasileira é acerca da privacidade, devido a Convenção estabelecer a previsão de autorização para que as autoridades dos Estados-membros coletem, analisem e divulguem dados armazenados em sistemas informáticos para a prevenção e repressão de crimes cibernéticos. Diante disso, essa autorização pode levar a invasão de privacidade, especialmente se não houver mecanismos adequados de proteção de dados pessoais.

Assim, essa preocupação pode ser descartada e evitada caso utilize mecanismos de proteção de dados, tais como a anonimização de dados pessoais, em que busca resguardar os dados dos usuários, para fins de prevenção e repressão dos crimes cibernéticos; a criptografia de dados pessoais, dificultando o acesso às informações, resguardando a privacidade das pessoas e prevenindo a invasão indevida de sistemas informáticos; a regulação de acesso e compartilhamento de dados, estabelecendo limites claros e precisos

para a coleta; e por fim, o fortalecimento das instituições de proteção de dados, em busca de garantir o direito dos cidadãos.

5 CONSIDERAÇÕES FINAIS

Ao final deste estudo, torna-se evidente que a adesão do Brasil à Convenção de Budapeste marca um ponto de inflexão significativo na luta contra o cibercrime no cenário nacional e internacional. Essa conclusão é fruto de uma análise crítica e detalhada dos diversos aspectos envolvidos nesse processo.

Inicialmente, é imprescindível reconhecer que a legislação brasileira já possuía uma base sólida para o tratamento de delitos virtuais, alinhada, em grande medida, aos preceitos estabelecidos pela Convenção de Budapeste. No entanto, o Decreto nº 11.419 de 17 de abril de 2023 não se limita a uma mera formalidade. Ele introduz nuances cruciais, especialmente no que tange à cooperação jurídica internacional. Essa nova dimensão normativa promete superar as barreiras jurisdicionais e operacionais, permitindo um combate mais eficiente e coordenado contra o cibercrime.

É imperativo destacar que a natureza transnacional do cibercrime apresenta desafios singulares. Os criminosos digitais operam frequentemente além das fronteiras nacionais, explorando as lacunas legais e a fragmentação da aplicação da lei. Neste contexto, a Convenção de Budapeste surge como um catalisador para a cooperação internacional. A participação de organizações como a Interpol e a Europol é crucial nesse cenário, fornecendo uma plataforma robusta para troca de informações, investigações conjuntas e a formalização de acordos cooperativos entre nações. Essa abordagem colaborativa é fundamental para enfrentar a complexidade e a agilidade dos cibercriminosos.

A conclusão deste estudo não seria completa sem a proposição de recomendações estratégicas para o Brasil. A adesão à Convenção é um passo positivo, mas deve ser acompanhada por um investimento consistente em capacitação em segurança cibernética. O fortalecimento de parcerias público-privadas também se mostra essencial para uma

resposta eficaz e integrada ao cibercrime. O Brasil, ao abraçar essas estratégias, não apenas salvaguardará seus interesses nacionais, mas também contribuirá de maneira significativa para o esforço global de criar um ciberespaço mais seguro e resiliente.

Em suma, a Convenção de Budapeste representa um marco na legislação e cooperação internacional contra o cibercrime. O Brasil, ao integrar-se a esse tratado, posiciona-se de forma proativa no cenário global, adotando uma postura firme contra as ameaças digitais. Este estudo evidencia que, com as estratégias adequadas e a colaboração contínua entre nações, é possível enfrentar os desafios do cibercrime de maneira eficiente, promovendo um ambiente digital seguro para todos.

REFERÊNCIAS

BITENCOURT, Cezar. **Tratado de Direito Penal**. 10. ed. São Paulo: Saraiva, 2006.

BOITEUX, Luciana. Crimes informáticos: reflexões sobre a política criminal inseridas no contexto internacional atual. São Paulo: Revista dos Tribunais, 2004.

BRASIL. Constituição de 1988. Constituição da República Federativa do Brasil. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 5 out. 1988.

BRASIL. **Convenção sobre Cibercrime**. Budapeste: MPF, 2001.

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 13 abr. 2023.

BRASIL. Decreto-Lei no 2.848, de 7 de Dezembro de 1940. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 20 out. 2023.

BRASIL. Decreto-Lei Nº 3.689, de 3 de Outubro de 1941. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 20 out. 2023.

BRASIL. Lei Complementar Nº 109, de 29 de Maio de 2001. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp109.htm. Acesso em: 20 out. 2023.

BRASIL. **Lei Nº 11.829, de 25 de Novembro de 2008.** Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em: 20 out. 2023.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 3 dez. 2012.

BRASIL. Lei Nº 13.709, de 14 de Agosto de 2018. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 out. 2023.

CASTRO, José Roberto Wanderley. **A tipicidade dos crimes cibernéticos no Direito Penal brasileiro**: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos. 2018. 231 f. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade Federal de Pernambuco, Recife, 2018.

COAF. **O que faz o Coaf?**. Brasília, DF: Coaf, 2020.

COLLI, Maciel. **Cibercrimes**: limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2010.

DUARTE, Ana Luísa Vieira. **Análise do encaixe da convenção de Budapeste no ordenamento jurídico brasileiro**. 2022. 48 f. TCC (Graduação em Direito) – Programa de Graduação em Direito, Universidade de Brasília, Brasília, DF, 2022.

JUNQUEIRA, Gustavo Octaviano Diniz e VANZOLINI, Maria Patrícia. **Manual de direito penal brasileiro**. São Paulo: Saraiva, 2018.

MAGGIO, Vicente de Paula Rodrigues.Novo crime: invasão de dispositivo informático - CP, Art. 154-A. **Jusbrasil**, 2023. Disponível em: https://vicentemaggio.jusbrasil.com.br/. Acesso em: 7 mar. 2023.

MARQUES, Garcia; MARTINS, Lourenço. **Direito da Informática**. 2. ed. Coimbra: Almedina, 2006.

NICOLAI, Thiago; ALVEZ, Guilhrme Serapicos Rodrigues. O aumento silencioso dos cibercrimes. **Migalhas**, [*S.l.*], 2020. Disponível em: https://www.migalhas.com.br/depeso/326593/o-aumento-silencioso-dos-cibercrimes. Acesso em: 29 maio 2023.

NOGUEIRA, José Helano Matos. **Fundamentos de segurança cibernética**. Joinville: Clube de Autores, 2021.

SIMAS, Diana Viveiros de. **O cibercrime**. 2014. 170 f. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito, Universidade Lusófona de Humanidades e Tecnologias, Lisboa, 2014.

VECCHIA, Evandro Dalla. **Perícia digital da investigação à análise forense**. Campinas: Millennium, 2020.