UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
Curso de Graduação em Direito

ANA LUÍSA VIEIRA DUARTE

ANÁLISE DO ENCAIXE DA CONVENÇÃO DE BUDAPESTE NO ORDENAMENTO JURÍDICO BRASILEIRO

BRASÍLIA
2022

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
Curso de Graduação em Direito

ANA LUÍSA VIEIRA DUARTE

ANÁLISE DO ENCAIXE DA CONVENÇÃO DE BUDAPESTE NO ORDENAMENTO JURÍDICO BRASILEIRO

Monografia apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília, campus Darcy Ribeiro, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Professor Doutor Alexandre Veronese

BRASÍLIA
2022

AGRADECIMENTOS

À minha mãe, Síndia, que sempre se esforçou muito para proporcionar aos filhos as melhores oportunidades e por sempre acreditar no meu sonho de entrar na Faculdade de Direito da UnB. Ao meu pai, Mauro, que me ensinou a nunca desistir e batalhar pelos meus objetivos. À Sebastiana, minha segunda mãe, que é meu apoio emocional e está sempre presente para me ajudar.

À minha irmã, Gabriela, que me levou e me buscou na faculdade diversas vezes, que me apoiou quando eu estava enfrentando dificuldades e que sempre acreditou em mim, mesmo quando nem eu acreditava. Ao meu irmão, pela criticas e incentivos que me fizeram chegar até aqui.

Ao meu namorado, Caio, pelo amor, amizade, suporte nos momentos mais desafiadores e por instigar meu interesse na área do Direito Virtual. Aos meus amigos, que me apoiaram e ajudaram a superar os momentos de tristeza.

Ao professor Alexandre Veronese, meu orientador, pela prontidão em me ajudar, pelos seus ricos ensinamentos e pela inspiração.

Aos professores Bruno Calabrich, João Costa Neto e Marcio Iorio por terem aceitado o convite para compor a Banca Examinadora desse trabalho.

Aos professores e professoras que estiveram presentes no meu caminho do Curso de Direito da Universidade de Brasília pelos ensinamentos acadêmicos e de vida. Aos meus colegas de faculdades, por acompanharem e compartilharem essa jornada.

RESUMO

Este trabalho tem o objetivo de analisar a harmonização da Convenção de Budapeste, que tem como matéria o enfrentamento aos crimes cibernéticos, ao ordenamento jurídico brasileiro. Partindo de uma revisão bibliográfica, apresentaram-se definições importantes para a compreensão do tema e seu contexto jurídico-normativo. Após analisar a evolução da legislação brasileira em relação aos cibercrimes, argumentou-se a falta de lei efetivas na investigação e punição dos criminosos digitais. Verificou-se que o processo de adesão do Brasil ao referido tratado não exigiu grandes mudanças em relação às normas sobre criminalização de determinadas condutas no meio digital, mas que precisa evoluir no quesito processual penal e cooperação internacional. Constatou-se que a Convenção de Budapeste se encaixou, em maior parte, bem ao ordenamento jurídico brasileiro, necessitando de alguns ajustes e debates, mas sem nenhum conflito de normas que cause perigo aos direitos já garantidos a população brasileira.

Palavras-chave: Cibercrimes, Convenção de Budapeste, proteção de dados pessoais.

ABSTRACT

This work aims to analyze the fit of the Budapest Convention, which has as its subject the fight against cybercrimes, in the Brazilian legal system. Starting from a bibliographic review, important definitions were present for the understanding of the theme and its legal-normative context. After analyzing the evolution of Brazilian legislations in relation to cybercrimes, the lack of effective laws in the investigation and punishment of digital criminals was argued. It was found that Brazil's accession process to the aforementioned treaty did not require major changes in relation to the norm on criminalizing certain conducts in the digital environment, but that it needs to evolve in terms of criminal procedure and international cooperation. It was found that the Budapest Convention fit, for the most part, well with the Brazilian legal system, requiring some adjustments and debates, but without any conflict of norms that could endanger the rights already guaranteed to the Brazilian population.

Keywords: Cybercrime, Budapest Convention, protection of personal data.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
ART	Artigo
BRICS	Brasil, Rússia, Índia, China e África do Sul
CDR	Coalizão Direitos na Rede
CP	Código Penal
CF	Constituição Federal
CPC	Código de Processo Civil
CPP	Código de Processo Penal
CPF	Cadastro de Pessoas Físicas
EUA	Estados Unidos da América
ECA	Estatuto da Criança e do Adolescente
RGPD	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
ONU	Organização das Nações Unidas
STF	Superior Tribunal Federal
STJ	Superior Tribunal de Justiça

SUMÁRIO

INTRODUÇÃO

A sociedade está em constante evolução. Atualmente uma das transformações mais relevantes ocorre pelo crescimento da tecnologia da informação. A partir disso, destaca-se o surgimento da rede mundial de computadores, a internet, a qual possibilita a interação entre pessoas de vários locais do mundo e por diversos meios.

A rede mundial de computadores surgiu no contexto da Guerra Fria e ao final desse período essa tecnologia foi aproveitada pelas universidades. Pouco tempo depois, tornou-se popular e presente na vida de quase todas as pessoas.

Desde então a internet, que surgiu com fins militares, tomou proporções imensas, presentes no dia-a-dia de grande parte da população mundial. Segundo relatório da União Internacional de Telecomunicação, publicado em 2022, apenas 37% da população não se conectam a Internet.

Todavia, com o aumento de pessoas usando a rede mundial de computadores, há também o aumento de ocorrências de diversas condutas criminosas nesse meio. Um fato que comprova essa relação de causa e efeito e o aumento significativo de crimes cometidos na Internet, no Brasil, durante a pandemia de COVID.

Isso ocorreu devido à necessidade de distanciamento pessoal, em que diversas situações do cotidiano, que antes eram realizadas presencialmente, passaram a ser realizadas online, como trabalhar, ir ao banco, solicitar documentos e interagir com outras pessoas.

Além disso, o programa de Auxílio Emergencial oferecido pelo governo brasileiro foi um alvo comum dos criminosos durante a pandemia, e deixou clara a fragilidade do governo do Brasil em inibir e evitar os crimes virtuais.[1]

Dessa forma, nota-se que a progressão tecnológica transforma positivamente a sociedade, bem como facilita as resoluções de atos do cotidiano, sejam eles complexos ou simples. Mas essa evolução dos meios de comunicação gerou malefícios para a

[1] BRANCO, Dácio Castelo. **Cibercriminosos teriam desviado R$ 1 bilhão do Auxílio Emergencial na pandemia** [Online]. Canaltech. 2022. Disponível em: < https://canaltech.com.br/seguranca/cibercriminosos-teriam-desviado-r-1-bilhao-do-auxilio-emergencial-na-pandemia-212611/ > Acesso em: 27 de junho de 2022.

segurança mundial, ela passou a ser um instrumento para práticas de condutas ilícitas de ordem diversa.

Esses crimes cometidos na rede mundial de computadores normalmente são chamados de "crimes cibernéticos", mas também podem ser referidos como "crimes virtuais", "cibercrimes", "crimes digitais" e "crimes relacionados a computadores".

Os cibercrimes podem ser descritos de deferentes formas. Segundo Peter Grabosky, o termo "crime cibernético" se refere a atividades criminosas no ambiente da Internet e/ou Rede mundial de computadores. Mas também vai ser usado para se referir a ofensas envolvendo computadores autônomos também[2]. Já David S. Wall descreve os crimes virtuais com atividade criminosa ou perigosa que envolve a aquisição e manipulação da informação para um ganho[3].

Esses crimes são diversos e podem incluir crimes não relacionados com meios digitais, mas cometidos no ambiente virtual, como a pedofilia, mas também pode se referir a atos criminosos que dependem dos computadores como um meio para cometer o ato criminoso, por exemplo, as invasões feitas por hackers.

Dessa forma os crimes cibernéticos podem ser divididos em categorias, e uma maneira de fazer isso é diferenciando o que o computador é naquele ato; ele pode ser o instrumento usado para cometer o crime; o alvo do criminoso; ou incidental ao crime.[4]

Outra característica dos crimes digitais é que um único ato pode atacar direitos fundamentais de uma única pessoa ou de múltiplas pessoas ao mesmo tempo. Esse fator causa grande preocupação às autoridades policiais, pois os cibercrimes tem uma grande capacidade de lesionar a sociedade como um todo.

Uma prova do perigo que os crimes cibernéticos representam à sociedade como um todo é o fato de diferentes governos pelo mundo serem frequentemente atacados pelos chamados hackers, pessoas que invadem sistemas computacionais para acessar informações confidenciais ou não autorizadas.

Um exemplo disso são os ataques que ocorreram no governo norte americano, no início de 2021, um país com diversos recursos, seja econômicos, científicos e/ou

---

[2] GRABOSKY, Peter et al. **Keynotes in criminology and criminal justice series: Cybercrime**. Oxford University Press, 2016.

[3] WALL, David. **Cybercrime: The transformation of crime in the information age**. Polity, 2007.

[4] Smith, Russell G., Grabosky, Peter e Urbas, Gregor. **Cyber Criminals on Trial. Cambridge** University Press, Cambridge UK. 2004.

tecnológicos, e ainda assim não conseguem encontram meios eficientes para evitar que informações sigilosas e de grande importância sejam acessadas.[5]

No Brasil se destaca o ataque ocorrido ao Superior Tribunal de Justiça, em novembro de 2020, o qual bloqueou processos e e-mails da corte, afetado diretamente a sociedade brasileira.[6]

Além disso, é importante destacar a facilidade dos cibercriminosos se adaptarem rapidamente, assim como o ambiente ao qual estão inseridos, dificultando muito a identificação dos atos ilícitos dos autores desses atos, e, por conseguinte, na criação de meios, como previsões legais, que os evitem ou punam aqueles que os praticam.

Assim, a dificuldade em identificar os autores dos crimes virtuais faz com que muitas vezes os atos ilícitos permaneçam impunes, o que dá confiança para os criminosos cometerem cada vez mais atos e com mais frequência.

Perante o aumento do número de casos de crimes virtuais e o surgimento de novas modalidades dessas infrações, o Estado passa a ter a responsabilidade de criar legislações e outros meios que acompanhem a grande capacidade de mudança da internet, para assim conseguir exercer o controle punitivo esperado do governo.

O Brasil, apesar de ter muito a melhorar, está evoluindo cada vez mais nas legislações que tratam sobre os crimes virtuais. Até o ano de 2012, o país não tinha nenhuma lei que punisse expressamente os crimes virtuais próprios, aqueles voltados contra os dispositivos e sistemas de informação.

Diante da necessidade de criar normas específicas que regulamentassem os crimes digitais, foram propostos alguns projetos de lei no Congresso Nacional brasileiro, entre eles o projeto de lei nº 2126/11, responsável por instituir o marco civil na internet.

Mas a norma pioneira sobre o assunto foi a Lei Carolina Dickmann, Lei 12.737/2012, que alterou o Código Penal, acrescentando os artigos 154-A e 154-B. Esses dispositivos legais tipificaram os crimes cometidos contra os dispositivos informáticos da vítima.

Após isso, em março de 2014, foi criado o Marco Civil da Internet (Lei ordinária nº 12.765/14). Essa norma visa proteger a privacidade do usuário na internet,

[5] CNN. **Medidas tomadas não são suficientes para impedir hackers russos, diz Casa Branca.** Disponível em: https://www.cnnbrasil.com.br/internacional/2021/04/25/medidas-tomadas-nao-sao-suficientes-para-impedir-hackers-russos-diz-casa-branca

[6] ALVES, Paulo. **Ataque hacker ao STJ: seis coisas que você precisa saber sobre o caso** [Online]. Techtudo. 2020. Disponível em: < https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml

assegurando a inviolabilidade e o sigilo das comunicações, conforme determina o artigo 5º, inciso X da Constituição Federal de 1988.

Em agosto de 2018, foi sancionada a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais, e dispõe sobre o tratamento dos dados pessoais, sobretudo em meios digitais, de pessoas físicas e jurídicas. Essa lei é importante no combate aos cibercrimes, pois ajuda evitar práticas criminosas ao exigir uma melhor maturidade da segurança da informação, o que torna as empresas menos vulneráveis aos criminosos digitais.

Além dessas normas voltadas especificamente aos crimes virtuais próprios, há outras normas que permitem que os cribercrimes impróprios possam ser punidos, isso porque o crime já era tipificado no ordenamento jurídico brasileiro, porém agora praticados no meio virtual.

Inclusive, o Brasil é signatário de alguns tratados internacionais que combatem os crimes virtuais impróprios, como a Convenção sobre os Direitos da Criança e os protocolos sobre a Venda de Crianças, a Prostituição Infantil e a Pornografia Infantil (Nações Unidas, 2000); a Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial (Nações Unidas, 1965); e o Protocolo para prevenir, suprimir, e punir o Trafico de pessoas - especialmente mulheres e crianças, um protocolo da Convenção das Nações Unidas contra o Crime Organizado (Nações Unidas, 2000).

Apesar de toda essa evolução na legislação brasileira, o numero de casos dos crimes virtuais continua crescendo de modo acelerado no Brasil, deixando claro que o país tem que se desenvolver muito, nas normas e nos procedimentos, para garantir a segurança da população nos meios digitais.

Portanto, visando garantir uma maior eficiência da identificação, prevenção e repressão dos delitos virtuais o Brasil aderiu formalmente à Convenção sobre os Crimes Cibernéticos em Budapeste.

Essa Convenção tem dois objetivos principais: o primeiro é listar as condutas criminosas que o país deve prever nas leis nacionais; já o segundo objetivo é estabelecer mecanismos legais e institucionais para cooperação internacional[7].

[7] VERONESE, Alexandre. CALABRICH, Bruno. **Cybercrime in Brazil After the COVID-19 Global Crisis: An Assessment of the Policies Concerning Internacional Cooperation for Investigations and Prosecutions**. 2022.

O Brasil ter aderido a tal Convenção é um avanço considerável no combate ao crime virtual. Considerando que esses crimes ocorrem em mais de um país ao mesmo tempo, é necessário à criação de uma rede de cooperação envolvendo o maior numero de nações possíveis, de modo a auxiliar e acelerar as investigações dos cribercrimes.

Contudo, é importante destacar que o encaixe da Convenção de Budapeste no ordenamento jurídico brasileiro também traz novos e diferentes enfrentamentos ao Brasil. Isso porque essa norma faz exigências que podem pôr direitos, já assegurados pelas leis brasileiras, em risco, tais como a proteção dos dados pessoais no escopo das investigações criminais.

Outros pontos que merecem uma análise cuidadosa nesse encaixe é a possível transposição do texto da Convenção no sistema jurídico brasileiro e a falta de instrumentos processuais nos ordenamentos jurídicos internos dos países e a cooperação internacional.

Assim, diante da crescente ocorrência de crimes cibernéticos no Brasil, principalmente durante a pandemia de COVID, fica clara a necessidade de o país desenvolver mais normas e métodos no combate aos crimes digitais.

Entre as estratégias escolhidas, a adesão à Convenção de Budapeste é a mais atual, e por ainda ser muito recente necessita de uma análise mais cuidadosa.

Por isso, esse trabalho apresenta uma análise sobre as principais legislações nacionais e internacionais sobre os crimes cibernéticos e como elas são afetam a adesão á Convenção de Budapeste. Bem como, busca apresentar as maiores dificuldades encontradas no encaixe dessa norma na legislação do Brasil.

CAPÍTULO 1 - A EVOLUÇÃO DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES VIRTUAIS

A evolução dos meios digitais é muito rápida e dinâmica, e consequentemente os crimes relacionados aos meios virtuais seguem o mesmo padrão. Essa característica dos cibercrimes é fator de grade preocupação das autoridades brasileiras.

Isso porque o sistema legislativo brasileiro tem um processo bem específico, em que se desenvolve em uma dinâmica entre duas Casas do Congresso Nacional: a

Câmara dos Deputados e o Senado Federal. Além disso, deve seguir as regras gerais previstas na Constituição Federal, que estabelecem os tipos de normas existentes e suas características, as iniciativas, as restrições, os quóruns e os prazos de tramitação.

Desse modo, é possível notar que o tempo necessário para se criar uma norma no sistema jurídico brasileiro, normalmente, não acompanha a capacidade de mutabilidade dos crimes virtuais, dificultando a criação de leis específicas e punições satisfatórias aos crimes cibernéticos.

Ademais, o Brasil demorou a legislar sobre esses crimes. Até o ano de 2012 não havia nenhuma lei no país que punisse os crimes cibernéticos voltados contra os dispositivos e sistemas de informação, chamados de crimes cibernéticos próprios. Somente eram punidos os crimes digitais impróprios, por meio de adaptações às normas já existentes no sistema jurídico brasileiro. Entre essa norma, com previsões de crimes virtuais impróprios, destaca-se a Lei 11.829, de 2008 que alterou o Estatuto da Criança e do Adolescente, penalizando a pornografia infantil virtual.

Desse modo, levando em consideração o princípio da legalidade, e suas subdivisões (princípio da reserva legal e principio da anterioridade) fica clara a necessidade de criação de norma válida para combater os crimes digitais. Pois o primeiro desses, princípio da reserva legal, informa que um ato criminoso só pode ser definido por lei, em sentido estrito, isso é, somente o ato legislativo pode determinar se uma conduta é crime ou não. Enquanto o princípio da anterioridade, diz que uma conduta só é considerada crime a partir do momento que a lei entra em vigor.

Devido à necessidade de normas punitivas específicas que protegessem as vítimas de crimes cibercrimes, iniciou-se a tramitação no Congresso Nacional de alguns projetos de leis com o intuito de regulamentar essas condutas, dentre os quais o projeto de lei nº 2126/11, que institui o marco civil na internet; o projeto de lei nº 2.793/11, de autoria do Deputado Paulo Teixeira; e o projeto de lei nº 84/99, de autoria do Deputado Eduardo Azeredo.[8]

[8] PINHEIRO, Patrícia Peck, Direito digital — 5. ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012 — São Paulo : Saraiva, 2013.

1.1 LEI CAROLINA DIECKMANN – LEI 12.737/2012

Em maço de 2012, a atriz Carolina Dieckmann, foi vítima de uma fraude virtual, por meio de um e-mail, e teve seu computador invadido. Nesse momento, diversas fotos íntimas da atriz foram copiadas de seu dispositivo e posteriormente foram usadas como instrumento em ameaças e extorsões.

Devido a esse evento, a atriz passou a ter grande engajamento na busca por punição dos autores desse tipo de conduta e na proteção das vítimas desses crimes. E por essa razão o projeto de lei 2.793/11, que já tramitava no Congresso Nacional ganhou força e foi acelerado, de forma que a Lei 12.737 de 2012 passou a ter o seu nome.

O objetivo dessa Lei foi tipificar os crimes cometidos contra os dispositivos informáticos da vítima. Para isso, a Lei alterou o Código Penal, acrescentando os artigos 154A e 154B, bem como, alterou a redação do crime já existente de Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (Art. 266, do CP) e do crime de Falsificação de documento particular (Art. 298, do CP).

Desse modo, nota-se que as autoridades brasileiras, após perceberem a necessidade de leis específicas sobre os crimes cibernéticos, começaram agir para evitar a ocorrência de tais atos. Porém a aprovação dessa norma foi apenas o primeiro passo no combate dos crimes virtuais, e ainda havia muitas mudanças a serem feitas no ordenamento jurídico brasileiro para evitar a crescente criminalidade digital.

1.2 MARCO CIVIL DA INTERNET – LEI 12.765/14

Apesar do projeto de lei 2.126/11, que criou essa lei, ser anterior a ao projeto de lei 2.793/11, que criou a Lei Carolina Dieckmann, o Marco Regulatório da Internet só foi sancionado dois anos após.

Um dos objetivos dessa norma é garantir a privacidade e a proteção de dados pessoais, apesar de também garantir a disponibilização de dados mediante ordem judicial. Além disso, essa lei é chamada de “Constituição da Internet”, pois ela regula, nacionalmente, o uso da internet. Sobre o assunto, Victor Hugo Pereira Gonçalves: “O

Marco Civil é uma legislação cujo objetivo precípuo é o de regular as relações sociais entre os usuários de internet.”.

O Marco Civil da Internet teve como base o princípio da governança e do uso da Internet. Esse princípio reconheceu que o acesso à internet é imprescindível ao exercício da cidadania. Além disso, ela versa sobre:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. (Brasil, 2014).

A referida norma está estruturada em cinco capítulos, sendo estes: o capítulo I trata das disposições preliminares, o capítulo II dos direitos e garantias dos usuários; o capítulo III da provisão de conexão e de aplicações de internet; o capítulo IV, da atuação do poder público e, por fim, o capítulo V trata das disposições finais (Lei nº 12.965 de 2014).

Entre os diversos objetivos da lei, outo ponto a se destacar é a intenção de proteger a privacidade do usuário na rede mundial de computadores, buscando garantir a inviolabilidade e o sigilo das comunicações, em acordo com a previsão constitucional do artigo 5º, inciso X e XII:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XII – é 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, 1988).

Ainda sim, mesmo com esse avanço significativo, no combate aos crimes cibernéticos, o ordenamento jurídico brasileiro não era eficiente, de modo que a criação de outras normas foi necessária.

De modo que, mesmo o Marco Civil da Internet tendo introduzido ferramentas judiciais do mundo físico, como a obtenção de ordem judicial, essas ferramentas não eram eficientes no mundo virtual, isso porque as velocidades entre os dois mundos não são compatíveis e a internet necessita de meios mais céleres do que a realidade física consegue proporcionar.

1.3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI 13.709/2018

O Marco Civil da Internet foi o primeiro passo na tentativa de proteger os dados dos usuários da rede mundial de computadores. Todavia, essa norma também aumentou a discussão sobre o tema, considerando que ainda havia muitos casos de vazamento de dados e escândalos envolvendo aplicativos e redes sociais.

Como resultado desses debates, em setembro de 2018, a Lei Geral de Proteção de Dados Pessoas entrou em vigor, e seu objetivo foi complementar o Marco Civil da Internet em relação ao tratamento de dados pessoais, detalhando mais e regulando novos direitos e deveres dos sujeitos das relações virtuais.

A LGPD tem como referencial a norma europeia, RGPD (General Data Protection Regulation), que trata dos diretos fundamentais de liberdade, privacidade e do livre desenvolvimento da personalidade da pessoa natural. Ela faz isso estabelecendo normas e procedimentos com o intuito de coletar e armazenar dados de pessoas físicas com maior segurança e transparência, penalizando aqueles que a descumprirem.

Levando em consideração o contexto atual, em que o mundo digital tem grande importância social, tratar sobre proteção de dados pessoais é altamente necessário, haja vista que garantir essa proteção assegura, concomitantemente, a segurança pública. Isso porque o roubo de dados, como o CPF e informações bancárias, bem como as invasões às de rede sociais, como WhatsApp e Instagram, estão em alta. Essas ações por si só já configuram uma conduta criminosa de sequestro de dados no ambiente digitam, mas, além disso, são mecanismos necessários na aplicação de diversos golpes.

De maneira que essa norma é relevante no enfrentamento contra os crimes virtuais, pois as empresas se tornaram responsáveis pela segurança de dados. As companhias passam a ter o dever de prestar contas à Autoridade Nacional de Proteção de Dados (ANPD), e caso deixem vazar algum dado terão que pagar uma multa, bem como ficam com a reputação ruim no meio empresarial, e podem ter seus dados bloqueados.

Assim, essas ações garantem uma dupla proteção dos usuários da Internet, uma vez que agora, além da proteção oferecida pelas autoridades brasileiras, os empresários no Brasil passam a ter o dever de protegê-los.

Todavia, essa lei trouxe outra discussão importante no quesito tratamento de dados pessoas na esfera da segurança pública, das investigações criminais e nas repressões de infrações penais, conforme o previsto no artigo 4º, III, "a" e "d" e o §1º, da LGPD.

> III - realizado para fins exclusivos de:
> a) segurança pública;
> [...]
> d) atividades de investigação e repressão de infrações penais; ou
> [...]
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. (Brasil, 2018)

A demanda em ponderar a necessidade do Estado em proteger os dados pessoais e dar segurança, e ao mesmo tempo assegurar direitos subjetivos, como a liberdade de expressão, a livre manifestação do pensamento e a privacidade foi assunto em uma comissão de jurista, entre eles alguns Ministro do Superior Tribunal de Justiça (STJ) e uma professora de Universidade de Brasília, apresentada como anteprojeto, na concepção da LGPD.

Desse modo, é preciso, para a melhor proteção da população brasileira sem deixar de garantir a aplicação dos direitos fundamentais, que essa norma seja utilizada com cautela e dentro dos limites da proporcionalidade.

Logo, verifica-se que essa norma tem consequências positivas no combate ao cibercrime no Brasil, seja pelas previsões legais que ela traz ao ordenamento jurídico no país, ou pelo debate sobre os limites entre as normas e os direitos fundamentais. Porém, a LGPD penal trata apenas de alguns crimes digitais, e, assim como as demais leis citadas anteriormente, não é suficiente nas investigações e punições dos criminosos virtuais.

1.4 LEGISLAÇÃO INTERNACIONAL

Parte dessa insuficiência das normas brasileiras está relacionada ao crime cibernético, normalmente, ultrapassar as fronteiras nacionais, o que dificulta muito a atuação das autoridades responsáveis.

O fato de a internet ser uma rede mundial de computadores e não possuir fronteiras delimitadas, como há no espaço físico, trouxe benefícios no quesito globalização, porém essa a falta de demarcação traz diversos problemas relacionados às soberanias e aos controles dos usuários. Pois, assim como a tecnologia da informação que tem como característica não se restringir por nenhum limite geográfico ou fronteiras, as condutas criminosas no meio digital também tem esse atributo. Elas podem ser praticadas em um país e ter resultados produzidos em outra nação.

Sem o fator território bem definido, fica difícil a aplicação das leis de forma satisfatória, considerando que uma legislação nacional, normalmente, tem sua aplicação limitada apenas ao território daquele Estado. Solucionar essa dificuldade encontrada no enfretamento aos crimes digitais envolve a criação e aplicação de uma legislação internacional.

Por essa razão é necessário analisar alguns instrumentos jurídicos internacionais a que o Brasil aderiu. Primeiramente, destacam-se algumas normas que não são específicas sobre crimes virtuais, e tratam apenas de crimes cibernéticos impróprios. Isso porque, assim como na legislação nacional, as normas sobre esse assunto são

relativamente recentes e tiveram início com a adaptação e, posteriormente, a modificação de leis internacionais já existentes.

Dentre essas normas já existentes que foram adaptadas ou modificadas, as que mais se destacam são: a Convenção sobre os Direitos da Criança e os protocolos sobre a Venda de Crianças, a Prostituição Infantil e a Pornografia Infantil (Nações Unidas, 2000); a Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial (Nações Unidas, 1965); e o Protocolo para prevenir, suprimir, e punir o Trafico de pessoas - especialmente mulheres e crianças, um protocolo da Convenção das Nações Unidas contra o Crime Organizado (Nações Unidas, 2000).

Outro ato, que apesar de não ser uma norma, é essencial na criação de leis internacionais contra os crimes cibernéticos é a Declaração de e-Thekwini, do BRICS e África, de 2013. Essa Declaração se concentra em outra ferramenta no enfrentamento dos crimes digitais, o de desenvolver uma cooperação internacional, possibilitando a criação de uma estrutura do BRICS para cooperar com as politicas da Internet, incluindo a segurança cibernética.[9]

Dentre os diversos assuntos tratados nesse debate, evidencio a de maior importância no combate aos crimes digitais:

> 34. Reconhecemos o papel crítico positivo que a Internet desempenha na promoção do desenvolvimento econômico, social e cultural globalmente. Acreditamos que é importante contribuir e participar de um ciberespaço pacífico, seguro e aberto e enfatizamos que a segurança no uso de Tecnologias da Informação e Comunicação (TIC) por meio de normas, normas e práticas universalmente aceitas é de suma importância (Centro de informação do BRICS, 2013, tradução do autor).

Por fim, aponto a norma sobre cibercrimes mais recente no ordenamento jurídico brasileiro, a Convenção de Budapeste. Essa norma internacional, considerada um tratado internacional de justiça criminal, foi criada em 2001 na Hungria pelo Conselho da Europa, entrou em vigor em 2004 e atualmente é o único instrumento internacional

[9] VERONESE, Alexandre. CALABRICH, Bruno. **Cybercrime in Brazil After the COVID-19 Global Crisis: An Assessment of the Policies Concerning Internacional Cooperation for Investigations and Prosecutions**. 2022.

vinculante que trata especificamente dos crimes cibernéticos. Apesar de originalmente ter objetivo de harmonizar as normas de direito penal e processual penal sobre os referidos crimes dos Estados-membros do Conselho da Europa, em 2013 passaram a convidar os Estados não membros.

Já são signatários desse tratado 44 Estados-membros do Conselho da Europa e 20 Estados não membros, como Argentina, Canadá, Chile, Colômbia, EUA, Peru e República Dominicana. Ainda que o Brasil tenha sido convidado a aderir tal norma em 2019, somente em 2021, com a publicação do Decreto Legislativo nº 37/2021, o país aderiu formalmente à Convenção de Budapeste.

Essa convenção versa sobre:

a) A criminalização de um conjunto de delitos contra e através de computadores no direito doméstico e a harmonização dos elementos normativos relativos às infrações;
b) Definição dos poderes necessários às autoridades competentes, de acordo com o código de processo penal pátrio, para proteger as provas digitais de qualquer crime, como mandado de busca e apreensão, etc. E ainda, limitar tais poderes, a fim de evitar abuso de poder e proteger os princípios fundamentais dos Estados;
c) Instigar uma cooperação internacional rápida e eficaz, além de uma cooperação das forças policiais e do judiciário. A criminalização de condutas específicas, mas também sobre a definição de procedimentos para investigação e produção de provas referentes aos crimes virtuais.[10]

A convenção está estruturada em 48 artigos, que estão separados em 4 capítulos: Terminologia; Medidas a tomar a nível nacional; Cooperação Internacional; e Disposições finais.

Assim, considerando que o Brasil não é único país a tentar, sem muita efetividade, combater os crimes virtuais, essa norma ajuda os Estados que ainda estão

[10] BORTOT, Jessica Fagundes. **Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional.** VirtuaJus, Belo Horizonte, v. 2, n. 2, p. 338-362, 1º sem. 2017.

legislando sobre o assunto a desenvolverem uma norma nacional que estará em harmonia com outras nações.

Por essa razão, a adesão do Brasil à Convenção de Budapeste foi um evento tão importante na evolução do ordenamento jurídico nacional, em relação aos crimes cibernéticos. A Convenção torna as normas mais fortes e harmoniosas a nível mundial, ajuda a criar uma cooperação internacional mais eficaz na investigação e na instauração de processos penais contra os referidos atos criminosos e em parcerias público-privadas mais estreitas. [11]

Desse modo, até momento, essa é norma internacional mais eficaz sobre os cibercrime e tem o potencial de ajudar muito as autoridades brasileiras a punirem os criminosos digitais. Porém, considerando que ela é uma norma muito nova, no Brasil, ainda não tem como garantir se a norma vai ser efetiva para o país, visto que ela pode afetar alguns dos direitos já garantidos aos brasileiros.

Por essa razão, é necessário fazer uma análise sobre como ela vai se encaixar no ordenamento jurídico brasileiro, quais os problemas que ela pode encontra e como solucioná-los.

CAPÍTULO 2 – O PROCESSO DE ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE

Conforme dito anteriormente, o Comitê de Ministros do Conselho da Europa convidou o Brasil a aderir à Convenção de Budapeste em 2019. Esse processo iniciou-se em junho de 2018, após o Governo brasileiro manifestar interesse em aderir esse tratado internacional.

A iniciativa brasileira em participar de tal instrumento internacional foi fruto do trabalho de uma coordenação interinstitucional, feita especificamente para esse fim,

[11] BORTOT, Jessica Fagundes. **Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional.** VirtuaJus, Belo Horizonte, v. 2, n. 2, p. 338-362, 1º sem. 2017.

entre o Ministério das Relações Exteriores, a Polícia Federal e o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional – ambos do Ministério da Justiça e Segurança Pública -, o Gabinete de Segurança Institucional da Presidência da República, a Agência Brasileira de Inteligência e o Ministério Público Federal[12].

A adesão do Brasil à Convenção de Budapeste não ocorreu logo após o convite formal feito pelo Conselho da Europa. Pelo contrário, demorou alguns anos para isso realmente acontecer. Porém esse foi o primeiro passo para o Estado tomar as providências legais internas necessárias. Além disso, apesar de, formalmente, o Brasil não ser signatário de tal norma, após o convite, já houve a possibilidade do país participar, como observador, das reuniões sobre a Convenção e seus protocolos.

Desse modo, considerado que essa norma internacional tem o objetivo de harmonizar elementos do direito penal, definir matéria processual penal interna, em relação aos crimes virtuais, bem como criar ações fundamentais para a obtenção de provas eletrônica, a Convenção traz recomendação às nações que desejam aderir o tratado. E em relação à verificação sobre as características legais internas necessárias para se juntar ao grupo de países que pertencem ao tratado, é essencial descrever a estrutura da Convenção[13].

As orientações para os países são criar ou adaptar seus ordenamentos jurídicos e implantar um regime de cooperação internacional entre os países signatários. Isso ocorre porque a Convenção sobre os Crimes Cibernéticos tem dois principais pontos que devem estar em acordo com as normas nacionais para que o tratado seja efetivo. O primeiro deles é a lista de condutas criminosas previstas na norma internacional, e que também deve estar presente no ordenamento jurídico brasileiro. Já o segundo é um conjunto de mecanismos legais e institucionais para a cooperação internacional.

Com isso, levado em conta à abrangência de cada medida que deve ser tomada, será feita a análise das características legais internas essenciais para a adesão do Brasil à Convenção de Budapeste de forma mais detalhada.

[12] Ministério das Relações Exteriores e Ministério da Justiça e Segurança Pública. **Processo de adesão à Convenção de Budapeste** [Online]. Brasília. 2019. Disponível em https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica

[13] VERONESE, Alexandre. CALABRICH, Bruno. **Cybercrime in Brazil After the COVID-19 Global Crisis: An Assessment of the Policies Concerning Internacional Cooperation for Investigations and Prosecutions**. 2022.

2.1 PREVISÃO DE CONDUTAS CRIMINOSAS

Uma das características mais complexas dos crimes digitais é falta de territorialidade da Internet, de modo que uma conduta criminosa realizada nesse meio pode gerar efeitos em diversas jurisdições diferentes. Esse fator foi crucial para a percepção da necessidade de harmonização de normas que preveem os crimes virtuais. Muitas vezes, as autoridades responsáveis por investigar os referidos crimes encontram disparidades legislativas entre Estados, que acaba inviabilizando a punição dos autores dos atos ilegais.

Foi por esse motivo que os Estados membros do Conselho da Europa elegeram essa característica como algo indispensável para fazer parte do grupo de países que aderem ao tratado.

Assim, após o convite coube aos legisladores e à sociedade brasileira se organizar para discutir, criar e modificar as leis penais e processuais penais, relacionadas aos cibercrimes, usando como guia a Convenção de Budapeste.

Na estrutura da Convenção sobre Crimes Cibernéticos, o capítulo que trata as condutas criminosas que cada país deve estabelecer como infração penal é o Capítulo II, em sua Seção 1. Nessa parte o tratado define 10 condutas a serem observadas pelos países signatários, distribuídas em cinco títulos, sendo estas:

a) Acesso intencional e ilegal à totalidade ou a parte de um sistema informático;
b) Interceptação intencional e ilegal de dados informáticos;
c) Interferência em dados informáticos, com apagar, danificar, deteriorar, alterar ou eliminar os dados;
d) Interferência em sistemas, por meio de introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados digitais;
e) Uso abusivo de dispositivos digitais, principalmente para cometer atos criminosos;
f) Falsidade informática, com fim de criar dados digitais não autênticos;

g) Fraude informática, por meio de introdução, alteração, eliminação, supressão de dados informáticos ou qualquer outra intervenção no funcionamento de um sistema informático, com a intenção de obter benefício econômico ilegítimo.
h) Infrações relacionadas com pornografia infantil;
i) Infrações relacionadas com a violação do direito autoral e dos direitos conexos;
j) Tentativa e ajuda ou cumplicidade.

A maior parte desses crimes está prevista no ordenamento jurídico brasileiro, fruto de todas as mudanças legislativas ocorridas no Brasil desde 2012. As leis mencionadas do Capítulo I desse trabalho, apesar de isoladamente não terem atingido a eficiência desejada no combate aos crimes digitais, em conjunto são fatores imprescindíveis à adesão do país à Convenção de Budapeste. Foram elas que viabilizaram o cumprimento do requisito de previsão nacional dos crimes virtuais.

Ainda sobre a compatibilidade das normas brasileiras com as previsões do tratado, o Conselho da Europa, em 2020, fez uma tabela mostrando, em resumo, que a legislação brasileira prescreve a maioria dos crimes virtuais exigidos.

Tabela 1: Correlação entre a Convenção de Cibercrimes e a lei penal brasileira.

Prescrições legais sobre a Convenção de Crimes Cibernéticos		**Prescrição penal no direito brasileiro: Código Penal (CP), Lei de Propriedade intelectual de programa de computador (Lei nº 9.609/98), Estatuto da Criança e do Adolescente (ECA), Norma de Interceptação de Comunicações Telefônicas e Informáticas (Lei nº 9.296/96).**	
Artigo 2	**Acesso ilegal.**	Artigo 154-A e 154-B (CP)	É uma invasão de um dispositivo informático (público ou privado).
Artigo 6	**Uso abusivo de dispositivo digital.**		
Artigo 3	**Interceptação ilegal.**	Artigo 10 (Lei nº 9.296/96)	Interceptação sem autorização judicial.
Artigo 4	**Interferências em dados informáticos.**	-	Sem previsão.
Artigo 5	**Interferência em sistemas.**	Artigo 313-B (CP).	Modificação ou alteração ilícita de sistemas de informação.
Artigo 7	**Falsidade**	Artigo 297 (CP)	Falsificação de documentos públicos.

	informática.	Artigo 298 (CP)	Falsificação de documentos particulares.
		Artigo 298, parágrafo único (CP)	Falsificação de cartões de crédito ou débito
		Artigo 313-A (CP)	Inserção de dados falsos em sistemas de informações.
Artigo 8	**Fraude Informática.**	Artigo 171 (CP)	Estelionato.
		Artigo 155 (CP)	Furto por fraude.
Artigo 9	**Infrações relacionadas com pornografia infantil.**	Artigo 240 (ECA)	É a produção ou reprodução de conteúdo explícito envolvendo crianças ou adolescentes.
		Artigo 241 (ECA)	Oferecer, comercializar, publicar ou distribuir conteúdo explícito envolvendo crianças ou adolescentes.
		Artigo 241-A (ECA)	Oferecer, comercializar, publicar ou distribuir conteúdo explícito envolvendo crianças ou adolescentes, usando computadores ou redes.
		Artigo 241-B (ECA)	Comprar, possuir ou armazenar conteúdo explícito envolvendo crianças ou adolescentes.
		Artigo 241-C (ECA)	Simular a participação de crianças ou adolescentes em conteúdos explícitos.
Artigo 10	**Infrações relacionadas com a violação dos direitos autorais e direitos conexos.**	Artigo 184 (CP). Artigo 2 (Lei nº 9.609/98).	É uma violação de direitos autorais e direitos relacionados.
Artigo 11	**Tentativa e ajuda ou cumplicidade.**	Artigo 14 (CP)	A tentativa de produzir conduta criminosa é punível.

Fonte: Elaborada pela autora com base em Veronese e Calabrich, 2022.

Ressalta-se que, apesar da ampla compatibilidade das leis brasileiras com as prescrições legais da Convenção de Budapeste, o Brasil ainda não assinou o protocolo adicional relativo à criminalização dos atos de racismo e xenofobia cometidos por meio de sistemas de informáticos, até o momento (Conselho da Europa, 2022).

Além disso, a convenção sobre os crimes cibernéticos, em sua Seção 2 do Capítulo II, traz prescrições especificas no campo processual penal, tais como:

a) Algumas provisões comuns;
b) Preservação antecipada de dados e de computadores armazenados;
c) Ordem de produção;
d) Busca e apreensão de dados armazenados em computadores;

e) Coleta de dados em tempo real e interceptação de dados.

E assim como no caso das normas penais, o ordenamento jurídico brasileiro tem algumas normas brasileiras que atendem essas determinações processuais. Entre elas, o Concelho da Europa destaca as seguintes:

Tabela 2: Leis processuais penais brasileiras que atendem as determinações da Convenção de Cibercrimes.

Prescrição processual penal no direito brasileiro: Código de Processo Penal (CPP), Marco Civil da Internet (MCI), Lei de Organização Criminosa (Lei nº 12.850/2013), Norma de Interceptação de Comunicações Telefônicas e Informáticas (Lei nº 9.296/96), Resolução 596/2012 da ANATEL.	
Artigo 10 (MCI).	Permite que autoridades policiais e Ministério Público solicitem diretamente aos prestadores de serviços a concessão de acesso aos dados de assinantes dos usuários, isso não inclui endereços IP que necessitam de dependam de ordem judicial.
Artigo 10, §3º (MCI).	Prevê que é necessária uma ordem judicial para que os provedores disponibilizem registros de conexão, bem como conteúdo armazenado de comunicações privadas.
Artigo 240 (CPP)	Fala sobre busca e apreensão tradicionais, mas que também são utilizadas para busca e apreensão de dados informáticos armazenados.
Lei 9.296/1996	Regulamenta a interceptação de comunicação, permitindo a interceptação em sistemas telefônicos e de informática no âmbito de investigações criminais. Essa interceptação está condicionada por ordem judicial e o pedido deve ser justificado por suspeita razoável do crime e pela impossibilidade de obtenção de prova por outros meios.
Artigo 10-A (Lei nº 12.850/2013)	Inclui e regulamenta a possibilidade de infiltração virtual de agentes policias.
Resolução 596/2012 (ANATEL)	Permite que o órgão solicite diretamente às prestadoras de serviços o acesso às informações da conta e aos registros de chamadas dos usuários.

Fonte: Elaborada pela autora com base em *Country Wiki* do Concelho da Europa[14].

Ademais, apesar do Brasil não ter previsões legais específicas sobre provas digitais, a Lei Geral de Proteção de Dados Pessoais, no Art. 7º, II e VI, traz a

[14] https://www.coe.int/en/web/octopus/country-wiki

possibilidade do tratamento de dados na hipótese de exercício de diretos em processo judiciais.

Portanto, levando em consideração que o Brasil já está criando norma sobre criminalizar determinadas condutas no meio digital há anos, após o convite do Conselho da Europa, não houve necessidade de grandes modificações no ordenamento jurídico brasileiro para se adaptar á esse fator. Inclusive, a criação das leis específicas no país, parece já ter usado essa Convenção como guia, mesmo antes do convite, vendo tamanha compatibilidade entre as normas brasileiras e a prescrição do tratado.

2.2 MECANISMOS LEGAIS E INSTITUCIONAIS PARA A COOPERAÇÃO INTERNACIONAL

Conforme dito anteriormente, os crimes virtuais não têm fronteiras, porém as normas e os procedimentos legais têm. E a melhor forma de conseguir que os criminosos do ciberespaço sejam punidos é criando uma rede de ajuda entre Estados, também conhecida como cooperação internacional.

Para iniciar o assunto, é necessário conceituar a cooperação jurídica internacional em matéria penal, e ela nada mais é que o conjunto de medidas e mecanismos pelos quais órgãos competentes dos Estados solicitam e prestam auxílio recíproco para realizar, em seu território, atos pré-processuais ou processuais que interessem à jurisdição estrangeira na esfera criminal[15]. Sendo assim, ela garante o direito de acesso à justiça penal, por meio da colaboração entre Estados.

Considerando essa necessidade, o principal ponto da criação de uma norma internacional que trate de crimes cibercrimes é criar uma estrutura eficaz no combate aos crimes digitais. Para isso os países, e nesse caso quanto mais aderirem melhor, devem uniformizar as normas para poder punir as mesmas condutas, mas, principalmente, precisam criar instrumentos que estreitem a união entre os membros desse acordo.

[15] ABADE, Denise Neves. **Direitos Fundamentais na Cooperação Jurídica Internacional**. São Paulo: Saraiva, 2013, p.27.

Assim, a ideia dessa norma internacional é garantir uma Internet livre, isso é, um local em que a informação pode fluir livremente, mas com a garantia de que se ela for usada de modo indevido a justiça criminal poderá atuar de forma eficaz. Para alcançar isso devem ser feitas algumas restrições ao uso da rede mundial de computadores, mas de forma limitada, pois apenas os crimes especificados nessa norma são investigados e processados, e os dados essenciais como provas em processos criminais são protegidos pelos direitos humanos e pelo estado de direito.

Por essa razão a Convenção de Budapeste tem uma parte só para tratar sobre os princípios gerais relativos ao auxílio mútuo entre as nações, em matéria de investigações relacionadas às infrações penais virtuais. Esse assunto está previsto, especificamente, no Título 3 do Capítulo III do referido tratado. Além disso, o Preâmbulo da Convenção mostra a necessidade de acreditar que a cooperação jurídica internacional em matéria penal é um meio rápido e eficaz para uma luta efetiva contra a cibercriminalidade.

No caso das previsões da Convenção de Budapeste, há duas situações sobre assistência mútua entre os países. Uma que está relacionada à inexistência de tratados ou legislações específica recíproca entre as nações que garantam a cooperação internacional em matéria de investigação penal, e nesse caso devem ser usadas as disposições dessa norma internacional. Já a outra, está relacionada aos casos em que já existem previsões legais que possibilita a investigação entre os Estados, e nesse caso caberá à Convenção se aplicada igualmente a tais acordos.

E é nessa característica legal interna necessária para se juntar ao grupo de países que pertencem ao tratado, que o Brasil está com déficit e precisa evoluir mais. Pois o país tem poucas normas que garantem a cooperação internacional desejada pelo Conselho da Europa.

O ordenamento jurídico brasileiro atém tem uma norma que fala sobre o assunto, o artigo 26 do Código de Processo Civil, que trata da cooperação jurídica internacional no país. Todavia essa norma ainda não é a melhor previsão legal no combate aos crimes cibernéticos, pois se processos criminais, por si só, já necessitam de normas mais específicas, os que investigam atos ocorridos no espaço digital precisam ser ainda mais especiais.

Dessa forma fica claro que legislativamente o Brasil estava atrasado no quesito cooperação jurídico internacional para combate aos crimes virtuais, considerando a falta de lei nacional e internacional específicas na investigação e punição desses crimes. Porém, a adesão do país à Convenção de Budapeste é o fator que deve mudar drasticamente essa circunstância.

Isso porque, agora, o Brasil passa a ter sua primeira norma sobre cooperação jurídica internacional no âmbito penal, não havendo outro tratado internacional que trate da captação de provas com tamanha eficiência por parte dos Estados, autoridades judiciais e policiais. E mais do que isso, trata especificamente dos dados informáticos pertinentes a investigações de delitos praticados no ciberespaço.

Entre os procedimentos de cooperação internacional presentes na Convenção sobre crimes cibernéticos destacam-se como os mais importantes as medidas específicas de auxílio mútuo e a Rede 24/7, que consiste na designação de um ponto de contato disponível 24 horas por dia, 07 dias por semana, por cada Estado signatário do tratado, para garantir a prestação de assistência imediata a investigações ou procedimentos relativos a infrações penais no meio digital, ou a fim de recolher provas eletrônicas.

Sendo assim, mesmo que no Brasil ainda não há uma verdadeira lei de regência para a assistência jurídica mútua em matéria penal (ARAS, 2019, p. 423)[16], a adesão do país a referida Convenção tem muito a contribuir para o progresso no enfrentamento aos crimes virtuais, especialmente estabelecimento dos procedimentos de auxílio mútuo e a Rede 24/7.

Mas só porque o país aderiu a esse tratado, não significa que ele tenha alcançado o seu objetivo final. Na verdade ele deve buscar sempre mais ferramenta de cooperação internacional, pois quanto mais conexões de ajuda entre Estados ele participar, mas fácil será punir os criminosos do ciberespaço. Participar dessa Convenção é apenas o passo inicial para criação de uma grande rede de ajuda entre nações.

[16] ARAS, Vladimir. Direito Probatório e Cooperação Jurídica Internacional. In SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.) **A Prova no Enfrentamento à Macrocriminalidade**. Salvador: JusPodivm, 2019, p.423.

Na busca em aumentar a criação de laços de auxílio mútuo entre as nações é preciso dar preferência aos tratados internacionais multilaterais, como a Convenção de Budapeste, pois é mais fácil centralizar os veículos em uma única norma, do que ter várias normas diferentes. Os países devem mudar seu paradigma de cooperação internacional de tratados bilaterais para multilaterais, proporcionando a efetiva criação de uma rede de cooperação (Veronese e Calabrich, 2022)[17].

No caso brasileiro destaca-se outro possível ponto de cooperação internacional multilateral, o BRICS. Considerando a Declaração de e-Thekwini, do BRICS e África, que não é uma norma, mas tem potencial de ser um anúncio do desenvolvimento de uma cooperação internacional entre os países desse bloco econômico, bem como pode possibilitar a criação de uma estrutura específica para esse auxílio.

Desse modo, levando em conta que a cooperação internacional faz com que o controle dos cibercrimes funcione com maior efetividade, fica clara a colocação desse fator como algo necessário para que o país participe da Convenção sobre crimes virtuais. E apesar de o Brasil, antes de adesão a essa norma, estar bem atrasado no quesito cooperação jurídica internacional, em processos criminais, principalmente nos relacionados aos meios digitais, após se tornar signatário da Convenção de Budapeste ele demonstrou estar disposto a evoluir sua legislação e seus procedimentos.

CAPÍTULO 3 – OS POSSÍVEIS PROBLEMAS NA ADESÃO DO BRASIL À CONVENÇÃO DE BUDAPESTE

Tendo em consideração as dificuldades que o Brasil vinha enfrentando no combate aos crimes cibernéticos, principalmente durante a pandemia do COVID-19, ficou clara a necessidade que o país precisava criar meio legais mais efetivos nesse enfrentamento. E a Convenção de Budapeste foi a melhor opção legal, no momento, para identificar e punir os cibercriminosos, de modo que o país precisou se organizar rapidamente para fazer parte dos países signatários desse tratado.

[17] VERONESE, Alexandre. CALABRICH, Bruno. **Cybercrime in Brazil After the COVID-19 Global Crisis: An Assessment of the Policies Concerning Internacional Cooperation for Investigations and Prosecutions**. 2022.

Porém, apesar da adesão ter sido considerada por muita gente, inclusive por autoridades governamentais, uma vitória para o ordenamento jurídico brasileiro e na luta contra os crimes virtuais, o processo gerou grandes preocupações por outra parte da sociedade brasileira, em relação a temas como: a) o processo ter sido acelerado e com caráter pouco participativo, b) a adesão total e irrestrita a Convenção de Budapeste e c) a ausência de uma lei geral de proteção de dados pessoais dedicada às atividades de persecução penal e segurança pública.

Desse modo faz-se necessário analisar cada uma dessas preocupações separadamente, e verificar se processo adesão ao tratado, tal como ocorreu, trouxe malefícios ao ordenamento jurídico brasileiro, ou se esses possíveis problemas podem ser superados de outra maneira.

3.1 PROCESSO ACELERADO E DEBATES RESTRITOS

O processo de adesão brasileira a esse tratado foi considerado acelerado por alguns acadêmicos e ativistas dos direitos humanos na área digital, principalmente os que participam da Coalizão Direitos na Rede, o que gerou algumas preocupações com os riscos e impactos que uma adesão apressada pode causar ao ordenamento jurídico nacional. A CDR é uma rede de entidades que reúne mais de 50 organizações acadêmicas e da sociedade civil em defesa dos direitos digitais, principalmente temas como a defesa do acesso à internet, da liberdade de expressão, da privacidade e da proteção de dados pessoais na Internet[18].

Segundo essa parcela da população, o processo teve um caráter pouco participativo e aberto a debates, e levando em conta que o Brasil ser um Estado signatário da Convenção sobre crimes cibernéticos gera enormes repercussões sobre o sistema nacional de proteção aos direitos digitais, seria necessária uma tramitação que mobilizasse um debate amplo, aberto e democrático.

[18] Coalisão Direitos na Rede. **Carta aos Membros do Senado Federal sobre a Convenção de Budapeste** [Online]. Brasília. 2021. Disponível em: https://direitosnarede.org.br/2021/10/21/carta-aos-membros-do-senado-federal-sobre-a-convencao-de-budapeste/.

Realmente o processo para o Brasil se tornar signatário à Convenção, que durou menos de um ano, ocorreu de forma acelerada e por consequência com poucas audiências públicas para tratar especificamente sobre essa adesão. Porém o fato de não ter havido discussões específicas para esse ato, não quer dizer que a sociedade brasileira não tenha debatido o assunto e outros momentos.

Conforme demostrado nos capítulos anteriores, o Brasil já discute o tema e as legislações necessárias à repressão dos crimes cibernéticos fazem anos, no momento das criações das leis nacionais sobre crimes virtuais, como a Lei 12.737/2012, Marco Civil da Internet e LGPD. Esses debates, apesar de anteriores ao processo de adesão à Convenção, discutiram exatamente as condutas previstas nessa norma internacional, vista a grande equivalência entre as normas nacionais e as previsões do tratado.

Além disso, as leis brasileiras têm tanta equivalência e similaridade com as condutas criminosas que estão previstas no referido tratado que demonstra como o país, desde 2012, vem criando suas normas dentro dos padrões internacionais criados pela Convenção sobre os cibercrimes. É possível, inclusive, que tenham usado tal norma internacional como um guia na criação das leis sobre combate aos crimes virtuais.

Entretanto, mesmo que o Brasil já tenha aderido à norma, o assunto ainda pode e deve ser debatido de outras maneiras, isso é, ainda há a necessidade de realizar debates futuros sobre a adequação do ordenamento jurídico brasileiro à Convenção. Essa discussão posterior, considerando que o país precisava de meios mais efetivos no combate aos crimes cibernéticos, foi a melhor solução para encontrar o equilíbrio entre a demanda das autoridades nacionais, principalmente o Ministério Público, e um processo amplo, aberto e democrático.

Desse modo, como, em primeiro momento, não se observou inovações legislativas na norma internacional que possam colocar os direitos dos brasileiros em risco, ter havido debates amplos em outros momentos legislativos, bem como existir e a possibilidade de se realizar uma discussão sobre a adequação das normas nacionais à referida norma internacional, não há que se falar de falta de debates amplos, abertos e democráticos no processo de adesão do Brasil à Convenção sobre crimes cibernéticos, desde seja realmente realizado as conversa posterior à adesão.

3.2 A ADESÃO TOTAL E IRRESTRITA A CONVENÇÃO DE BUDAPESTE

Além disso, o CDR também questionou o caráter total e irrestrito da adesão brasileira a essa norma internacional. Dada a enorme variedade de sistemas jurídicos presentes no tratado e a soberania dos Estados para legislar em suas respectivas jurisdições, algumas adaptações podem ser necessárias para compatibilizar o ordenamento jurídico brasileiro com a norma internacional.[19]

A adesão total e irrestrita pode gerar conflitos entre as disposições da Convenção e outras previsões vigentes no direito brasileiro, segundo a CDR. Porém, essa preocupação não é um assunto novo, pois a própria Convenção de Budapeste expressa preocupações com o alinhamento entre se conteúdo e normas internas dos signatários e com instrumentos internacionais de direitos humanos. Sobre o assunto o artigo 15 da Convenção de Budapeste prevê:

> 1. Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos revistos na presente Seção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma proteção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Proteção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do pacto Internacional das Nações Unidas sobre os Direitos Civis e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade. (Convenção Sobre o Cibercrime, 2001, tradução da autora).

Além disso, esse tratado também trouxe disposições que preveem mecanismos que facilitam a uma adesão que respeite as leis nacionais de todos os signatários. Elas são instrumentos para o exercício da soberania de cada país que integra a Convenção. São ela as chamadas declarações, do Art. 40, e as reservas, do Art. 42, que dispõem o seguinte:

[19] Coalisão Direitos na Rede. **Carta aos Membros do Senado Federal sobre a Convenção de Budapeste** [Online]. Brasília. 2021. Disponível em: https://direitosnarede.org.br/2021/10/21/carta-aos-membros-do-senado-federal-sobre-a-convencao-de-budapeste/.

> Artigo 40º - Declarações
> Qualquer Estado pode, mediante notificação por escrito dirigida ao Secretário Geral do Conselho da Europa no ato da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declarar que fará uso da faculdade de exigir, se for o caso disso, um ou mais elementos suplementares, tal como previsto nos artigos 2º, 3º, 6º, n.º1, *alínea b)*, 7º, 9º, n.º 3 e 27º, n.º 9, *alínea e).*
> (...)
> Artigo 42º - Reservas
> Qualquer Estado pode, mediante notificação por escrito dirigida ao Secretário Geral do Conselho da Europa no ato da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, declara a sua intenção de fazer uso da(s) reserva(s) previstas nos artigos 4º, n.º 2, 6º, n.º 3, 9º, n.º 4, 10º, n.º 3, 11º, n.º3, 22º, n.º 4, e 41, n.º1. Nenhuma outra reserva poderá ser formulada.
> (Convenção Sobre o Cibercrime, 2001, tradução da autora).

Apesar do Brasil não fazer uso desses dispositivos não quer dizer que o país tenha aceitado o tratado de forma total, pois o Brasil não é signatário do protocolo adicional que tem como objetivo a harmonização entre legislações relevantes na matéria do direito criminal relativa à criminalização do racismo e da xenofobia na internet. Desse modo, se pode dizer que foi uma adesão total e irrestrita.

Além do mais, no processo de adesão e após ele, não se notou nenhum tipo de conflito significante entre as disposições da Convenção de Budapeste e a legislação brasileira e outro instrumento internacional de direitos humanos: apenas há dispositivos da Convenção que não encontram, ainda, correspondentes na legislação nacional.

Desse modo, até o momento esse possível problema não foi constatado como uma dificuldade que tenha realmente trazido prejuízos ao sistema jurídico brasileiro. Pelo contrário, a Convenção tem o potencial em ajudar a legislação nacional a evoluir, garantindo uma maior punibilidade dos cibercriminosos.

3.3 A PROTEÇÃO DE DADOS PESSOAIS NO ESCOPO DAS INVESTIGAÇÕES CRIMINAIS

A proteção de dados pessoais no Brasil teve uma grande evolução após a Lei Geral de Proteção de Dados Pessoais, no final de 2020, bem como com a criação Autoridade Nacional de Proteção de Dados, entidade autárquica. Já em relação ao

tratamento de dados na esfera de persecução penal e de segurança pública, foi o anteprojeto de LGPD Penal que ampliou a discussão no país.

O referido anteprojeto foi apresentado pela comissão de juristas presidida pelo ministro aposentado do STJ, Nefi Cordeiro, e tem o objetivo de regulamentar as exceções colocadas pelo artigo 4º da LGPD, que retirou atividades de segurança pública, investigações penais e persecução criminal do escopo de aplicação da LGPD. Essa proposta é de grande importância para a compatibilização fundamental entre a necessidade de o Estado acessar dados pessoais para atividades de segurança pública e a importância de se salvaguardar direitos dos cidadãos e oferecer remédios a eventuais abusos cometidos por autoridades.

Recentemente o anteprojeto deu origem ao Projeto de Lei 1515/22, do Deputado Armando (PL-SC), que está baseado em três pilares: proteção dos direitos fundamentais de segurança, liberdade e de privacidade; eficiência da atuação dos órgãos responsáveis; e intercâmbio de dados pessoais entre autoridades competentes. (Agência Câmara de Notícias). Esse Projeto de Lei é imprescindível, visto a necessidade de debater a conformidade do tratamento dos dados nessa área, principalmente após a adesão brasileira à Convenção sobre crimes cibernéticos, uma vez que o processamento transnacional de dados cria conflitos em relação aos princípios da territorialidade e da soberania.

O fato de uma autoridade responsável por uma investigação penal de um país ter acesso a provas em servidores ou dispositivos digitais, que podem estar em outros Estados ou em nuvens, isso é, fora de um território físico, cooperação jurídica internacional em matéria penal se tornou uma das maiores preocupações.

Foi exatamente diante dessa preocupação que o Conselho da Europa iniciou a criação da Convenção de Budapeste, documento que regulamenta a questão e prevê o acesso transfontreiço aos dados quando estiverem publicamente acessíveis ou quando houver o consentimento legal e voluntário da pessoa legalmente autorizada a divulga-los.

O problema é que a pessoa legalmente autorizada a divulgar os dados vai mudar a depender de fatores como a circunstância, a pessoa e a lei aplicada naquele caso, de modo que pode haver dúvida sobre a harmonia da norma internacional com a proteção de dados nacionais.

A respeito desse o problema, o Art. 7º, II e VI, da LGPD, dizem sobre a possibilidade do tratamento de dados na hipótese de exercício de diretos em processo judiciais. Essa norma poderia ser usada por analogia nos casos necessários se a LGPD não excluísse a proteção de dados pessoais em matéria penal, de maneira que usá-la nesse caso apenas causaria mais um problema, a insegurança jurídica. Por essa razão, a aprovação do Projeto de Lei 1515/22 é melhor opção de legislação específica, até o momento, para o Brasil resolver esse impasse.

Já em relação à norma internacional, segundo a Convenção de Budapeste, qualquer Estado signatário, ao fornecer dados ou informações, voluntariamente, por meio do intercâmbio espontâneo de informações previsto no Art. 26, nessa norma internacional, ou em atendimento a um pedido de auxílio mútuo, pode determinar limites ou restrições à utilização desses dados e informações.

Vale ressaltar que a Convenção de Budapeste diverge de outros tratados internacionais que tratam de auxílio mútuo, uma vez que, os normalmente tratados e convenções internacionais usam a regra da especialidade. Essa regra proíbe utilize os documentos e informações fornecidos para outros fins que não a punição das infrações pelas quais o país requerido concedeu sua cooperação.

De forma, segundo o princípio da especialidade, uma vez fornecida às informações ou elementos de prova ao país requerente, fica ele automaticamente vinculado à observância da regra, não sendo necessária a expressa manifestação dele sobre o assunto. Porém, no caso da Convenção sobre crimes cibernéticos, o Estado que fornece os dados deve solicitar a aplicação desse princípio, caso deseje.

Mesmos com essas considerações, alguns doutrinadores acreditam que permanecem alguns perigos em relação às liberdades individuais na esfera de acesso aos dados hospedados em Estados estrangeiros que não estão contemplados pelas normas que regulam os princípios e garantias dos acusados e, em alguns casos, terceiros, bem como os proprietários dos servidores onde esses dados então armazenados.

Sobre o assunto, a Organização das Nações Unidas e a Corte Internacional de Direitos Humanos, em 2015, falaram sobre os riscos oferecidos pela coleta massiva de dados pessoais para a livre circulação de ideias na Internet. Segundo eles, a vigilância

desproporcional afeta o direito à privacidade e liberdade de expressão de grupos vulneráveis.

Porém, a simples adesão do país à Convenção sobre crimes cibernéticos não significa que está autorizado ao governo vigiar as ações população realizadas em meios digitais e acessar dados pessoais e usar nas persecuções penais, sem qualquer limite ou formalidade legal. Desse modo, a adesão à Convenção sobre crimes cibernéticos não impõe aos países signatários a obrigação de decretar um poder legal para a autoridade policial invadir remotamente os sistemas de computação (Hildebrant, 2020).

Inclusive, a Emenda Constitucional 115, promulgada em 10 de fevereiro de 2022, que acrescentou previsões à Constituição Federal sobre o direito fundamental à proteção de dados pessoais, que a partir disso passou a fazer parte do rol de direitos e garantias fundamentais com previsão constitucional. Essa Emenda também determinou a competência privativa da União para legislar sobre o tema, organizar e fiscalizar a proteção e o tratamento dos dados pessoais. Assim, essa ação reforça a impossibilidade das autoridades brasileiras usar os dados pessoais, principalmente em ações penais, de modo ilimitado e fora da formalidade legal.

Outro fator que causa dúvidas em relação ao Brasil se tornar signatário dessa norma internacional é o fato do Brasil não ter uma entidade autônoma e independente para auxiliar na implantação da Convenção e realizar uma fiscalização dos agentes de tratamentos de dados, também traz preocupações em relação à proteção de direitos fundamentais e o acesso transnacional aos dados. Diferente de outros Estados signatários, como África do Sul, Canadá, EUA, Japão e países europeus.

Contudo, o Brasil não está totalmente despreparado nesse quesito, ele tem a ANPD, que após a publicação da Medida Provisória 1.124, se tornou um órgão autárquico de natureza especial, isso é, não subordinada hierarquicamente a ministérios ou à Presidência. Essa autarquia é responsável por fiscalizar e divulgar como as informações e dados pessoais que circulam nos meios digitais são utilizados e tratados, bem como, aplicar as leis referentes à proteção de dados no país.

A ANPD é um órgão independente, composta por um Conselho Diretor de cinco pessoas indicadas pelo Poder Executivo e aprovado pelo Senado e por outros servidores. Entre essas pessoas indicadas têm pessoas da sociedade civil, de instituições científicas,

do setor produtivo, do Senado, da Câmara dos Deputados, do Ministério Público e por empresários. E assim, como um órgão autônomo, tem a responsabilidade de garantir o cumprimento da legislação e punir aqueles que não observem o devido tratamento dos dados.

Assim, apesar de ainda necessitar de algumas evoluções no quesito proteção de dados pessoais, principalmente em matéria penal, o ordenamento jurídico brasileiro tonou, por meio da Emenda Constitucional 115/22, a proteção de dados pessoais um direto fundamental, fator o que garante que as normas do tratado sejam aplicadas respeitando o direitos fundamentais dos brasileiros. Além disso, se o Brasil fizer as exigências necessárias em caso de auxílio mútuo, não haverá nenhum problema de encaixe entre a Convenção de Budapeste e o ordenamento jurídico nacional.

CONCLUSÃO

O principal objetivo do presente trabalho foi analisar como a Convenção de Budapeste se encaixou no ordenamento jurídico brasileiro e quais problemas o país poderia encontra ao final do processo de adesão ao tratado. Para isso foi necessário, primeiramente, fazer uma pesquisa em relação à evolução das normas e procedimentos brasileiros, relativos à investigação e punição dos crimes cibernéticos, até o momento atual.

A importância do combate aos crimes digitais se tornou ainda mais necessária após o Brasil enfrentar diversas dificuldades no combate aos referidos crimes, e que essas complicações se tornaram ainda pior no período da pandemia de COVID-19, momento em que se estima que ouve um aumento de mais de 200% dos crimes praticados no ambiente virtual[20]. Isso porque durante esse momento as pessoas precisaram se distanciar fisicamente uma das outras e a atividades do cotidiano, que antes eram realizadas presencialmente, tiveram que ocorrer por meios virtuais.

[20] Valor, Globo. **Crimes digitais crescem pós-pandemia e provocam corrida por ciberseguros.** Disponível em: https://valor.globo.com/patrocinado/dino/noticia/2022/06/27/crimes-digitais-crescem-pos-pandemia-e-provocam-corrida-por-ciberseguros.ghtml.

Apesar de essas condutas criminosas terem a característica de conseguir ferir os direitos fundamentais de diversas pessoas, e em alguns casos atacar um Estado, em um só ato, fator esse que por si só já causa grande preocupação as autoridades nacionais, não é o aspecto que mais traz problema na repressão dos cibercrimes, mas sim a aptidão desses crimes se adaptarem tão rápido quanto a tecnologia atual e falta de territorialidade nos meios digitais.

O caráter de rápida mutabilidade traz a necessidade de o legislador pensar em normas mais amplas, que consigam acompanhar as mudanças nas praticas criminosas sem ter que iniciar um novo processo de criação de lei, visto que o sistema de criação de normas no Brasil é bem específico, e em alguns casos demorado.

Por problemas como esses o país demorou anos a iniciar as produções de leis que tratavam de atos ilegais praticados no ambiente virtual, sendo apenas em 2012 a primeira norma específica sobre crimes cibernética própria promulgada. Essa lei, chamada de Lei Carolina Dickmann, alterou o Código Penal, acrescentando dispositivos legais que tipificaram os crimes cometidos contra os dispositivos informático da vítima, previstos nos artigos 154-A e 154-B.

Após isso o país criou mais duas normas de grande importância para o assunto de crimes digitais. Em 2014, foi criado o Marco Civil da Internet, norma que tem o objetivo de proteger a privacidade do usuário na internet assegurando a inviolabilidade e o sigilo das comunicações. E por fim, a Lei Geral de Proteção de Dados Pessoais, sancionada em 2018, dispondo sobre o tratamento de dados pessoas, principalmente em meios digitais.

Apesar do grande avanço do Brasil em relação à sua legislação, em matéria de crimes digitais as normas brasileiras ainda não foram suficientes para, efetivamente, combaterem as referidas condutas criminosas. E a principal razão para elas não serem suficientes é a característica de falta de territorialidade dos meios digitais.

Considerando que uma conduta criminosa realizada no meio virtual pode gerar efeitos em diversas jurisdições diferentes, é necessário que os países unam-se para criar uma rede de apoio no enfrentamento dos crimes cibernéticos. E a forma mais adequada de fazer isso é por norma internacional que harmonize as normas que preveem os crimes

virtuais e crie meios e procedimentos de cooperação entre os Estados nas investigações criminais.

E é exatamente esse o objetivo da Convenção de Budapeste, que apesar de não ser a única norma internacional sobre o assunto, é a norma mais específica, completa e com mais países signatários. Logo, é a com maior capacidade de ser um instrumento legal eficaz nas investigações e repressões dos cibercrimes.

Diante de tal fato, o Brasil, que vem enfrentando problemas relativos à segurança digital, aderiu a Convenção sobre crimes cibernéticos no final de 2021. O processo de adesão a tal norma tem necessita da observância de algumas recomendações, sendo elas a) a equivalência entre as condutas criminosas previstas na norma internacional, e a leis nacionais; b) a criação de um conjunto de mecanismos legais e institucionais para a cooperação internacional.

Quanto à equivalência entre as condutas criminosas previstas na Convenção de Budapeste e as leis prescritas no ordenamento jurídico brasileiro, o país não precisou empreender grandes esforços, visto que a maior parte dos crimes é previsto pelas leis brasileiras, fruto de todas as mudanças legislativas ocorridas no Brasil desde 2012.

No caso das leis processuais penais e nos mecanismos e institucionais para a cooperação internacional, o Brasil tem algumas previsões, mas não tão amplas quanto às normas de direito penal, de modo que ainda precisa realizar algumas evoluções. Além disso, a adesão do país à Convenção de Budapeste já se caracteriza como um progresso nessas áreas, pois a partir de agora passa ter uma norma que trate sobre esses pontos.

Por essas razões, a adesão do Brasil à Convenção sobre crimes cibernéticos, a muito tempo esperada por muitas autoridades brasileiras, foi considerada uma vitória em matéria penal para o país para diversos brasileiros. Mas esse evento também foi visto com muita desconfiança por outras pessoas, devido a fatores como: a rapidez com que ocorreu o processo de adesão, o caráter pouco participativo dele, a adesão total e irrestrita a Convenção e a ausência de uma lei geral de proteção de dados pessoais dedicada às atividades de persecução penal e segurança pública.

Contudo, o trabalho mostrou que essas preocupações foram infundadas ou facilmente superadas. O Brasil se tornar signatário de tal norma internacional traz mais benefícios do que malefícios, e não havia motivo para atrasar esse evento. Até porque o

país já vinha realizando todas as ações necessárias há anos, tempo esse que foi mais do suficiente para o amadurecimento do tema.

Assim, as preparações legislativas, que encontram grande similaridade com as normas previstas na Convenção de Budapeste, foram fator essencial não só no processo de adesão exigido pelo Conselho da Europa, mas também para solidificar os debates sobre os crimes cibernéticos no Brasil.

Desse modo, a Convenção de Budapeste se encaixou, em maior parte, bem ao ordenamento jurídico brasileiro, necessitando ainda a criação ou adesão a outras normas nacionais ou internacionais referentes ao processo de persecução penal e a cooperação internacional. Mas não há nenhum conflito entre as previsões do tratado as normas do Brasil, que causem perigo aos direitos já garantidos a população brasileira, visto que a Constituição Federal, após a promulgação da Emenda 115/22, garante que a proteção de dados pessoais é um direto fundamental.

REFERÊNCIAS

- ABADE, Denise Neves. **Direitos Fundamentais na Cooperação Jurídica Internacional**. São Paulo: Saraiva, 2013.
- ARAS, Vladimir. Direito Probatório e Cooperação Jurídica Internacional. In SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro de (Org.) **A Prova no Enfrentamento à Macrocriminalidade**. Salvador: JusPodivm, 2019.
- ALVES, Paulo. **Ataque hacker ao STJ: seis coisas que você precisa saber sobre o caso** [Online]. Techtudo. 2020. Disponível em: < https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml > Acesso em 15 de junho de 2020.
- BARRETO, Alessandro Gonçalves. **Investigação Digital em fontes abertas**. Rio de Janeiro. Brasport, 2017.
- BORTOT, Jessica Fagundes. **Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional.** VirtuaJus, Belo Horizonte, v. 2, n. 2, p. 338-362, 1º sem. 2017.
- BRANCO, Dácio Castelo. **Cibercriminosos teriam desviado R$ 1 bilhão do Auxílio Emergencial na pandemia** [Online]. Canaltech. 2022. Disponível em: < https://canaltech.com.br/seguranca/cibercriminosos-teriam-desviado-r-1-bilhao-do-auxilio-emergencial-na-pandemia-212611/ > Acesso em: 27 de junho de 2022.
- BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.
- BRASIL. Decreto-lei nº 2.848, de 07 de dezembro de 1940 (**Código Penal**). Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 14 de agosto de 2022.
- BRASIL. **Lei Geral de Proteção de Dados Pessoais** (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >Acesso em: 18 de agosto de 2022.

- BRASIL. Marco Civil da Internet. Lei 12.964/14. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >.Acesso em 18 de agosto de 2022.
- BRASIL. Medida Provisória nº 1.124, de 13 de junho de 2022. Disponível em: < https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Mpv/mpv1124.htm#:~:text=MEDIDA%20PROVIS%C3%93RIA%20N%C2%BA%201.124%2C%20DE%2013%20DE%20JUNHO%20DE%202022&text=Altera%20a%20Lei%20n%C2%BA%2013.709,e%20transforma%20cargos%20em%20comiss%C3%A3o > Acesso em 03 de setembro de 2022.
- BRASIL . Lei nº 3.689, de 03 de outubro de 1941 (**Codigo de Processo Penal Brasileiro**). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm >. Acesso em: 14 de agosto de 2022.
- BRASIL. Lei no 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm#art266 >. Acesso em: 20 de agosto de 2022.
- BRASIL, Emanuelle. **Projeto altera Lei de Proteção de Dados para resguardar segurança pública e defesa nacional** [Online]. Brasília: Câmara dos Deputados. 2022. Disponível em: < https://www.camara.leg.br/noticias/893704-projeto-altera-lei-de-protecao-de-dados-para-resguardar-seguranca-publica-e-defesa-nacional/ > Acesso em 03 de setembro de 2022.
- BRICS. Centro de informação. ***BRICS and Africa: Partnership for development, integration, and industrialization – eThekwini Declaration* – 27 de Março de 2013**. Universidade de Toronto [Online]. Disponível em: < http://www.brics.utoronto.ca/docs/130327-statement.html > Acesso em 10 de agosto de 2022.
- CASSANTI, Moisés de Oliveira**. Crimes Virtuais, Vítimas reais**. Rio de Janeiro: Brasport, 2014.
- CNN. **Medidas tomadas não são suficientes para impedir hackers russos, diz Casa Branca.** Disponível em: < https://www.cnnbrasil.com.br/internacional/2021/04/25/medidas-tomadas-nao-sao-suficientes-para-impedir-hackers-russos-diz-casa-branca > Acesso em: 27 de abril de 2021.

- Coalisão Direitos na Rede. **Carta aos Membros do Senado Federal sobre a Convenção de Budapeste** [Online]. Brasília. 2021. Disponível em: < https://direitosnarede.org.br/2021/10/21/carta-aos-membros-do-senado-federal-sobre-a-convencao-de-budapeste/> Acesso em: 02 de setembro de 2022.
- Coalisão Direitos na Rede. **Congresso Nacional inclui direito à proteção de dados pessoais na Constituição Federal** [Online]. Disponível em: https://direitosnarede.org.br/2022/02/10/congresso-nacional-inclui-direito-a-protecao-de-dados-pessoais-na-constituicao-federal/> Acesso em 02 de setembro de 2022.
- Coalisão Direitos na Rede**. Proteção de dados pessoais na segurança pública e em investigações criminais** [Online]. Brasília. 2020. Disponível em: < https://direitosnarede.org.br/2020/11/09/protecao-de-dados-pessoais-na-seguranca-publica-e-em-investigacoes-criminais/> Acesso em 02 de setembro de 2022.
- COLLI, Maciel. **Cibercrimes: Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos**. Curitiba: Juruá Editora, 2010.
- Conselho da Europa. Lista Completa dos Tratados do Concelho da Europa [Online]. Estraburgo. Disponível em: < https://www.coe.int/en/web/conventions/full-list >. Acesso em 20 de agosto de 2022
- Conselho da Europa. ***Consultations with civil society, data protection authorities and industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime*** [Online]**.** Estraburgo. Disponível em: < https://www.coe.int/en/web/cybercrime/protocol-consultations > Acessado em 29 de agosto de 2022.
- Conselho da Europa. ***Congress of Brazil approves accession to the Budapest Convention*** [Online]**.** Estraburgo. 2021. Disponível em: < https://www.coe.int/en/web/cybercrime/-/congress-of-brazil-approves-accession-to-the-budapest-convention > Acesso em: 05 de agosto de 2022.
- Conselho da Europa. ***Brazil: Cybercrime legislation – Domestic equivalent to the provisions of the Budapest Convention*** [Online]**.** Estraburgo. 2020. Disponível em: < https://rm.coe.int/octocom-legal-profile-brazil-final/1680a11cb5 > Acesso em: sso em: 05 de agosto de 2022.
- Conselho da Europa. ***Country Wiki*** [Online]**.** Estraburgo. 2021. Disponível em: < https://www.coe.int/en/web/octopus/country-wiki > Acesso em: 05 de agosto de 2022.

- Conselho dos Direitos Humanos. ***Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression***. David Kaye. Disponível em: < www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc > Acessado em 29 de agosto de 2022.
- CONVENÇÃO SOBRE CIBERCRIME. Disponível em: < convencao_cibercrime (mpf.mp.br) > . Acesso em 18 de agosto de 2022.
- CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 5 ed. São Paulo, Saraiva, 2010.
- 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/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos > Acesso em: 10 de abril de 2021.
- EILBERG, Daniela D. ZANATTA, Rafael A. F. SANTOS, Bruna M. SALIBA, Pedro. VERGILI, Gabriela. CUNHA, Brenda. **Os Cuidados com a Convenção de Budapeste** [Online]. JOTA. 2021. Disponível em: < https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste-08072021 > Acesso em 26 de agosto de 2022.
- FERREIRA, Ivette Senise**. Direito & Internet**: Aspectos Jurídicos Relevantes. 2 ed. São Paulo: Quartier Latin, 2005.
- GARCEZ, Júnior da Silva. Breves Anotações Sobra a **Cooperação Jurídica Internacional na Convenção de Budapeste e a Investigação e Persecução de Crimes Cibernéticos**. Jus.com. 2022 [Online]. Acesso em 24 de agosto de 2022.
- G1. **Polícia Civil inicia investigação sobre ataque cibernético ao sistema do TJ-RS.** Disponível em: < https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/04/30/policia-civil-inicia-investigacao-sobre-ataque-ao-sistema-informatico-do-tj-rs.ghtml > Acesso em 01/05/2021.
- G1. **Deep web: o que é e como funciona – G1 Explica.** Disponível em: < http://g1.globo.com/tecnologia/blog/seguranca-digital/post/deep-web-o-que-e-e-como-funciona-g1-explica.html > Acesso em 01/05/2021.
- GONÇALVES, Victor Hugo Pereira, **Marco civil da internet comentado** – 1. ed. – São Paulo : Atlas, 2017.

- GRABOSKY, Peter et al. **Keynotes in criminology and criminal justice series: Cybercrime**. Oxford University Press, 2016.
- HILDEBRANT, Mireille. ***Law for Computer Scientists and Other Folks***. Oxford: Oxford University Press, pag. 181 Oxford: Oxford University Press [Online]. 2022. < https://www.cohubicol.com/assets/uploads/law_for_computer_scientists.pdf > Acesso em 29 de agosto de 2022.
- MEDEIROS, Gutembergue Silva. **Crimes Cibernéticos: Considerações Sobre a Criminalidade na Internet.** Disponível em: < https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/#_ftn1 > Acesso em: 19 de abril de 2021.
- Ministério das Relações Exteriores e Ministério da Justiça e Segurança Pública. Processo de adesão à Convenção de Budapeste [Online]. Brasília. 2019. Disponível em <https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/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 de agosto de 2022.
- OLIVEIRA, B. M.; MATTOS, K. R.; SIQUEIRA, M. S.; OLIVEIRA, N. Crimes virtuais e a legislação brasileira, (re)pensando direito. **Revista do Curso em Graduação em Direito do Instituto Cenecista de Ensino Superior de Santo Ângelo, EDIESA**, ano 7, n. 13, p. 119-130, jan./jun. 2017. ISSN versão eletrônica 2447-3464;
- ORTHMANN, Patrícia et al. CRIMES CIBERNÉTICOS E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). **Revista de Estudos Jurídicos UNA**, v. 9, n. 1, p. 133-145, 2022.
- PACHECO, Luciana Botelho. **Como se fazem as leis** [recurso eletrônico]. – 3. ed. – Brasília : Câmara dos Deputados, Edições Câmara, 2013. 81 p. – (Série conhecendo o legislativo; n. 9). Acesso em 15/08/2022
- PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. **A nova lei de crimes digitais**, 2013. Disponível em: < www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432>. Acesso em 15 de agosto de 2022
- PINHEIRO, Patrícia Peck, Direito digital — 5. ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012 — São Paulo : Saraiva, 2013.
- PINHEIRO, Patrícia Peck. **Direito Digital**. 6°. Ed. São Paulo: Saraiva, 2016.

- RODRIGUES, Gustavo. **A Convenção de Budapeste sobre o Cibercrime e as controvérsias sobre a adesão brasileira** [Online]. IRIS. 2021. Disponível em: < https://irisbh.com.br/a-convencao-de-budapeste-sobre-o-cibercrime-e-as-controversias-sobre-a-adesao-brasileira/ > Acesso em 28 de agosto de 2022.
- ROHRMANN, Carlos Alberto. **Curso de Direito Virtual**. Belo Horizonte: Del Rey, 2005.
- SECRETARIA DE COOPERAÇÃO INTERNACIONAL (MPF). **Convenção Sobre o Cibercrime**. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf/>. Acesso em: 25 de agosto de 2022.
- SENADO FEDERAL. **Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético.** Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico>. Acesso em: 25 de agosto de 2022.
- SENADO FEDERAL. Decreto Legislativo nº 37 de 16/12/2021. Disponível em: <https://legis.senado.leg.br/norma/35289207/publicacao/35300588>. Acesso em: 25 agosto de 2022.
- SENADO FEDERAL. **MP concede autonomia de autarquia à Autoridade Nacional de Proteção de Dados**. Disponível em: < https://www12.senado.leg.br/noticias/materias/2022/06/14/mp-concede-autonomia-de-autarquia-a-autoridade-nacional-de-protecao-de-dados > Acesso em 04 de setembro de 2022.
- Smith, Russell G., Grabosky, Peter e Urbas, Gregor. **Cyber Criminals on Trial. Cambridge** University Press, Cambridge UK. 2004.
- SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. **A Convenção de Budapeste e as leis brasileiras**. Seminário Cibercrime e Cooperação Penal Internacional, n. 1, 2009 [Online]. Disponível em: < https://www.mpam.mp.br/images/stories/A_convencao_de_Budapeste_e_as_leis_brasileiras.pdf >. Acesso em 25 de agosto de 2022.
- TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. 5. ed. São Paulo: Saraiva Educação, 2020.

- União Internacional de Telecomunicação - UIT. **Relatório Global de Conectividade 2022.** Disponível em: < https://www.itu.int/hub/publication/d-ind-global-01-2022/#> Acesso em: 14 de julho de 2022.
- VADEMECUM, Código Penal, 5ª edição. São Paulo. Editora JusPODIVM, 2019.
- Valor, Globo. **Crimes digitais crescem pós-pandemia e provocam corrida por ciberseguros.** Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2022/06/27/crimes-digitais-crescem-pos-pandemia-e-provocam-corrida-por-ciberseguros.ghtml>. Acesso em: 05 de setembro de 2022.
- VERONESE, Alexandre. CALABRICH, Bruno. **Cybercrime in Brazil After the COVID-19 Global Crisis: An Assessment of the Policies Concerning Internacional Cooperation for Investigations and Prosecutions**. 2022.
- WALL, David. **Cybercrime: The transformation of crime in the information age**. Polity, 2007.
- WALL, DavidS. **Crime and deviance in cyberspace.** Ashgate**.** 2009**.**
- ZANELLATO, Marco Antônio. **Condutas Ilícitas na sociedade digital,** Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet, julho de 2002.