Convenção sobre o Crime Cibernético: impactos da internalização no ordenamento jurídico brasileiro e na cooperação internacional[1]

Rogério Postai

Técnico do Ministério Público da União. Especializado em Informação e Comunicação, Jornalista e Repórter Cinematográfico. Bacharel em Direito pelo Centro Universitário Sociesc, Joinville-SC.

Welligton José Fernandes Moreira

Bacharel em Direito pelo Centro Universitário Sociesc, Joinville-SC.

Resumo: O presente artigo objetiva analisar como o ordenamento jurídico e as instituições brasileiras têm-se adaptado para lidar com a crescente criminalidade no ciberespaço, bem como examinar os benefícios e os impactos que a internalização da Convenção sobre o Crime Cibernético, também conhecida como Convenção de Budapeste, trouxe para a investigação, a persecução penal e a cooperação internacional no combate aos crimes cibernéticos. Para a consecução desse objetivo, utilizou-se o método indutivo e as técnicas de pesquisa bibliográfica, documental e legislativa, e também a pesquisa em *websites* e periódicos na internet. Por fim, nas considerações finais deste artigo são elencadas as conclusões obtidas no que concerne aos benefícios e impactos decorrentes da adesão do Brasil à convenção, tornando-o mais efetivo no combate aos crimes cibernéticos mas, ao mesmo tempo, resguardando os direitos e garantias individuais arduamente conquistados pela Constituição brasileira de 1988.

Palavras-chave: Convenção sobre o Crime Cibernético; Convenção de Budapeste; cibercrime; cooperação internacional; direitos fundamentais.

Processo de internalização da Convenção de Budapeste. 2.4 A Convenção de Budapeste e a cooperação internacional. 3 Conclusões.

1 Introdução

A Convenção sobre o Crime Cibernético (ou Convenção de Budapeste), surgida no âmbito do Conselho da Europa,[2] é o primeiro instrumento jurídico internacional que reprime a cibercriminalidade. As discussões se iniciaram na década de 1990, e o texto final da convenção foi aberto para assinaturas em 23 de novembro de 2001, na cidade de Budapeste (Hungria), entrando em vigor em 1º de julho de 2004, após atingir número mínimo de ratificações.

Embora tenha origem no Conselho da Europa, a convenção mostrou desde o início o propósito de ser um mecanismo internacional, uma vez que países não europeus, como Estados Unidos, Canadá, Japão e África do Sul, participaram dos debates que resultaram no texto final da convenção. Atualmente, a convenção conta com 68 Estados Partes e 21 países observadores ou convidados a aderirem, estando o Brasil no primeiro grupo (THE BUDAPEST..., 2023).

Conforme se constata no Preâmbulo da convenção, uma das motivações que levaram à sua elaboração como um tratado internacional vinculante foi

> a necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adopção de legislação adequada e da melhoria da cooperação internacional. (CONSELHO DA EUROPA, 2001).

Desde a sua entrada em vigor, a Convenção sobre o Crime Cibernético tem sido referência não apenas para os países que a ratificaram, como também para outros países que nela se apoiam para ajustar o seu ordenamento jurídico ao surgimento de novas formas de criminalidade envolvendo sistemas informáticos.

No Brasil, embora a convenção estivesse presente no debate legislativo ao longo das últimas duas décadas, quando serviu como referência aos Projetos de Lei 84/1999, que deu origem à Lei n. 12.735/2012,

e 2.793/2011, que originou a Lei n. 12.737/2012, apenas em 2019 é que o Poder Executivo manifestou ao Conselho da Europa o interesse de adesão como Estado Parte. Em 16 de dezembro de 2021, após dois anos de tramitação na Câmara dos Deputados e no Senado Federal, o texto da convenção foi aprovado.

Neste artigo, buscou-se evidenciar as implicações decorrentes das obrigações assumidas por um Estado Parte da convenção, bem como eventuais divergências e lacunas jurídicas que deverão ser conformadas para a obtenção de uma legislação que se coadune com uma política criminal comum entre os Estados Partes. Também se analisou a temática da cooperação internacional no combate aos crimes cibernéticos, um dos temas chaves da convenção e no qual o Brasil mais poderá evoluir e dele se beneficiar.

Sem a pretensão de ser exaustivo, este artigo buscou dar respostas ao seguinte problema: quais as limitações e dificuldades enfrentadas pelas instituições brasileiras no combate aos crimes cibernéticos e de que forma a ratificação da Convenção de Budapeste pode tornar este combate mais efetivo?

Como objetivo geral, buscou-se analisar como o ordenamento jurídico e as instituições brasileiras têm-se adaptado para lidar com a crescente criminalidade no ciberespaço, bem como examinar os benefícios e os impactos que a internalização da Convenção de Budapeste tem para a investigação, a persecução penal e a cooperação internacional no combate aos crimes cibernéticos.

Sem perder de vista a temática exposta no objetivo geral, buscou-se, ainda, como objetivos específicos: I) descrever os temas abordados na Convenção de Budapeste, buscando compreender seu processo de formação, seu alcance no cenário internacional e como se dá o processo de adesão de terceiros interessados; II) analisar o quadro jurídico de que o Brasil dispõe para combater a cibercriminalidade e identificar como esta legislação dialoga com a Convenção de Budapeste, bem como eventuais lacunas que possam vir a ser supridas por meio da harmonização com o texto da convenção; III) analisar os benefícios e impactos que a internalização da convenção proporciona às instituições brasileiras responsáveis pela prevenção, investigação, resolução e repressão aos crimes cibernéticos.

De forma a responder ao problema proposto e garantir a consecução dos objetivos, a metodologia utilizada foi a da abordagem qualitativa, de natureza básica, com objetivos de pesquisa exploratória. Como procedimento, utilizou-se da revisão bibliográfica e da pesquisa em *websites* e periódicos na internet.

Por fim, nas considerações finais são elencadas as conclusões obtidas no que concerne aos benefícios e impactos decorrentes da adesão do Brasil à Convenção de Budapeste, que inegavelmente gera instrumentos para maior efetividade na prevenção, investigação, resolução e repressão aos crimes cibernéticos, mas, por outro lado, demanda que legislador e sociedade civil dialoguem a fim de que sejam resguardados direitos individuais, garantias fundamentais e o interesse nacional, pilares da Constituição brasileira de 1988.

2 A internalização da Convenção de Budapeste no ordenamento jurídico brasileiro

Tendo o Brasil manifestado interesse de adesão à Convenção de Budapeste em 2019, é mister conhecer os temas nela abordados, a fim de se compreenderem as compatibilidades e as lacunas que o arcabouço jurídico nacional em vigor apresenta em relação à convenção.

2.1 Temas abordados na Convenção de Budapeste

O texto principal da Convenção de Budapeste sobre Cibercrime se divide em quatro capítulos: (I) terminologia; (II) medidas a serem tomadas em nível nacional; (III) cooperação internacional; e (IV) disposições finais.

A terminologia padronizada pela convenção é definida no artigo primeiro. Nele encontram-se os conceitos de "Sistema informático", "Dados informáticos", "Fornecedor de serviço" e "Dados de tráfego".

No Capítulo II, são abordadas as medidas a serem tomadas em âmbito nacional por Estado Parte da convenção. Esse capítulo subdivide-se em seções: na seção 1, aborda-se o direito penal material; na seção 2, o direito processual; e a seção 3 trata das questões relativas à competência.

No Capítulo III, também subdividido em seções, o foco é a cooperação internacional. A seção 1 trata dos princípios gerais, e a seção 2, das disposições específicas relativas à cooperação.

O Capítulo IV, que engloba os artigos 36 a 48, trata das disposições finais. Nele são tratados temas gerais, tais como assinatura e entrada em vigor, adesão à convenção, aplicação territorial, reservas, resolução de litígios, entre outros.

2.1.1 Visão geral do direito material penal na Convenção de Budapeste

Os artigos de 2 a 13 da convenção formam o arcabouço de direito material penal e neles são tipificadas as infrações penais que devem estar contidas na legislação interna dos Estados Partes: acesso ilegítimo (artigo 2); intercepção[3] ilegítima (artigo 3); interferência em dados (artigo 4); interferência em sistemas (artigo 5); uso abusivo de dispositivos (artigo 6); falsidade informática (artigo 7); burla informática (artigo 8); infrações relacionadas com pornografia infantil (artigo 9); e infrações relacionadas com a violação do direito de autor e dos direitos conexos (artigo 10). O artigo 11 trata da tentativa e cumplicidade; o artigo 12 trata da responsabilidade de pessoas colectivas;[4] e o artigo 13 trata das sanções e medidas concernentes às infrações penais a serem adotadas pelos Estados Partes.

2.1.2 Visão geral do direito processual penal na Convenção de Budapeste

O direito processual, que estabelece as regras na investigação e persecução penal de crimes cibernéticos, está disposto nos artigos de 14 a 22: âmbito das disposições processuais (artigo 14); condições e salvaguardas (artigo 15); conservação expedita de dados informáticos armazenados (artigo 16); conservação expedita e divulgação parcial de dados de tráfego (artigo 17); injunção (artigo 18); busca e apreensão de dados informáticos armazenados (artigo 19); recolha em tempo real de dados relativos ao tráfego (artigo 20); intercepção de dados relativos ao conteúdo (artigo 21); e competência (artigo 22).

2.1.3 A cooperação internacional no âmbito da Convenção de Budapeste

O Capítulo III da convenção, que compreende os artigos de 23 a 35, é dedicado ao tema da cooperação internacional. Neles estão dispostos: princípios gerais relativos à cooperação internacional (artigo 23); extradição (artigo 24); princípios gerais relativos ao auxílio mútuo (artigo 25); informação espontânea (artigo 26); procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis (artigo 27); confidencialidade e restrição de utilização (artigo 28); conservação expedita de dados informáticos armazenados (artigo 29); divulgação expedita dos dados de tráfego conservados (artigo 30); auxílio mútuo relativamente ao acesso a dados informáticos armazenados (artigo 31); acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público (artigo 32); auxílio mútuo relativamente à recolha de dados de tráfego em tempo real (artigo 33); auxílio mútuo em matéria de intercepção de dados de conteúdo (artigo 34); e rede 24/7 (artigo 35).

2.2 Protocolos adicionais à Convenção de Budapeste

Além do texto principal, o Conselho da Europa, por meio do Comitê da Convenção sobre o Crime Cibernético (T-CY), elabora e disponibiliza protocolos adicionais, com o objetivo de articular novos temas e demandas dos Estados Membros na luta contra o cibercrime.

Atualmente, dois protocolos adicionais ao texto original estão disponíveis para adesão. Ressalta-se, porém, que a convenção e os protocolos adicionais são instrumentos jurídicos independentes, podendo um país ratificar a convenção sem se vincular aos protocolos adicionais.

2.2.1 Primeiro protocolo adicional

O primeiro protocolo adicional[5] à convenção dispõe sobre a incriminação de atos de natureza racista e xenófoba praticados através de sistemas informáticos. Foi publicado em janeiro de 2003, mas entrou em vigor somente em 2006.

Esse protocolo tem como objetivo principal a promoção de uma maior harmonização entre legislações relevantes no campo do direito criminal sobre a luta contra o racismo e a xenofobia na internet.

2.2.2 Segundo protocolo adicional

O segundo protocolo adicional[6] à convenção, que dispõe sobre o reforço da cooperação e da divulgação de provas sob a forma eletrônica, foi disponibilizado para assinatura pelos Estados Partes interessados em maio de 2022.

Discussões preliminares nos últimos cinco anos no âmbito do Comitê sobre Cibercrime da Convenção de Budapeste (T-CY) concluíram que existia uma dificuldade dos Estados em obter acesso a dados privados em função de questões como territorialidades, computação em nuvem e alcance de jurisdições. Nele são tratadas questões como acesso transfronteiriço a dados e Assistência Judiciária Mútua (*Mutual Legal Assistance* – MLA),[7] além de estabelecer parâmetros mais claros para cooperação direta entre autoridades e provedores de serviços digitais (SANTOS, 2022, p. 13).

2.3 Processo de internalização da Convenção de Budapeste

O Brasil não participou da elaboração do texto da Convenção de Budapeste, mas desde que entrou em vigência em 2001, ela tem sido referência para o legislativo pátrio nas discussões de projetos de lei que versam sobre crimes cibernéticos. Apenas no final de 2019 é que o Poder Executivo brasileiro manifestou interesse ao Conselho da Europa em ser convidado a se tornar Estado Parte da convenção. Recebido o convite em 11 de dezembro de 2019, a aprovação legislativa do texto da convenção foi concluída em 16 de dezembro de 2021, por meio do Decreto Legislativo n. 37 (BRASIL, 2021). É importante destacar que tal aprovação não fez menção a reservas ao texto da convenção, caracterizando adesão irrestrita por parte do Brasil.

O Decreto n. 11.491, de 12 de abril de 2023,[8] ratificou a convenção pelo Poder Executivo, após o que os dispositivos do texto passaram a integrar o ordenamento jurídico interno, elevando o Brasil da condição de país observador a Estado Parte da convenção.

2.4 A Convenção de Budapeste e a cooperação internacional

A possibilidade de usufruir dos benefícios da cooperação internacional foi o um dos principais motivos que levaram as instituições encarregadas da prevenção, investigação, resolução e repressão aos crimes cibernéticos no Brasil a requererem celeridade no processo de ratificação da Convenção de Budapeste.

Como tais crimes se caracterizam por não respeitarem fronteiras, a cooperação internacional precisa ser ágil e eficiente, principalmente no que diz respeito a provas digitais, cuja natureza volátil eleva o risco de se perderem, e também no que diz respeito às consequências das condutas criminosas praticadas nos meios digitais interconectados, os quais proporcionam rápido alcance global.

Nesse sentido, tanto o texto principal da convenção como o seu segundo protocolo adicional dispõem de ferramentas e procedimentos que facilitam a cooperação entre os países membros.

Essa cooperação já se faz presente nos grupos de discussão derivados do Comitê da Convenção do Cibercrime (T-CY), nos quais representantes dos países membros tratam da interpretação e do alcance das normas da convenção. Dentre esses grupos, destacam-se o Comitê para o acesso transfronteiriço a provas, o Comitê para o acesso da prova digital na nuvem e o Comitê para o artigo 13, que trata das sanções[9] (MPF, 2018).

A cooperação internacional é objeto do Capítulo III da convenção. Nele estão dispostos os princípios relativos à cooperação internacional, à extradição e ao auxílio mútuo, as diretrizes para a comunicação de informações espontâneas (quando uma parte espontaneamente compartilha informações obtidas em investigação com outra parte) e o os procedimentos relativos aos diversos tipos de pedidos de auxílio mútuo entre as partes.

Contudo, o grande diferencial da convenção em termos de cooperação internacional é a criação da Rede 24/7. No artigo 35, a convenção estabelece que:

> 1. Cada parte designará um ponto de contacto disponível 24 horas sobre 24 horas, 7 dias por semana, a fim de assegurar a prestação de

> assistência imediata a investigações ou procedimentos respeitantes a infracções penais relacionadas com dados e sistemas informáticos, ou a fim de recolher provas, sob forma electrónica, de uma infracção penal. O auxílio incluirá a facilitação, ou se o direito e práticas internas o permitirem, a aplicação directa das seguintes medidas:
>
> a) A prestação de aconselhamento técnico;
>
> b) A conservação de dados em conformidade com os artigos 29 e 30; e
>
> c) A recolha de provas, informações de caráter jurídico e localização de suspeição. (CONSELHO DA EUROPA, 2001).

Ciente das limitações no texto da convenção, em maio de 2022 o Conselho da Europa disponibilizou para assinatura pelos países interessados o segundo protocolo adicional à Convenção sobre o Cibercrime, o qual dispõe sobre o reforço da cooperação e da divulgação de provas sob a forma eletrônica.

Na "Nota Técnica do Grupo de Apoio sobre Criminalidade Cibernética sobre a Convenção do Cibercrime (Convenção de Budapeste)", o Ministério Público Federal destaca que no segundo protocolo adicional estão sendo deliberadas formas de MLA emergenciais e ordinárias, porém com rito abreviado, além de outras formas de cooperação diligentes e mais eficientes, tais como a formação de equipes de investigação conjunta e a aceitação de videoconferências como prova no âmbito da convenção (MPF, 2018).

Ainda segundo o entendimento do Ministério Público Federal,

> [o] novo protocolo irá moldar a forma da investigação e cooperação internacional nessa área por muitos anos e há todo o interesse do MPF em poder utilizar desde logo as ferramentas já existentes para a eficiência da investigação criminal, bem como influenciar no formato das novas formas de cooperação. (MPF, 2018).

Além dos instrumentos jurídicos supracitados, também é de grande interesse das instituições brasileiras o acesso aos programas de capacitação e treinamento implementados por meio do Gabinete do Programa de Cibercrime do Conselho da Europa (C-PROC).[10]

Dentre os programas, destaca-se o *Global Action on Cybercrime Extended* (GLACY+, 2022), projeto conjunto da União Europeia e do Conselho da

Europa, iniciado em 2016 e previsto para encerrar em 2024, que visa a dar apoio a dezenove países na África, Ásia-Pacífico, América Latina e Caribe: Benin, Brasil, Burkina Faso, Cabo Verde, Chile, Colômbia, Costa Rica, República Dominicana, Fiji, Gana, Ilhas Maurício, Marrocos, Nigéria, Paraguai, Peru, Filipinas, Senegal, Sri Lanka e Tonga. Esses países podem servir como centros para compartilhar suas experiências em suas respectivas regiões.

No âmbito desse projeto, realizou-se, nos meses de maio e junho de 2022, a "Série de workshops de *stakeholders* sobre o novo quadro jurídico nacional em matéria de cibercrime e a Convenção de Budapeste", evento online organizado pelo Ministério Público Federal e pela Escola Nacional de Formação e Aperfeiçoamento de Magistrados (Enfam), com participação de especialistas europeus e americanos.

No que concerne à cooperação internacional, tiveram destaque:

a) A Agência da União Europeia para Cooperação em Justiça Criminal (Eurojust): esta instituição ajuda os Estados Membros da União Europeia a combaterem os crimes cibernéticos, auxiliando as autoridades judiciárias a mapear os requisitos legais para efetuar as intervenções necessárias, facilitando o uso de ferramentas de cooperação judiciária. Conforme pontuou Cláudia Pina, representante do Conselho da Europa, "[o] Eurojust pode celebrar acordos internacionais para consolidar parcerias com países terceiros, aproximando-os de Estados Membros na luta contra a criminalidade transfronteiriça grave, incluindo o cibercrime" (QUEM..., 2023).

b) A Rede 24/7: a representante do gabinete de procuradores da Romênia,[11] Ioana Albani, explanou sobre a "Rede 24/7", a rede de contatos no âmbito da Convenção de Budapeste na qual cada parte deve nomear um ponto de contato disponível para fornecer auxílio imediato à outra parte da investigação dos crimes cibernéticos.

c) As parcerias público-privadas para resolução de cibercrimes: o assessor para Assuntos de Propriedade Intelectual, vinculado ao Consulado dos Estados Unidos, Daniel Ackerman, falou sobre as parcerias público-privadas e as empresas relacionadas a criptoativos. Ele defendeu a importância de se "conhecer as políticas dos provedores nacionais e, com base nisso, elaborar estratégias para acesso e preservação de dados" (ENFAM, 2022).

3 Conclusões

Após os estudos empreendidos no presente artigo, conclui-se que, dadas as condições de interdependência que permeiam as intrincadas relações estatais neste início do século XXI e a inexistência de outros acordos internacionais relativos aos crimes cibernéticos disponíveis para adesão, é premente a necessidade de assegurar ao Brasil um arcabouço jurídico apropriado para a efetividade da prestação jurisdicional no que concerne ao crescente aumento dos crimes cibernéticos. Nesse sentido, o processo de internalização da Convenção de Budapeste pode suprir as lacunas e deficiências existentes no ordenamento jurídico brasileiro.

Com base nas declarações dos diversos autores consultados e no lapso temporal de quase vinte anos decorrido entre a disponibilização da convenção para assinatura e o pedido de adesão feito pelo governo brasileiro, conclui-se que nem o Poder Executivo nem o Poder Legislativo têm dado a devida importância ao tema dos crimes cibernéticos, bem como não têm feito o devido uso de legislações estrangeiras já em vigor, tais como a Convenção de Budapeste, resultante de amplas e equilibradas discussões, para aperfeiçoar o direito interno.

Dentro do que foi proposto como objetivo geral deste artigo, buscava-se compreender como o ordenamento jurídico e as instituições brasileiras têm se adaptado para lidar com a crescente criminalidade no ciberespaço, bem como analisar os benefícios e os impactos que a internalização da Convenção de Budapeste trouxe para a investigação, a persecução penal e a cooperação internacional no combate aos crimes cibernéticos.

No que concerne à parte inicial do objetivo geral, após a análise da legislação correlata já em vigor e do respectivo processo de tramitação, constatou-se uma grande morosidade legislativa, tal como se deu com o PL n. 84/1999, que resultou na Lei n. 12.735 ("Lei Azeredo"), a qual levou mais de treze anos para ser aprovada. Além disso, esse projeto de lei foi significativamente reduzido, resultando ao final em duas normas praticamente inócuas e que pouco supriam as necessidades da sociedade brasileira. Portanto, morosidade e ineficiência é o que tem caracterizado o legislador brasileiro na tratativa dos crimes cibernéticos.

Quanto à parte final do objetivo geral, buscou-se identificar os benefícios e os impactos que a internalização da Convenção de Budapeste trouxe para a investigação, a persecução penal e a cooperação internacional no combate aos crimes cibernéticos. De acordo com o Ministério Público Federal (2018), a adesão à convenção proporcionará ao Brasil, entre outros, os seguintes benefícios:

a) Harmonização da legislação brasileira com a legislação dos demais países da convenção: um dos requisitos para a punibilidade quando se trata de crimes transfronteiriços ou quando se trata de pedidos de extradição é o princípio da dupla punibilidade, ou seja, a conduta precisa ser penalmente relevante nas legislações dos respectivos países envolvidos. Na medida em que os dispositivos da convenção preestabelecem quais tipos penais devem ser previstos nas legislações internas de cada Estado Membro, reduzem-se as possibilidades de impunibilidade dos crimes cibernéticos por discrepâncias entre as legislações nacionais.

b) Vigor da legislação penal brasileira: embora o Brasil tenha editado leis que atacam o problema da cibercriminalidade, duas deficiências podem ser apontadas, quais sejam, penas excessivamente brandas e lacunas jurídicas que impedem que determinadas condutas sejam punidas. Ao aderir à convenção, cria-se a obrigação da aprovação de leis que supram essas deficiências.

c) Ao tornar-se Estado Parte, o Brasil participará do Comitê da Convenção sobre o Cibercrime (T-CY) como membro, com direito a voto. Como esse comitê é responsável pela elaboração de novos instrumentos jurídicos (protocolos adicionais) e pela constante evolução da convenção, o Brasil terá a oportunidade de influenciar nos debates, além de diminuir o atraso entre a disponibilização de novos instrumentos e a adoção destes internamente.

d) Com a adesão, as instituições brasileiras diretamente implicadas no combate aos crimes cibernéticos passam a receber capacitação por meio do Gabinete do Programa de Cibercrime do Conselho da Europa (C-PROC).

e) Com a adesão, o Brasil passará a dispor de quadro jurídico para a cooperação internacional em matéria de cibercriminalidade e prova

eletrônica, uma vez que a própria convenção poderá ser utilizada como base legal quando o Brasil requerer a cooperação de um país com o qual não possua acordo bilateral em matéria penal.

Em que pese serem cristalinos os benefícios da adesão à convenção, uma análise que se pretenda pautar pela imparcialidade não pode se furtar de apontar aqueles que seriam os pontos de vulnerabilidade em que o Brasil poderá incorrer após a adesão à convenção. Assim, os seguintes aspectos requerem a atenção cuidadosa, sobretudo da sociedade civil:

a) O processo de adesão, além de ter sido discutido de forma célere, teve pouca participação de representantes da sociedade civil. A proteção de direitos humanos e de direitos fundamentais pode ter sido negligenciada na fase de adesão, requerendo uma análise mais atenta na fase de adequação da legislação doméstica ao texto da convenção.

b) A convenção foi aprovada sem qualquer reserva, com aceitação integral dos dispositivos do texto. Dessa forma, eventuais conflitos entre a legislação interna e os dispositivos da convenção obrigam o Brasil a uma adequação que poderá ser desfavorável aos seus interesses. Tal ausência de reservas é ainda mais preocupante quando se encontra em discussão no Congresso Nacional um novo Código de Processo Penal.

c) Na fase de adequação da legislação interna à convenção, há risco de o legislador, por interesses obscuros de setores privados interessados ou até mesmo de um eventual Poder Executivo com viés autoritário, promover reformas na legislação penal e processual penal que coloquem em risco direitos à privacidade, à proteção de dados e ao devido processo legal.

Concluída essa análise de benefícios e impactos da adesão do Brasil à Convenção de Budapeste e uma vez que seus dispositivos tenham passado a integrar o ordenamento jurídico brasileiro, espera-se que a internalização do tratado possa trazer solução à problemática que suscitou este estudo, ou seja, que as instituições brasileiras possam suprir as limitações e dificuldades que as impedem de serem plenamente efetivas no combate aos crimes cibernéticos e que a adesão à convenção, seguida de uma implementação mais participativa dos diversos setores

da sociedade civil, seja o instrumento que permitirá ao Brasil se tornar um local seguro, inclusive na pequena parte que lhe compete jurisdição deste novo território que desconhece fronteiras: o ciberespaço.

Referências

BRASIL. **Decreto Legislativo n. 37, de 16 de dezembro de 2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília, 16 dez. 2021. Disponível em: https://tinyurl.com/3m8h85e9. Acesso em: 5 jun. 2023.

COMMITTEE of Ministers: Convention on Cybercrime (ETS n. 185). Request by Brazil to be invited to accede. **Council of Europe Portal**, Strasbourg, 2023. Disponível em: https://tinyurl.com/mr33s9b7. Acesso em: 29 out. 2022.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23 de novembro de 2001. Disponível em: https://tinyurl.com/55watk36. Acesso em: 1º out. 2022.

CONSELHO DA EUROPA. **Protocolo adicional à Convenção sobre o Cibercrime relativo à incriminação de actos de natureza racista e xenófoba praticados através de sistemas informáticos**. Estrasburgo: Conselho da Europa, 28 jan. 2003. Disponível em: https://tinyurl.com/79aafaee. Acesso em: 1º out. 2022.

CONSELHO DA EUROPA. **Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da divulgação de provas sob a forma eletrônica**. Estrasburgo, 12 maio 2022. Disponível em: https://tinyurl.com/4enkya32. Acesso em: 1º out. 2022.

CYBERCRIME Programme Office (C-PROC). **Council of Europe Portal**, Strasbourg, 2023. Disponível em: https://tinyurl.com/45mmnuta. Acesso em: 28 out. 2022.

ENFAM – ESCOLA NACIONAL DE FORMAÇÃO E APERFEIÇOAMENTO DE MAGISTRADOS. **Enfam finaliza a série de workshop de stakeholders em matéria de cibercrime e a Convenção de Budapeste**. Brasília: Enfam, jun. 2022. Disponível em: https://tinyurl.com/227xvf9t. Acesso em: 28 out. 2022.

GLACY+ – GLOBAL ACTION ON CYBERCRIME EXTENDED. **Série de workshops de stakeholders sobre o novo quadro jurídico nacional em matéria de cibercrime e a Convenção de Budapeste**. Organizado no âmbito do projeto Glacy+ em cooperação com o Ministério Público Federal e a Escola

Nacional de Formação e Aperfeiçoamento de Magistrados. *Online*. Maio/jun. 2022. Disponível em: https://tinyurl.com/ymafxcft. Acesso em: 28 out. 2022.

MINISTÉRIO PÚBLICO FEDERAL. **Nota Técnica do Grupo de Apoio sobre Criminalidade Cibernética sobre a Convenção do Cibercrime (Convenção de Budapeste)**. [*S. l.*], Grupo de Apoio sobre Criminalidade Cibernética da 2ª Câmara de Coordenação e Revisão do Ministério Público Federal, 28 de agosto de 2018. Disponível em: https://tinyurl.com/yndnax6s. Acesso em: 1º out. 2022.

O CONSELHO da Europa em resumo: quem somos. **Council of Europe Portal**, Strasbourg, 2023. Disponível em: https://tinyurl.com/2sexzupr. Acesso em: 1º out. 2022.

QUEM somos. **Agência da União Europeia para a Cooperação em Justiça Criminal (EUROJUST)**. Haia, 2023. Disponível em: https://tinyurl.com/bdfb33rh. Acesso em: 17 jul. 2023.

SANTOS, Bruna Martins dos. **Convenção de Budapeste sobre o Cibercrime na América Latina**: uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México. [*S. l.*]: Derechos Digitales América Latina, maio 2022. Disponível em: https://tinyurl.com/243yetrw. Acesso em: 1º out. 2022.

THE BUDAPEST Convention (ETS n. 185) and its Protocols. **Council of Europe Portal**, Strasbourg, 2023. Disponível em: https://tinyurl.com/4k7dwfzw. Acesso em: 30 out. 2022.

VASCONCELLOS, Helena. **Cooperação jurídica internacional em matéria penal**: uma análise do *mutual legal assistance treaty* Brasil/Estados Unidos. 2013. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2013. Disponível em: https://tinyurl.com/2p8v9hkn. Acesso em: 29 out. 2022.

Notas

[1] Artigo apresentado como requisito parcial para a conclusão do curso de Graduação em Direito do Centro Universitário Sociesc, 2022. Orientador: Prof. Augusto Luciano Ginjo, Mestre em Direito.

[2] O Conselho da Europa é uma organização política europeia com sede em Estrasburgo (França), fundada em 1949, com o propósito de, entre outros, "defender os direitos do homem e a democracia parlamentar e assegurar a preeminência do direito". É composta por 46 Estados Membros europeus, incluindo todos os 27 países que integram a União Europeia (O CONSELHO..., 2023).

[3] O texto da Convenção de Budapeste disponível em português utiliza a nomenclatura de Portugal, o que explica a utilização de termos e palavras pouco usuais no Brasil. Neste caso, "intercepção" equivale ao que no Brasil é designado como "interceptação".

[4] "Pessoas colectivas", nomenclatura de Portugal, equivale ao que no Brasil é designado como "pessoas jurídicas".

[5] "Protocolo adicional à Convenção sobre o Cibercrime relativo à incriminação de actos de natureza racista e xenófoba praticados através de sistemas informáticos. Estrasburgo, 28 jan. 2003." (CONSELHO DA EUROPA, 2003).

[6] "Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da divulgação de provas sob a forma eletrônica. Estrasburgo, 12 de maio de 2022." (CONSELHO DA EUROPA, 2022).

[7] MLA (*Mutual Legal Assistance*) é uma espécie de cooperação internacional firmada entre os governos de dois países, os quais se comprometem a cooperar no âmbito da matéria objeto do tratado. Um tratado de MLA (MLAT) permite substituir as cartas rogatórias, as quais apresentam entraves burocráticos retardantes, tais como escopo limitado, absoluta discricionariedade do país estrangeiro, exigência de dupla incriminação e longo trâmite diplomático, enquanto os MLAT propiciam respostas céleres e adequadas quando se trata de criminalidade transnacional. Um exemplo de tratado de MLA (MLAT) é aquele firmado em matéria penal entre Brasil e Estados Unidos, internalizado no ordenamento jurídico brasileiro por meio do Decreto n. 3.810, de 2 de maio de 2001 (VASCONCELLOS, 2013).

[8] Decreto n. 11.491 - "Art. 1º Fica promulgada a Convenção sobre o Crime Cibernético, firmada em Budapeste, em 23 de novembro de 2001 [...]".

[9] Artigo 13 – Sanções e medidas

Cada parte adoptará as medidas legislativas e outras que se revelem necessárias para assegurar que as infracções penais verificadas em aplicação

dos Artigos 2 a 11 sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo penas privativas da liberdade.

Cada parte assegurará que as pessoas colectivas consideradas responsáveis nos termos do artigo 12, fiquem sujeitas à aplicação de sanções ou medidas, penais ou não penais eficazes, proporcionais e dissuasivas, incluindo sanções pecuniárias (CONSELHO DA EUROPA, 2001).

[10] O Gabinete do Programa de Cibercrime do Conselho da Europa (C-PROC) é responsável por ajudar os países em todo o mundo a fortalecer a capacidade de seus sistemas jurídicos para responder aos desafios colocados pelo cibercrime e evidências eletrônicas com base nos padrões da Convenção de Budapeste sobre o Cibercrime. Entre seus projetos de capacitação, inclui-se o GLACY+ (CYBERCRIME..., 2023).

[11] A participação de representantes romenos nos programas de capacitação GLACY+ muito se deve ao fato de o Gabinete do Programa de Cibercrime do Conselho da Europa (C-PROC) estar localizado em Bucareste, capital da Romênia.