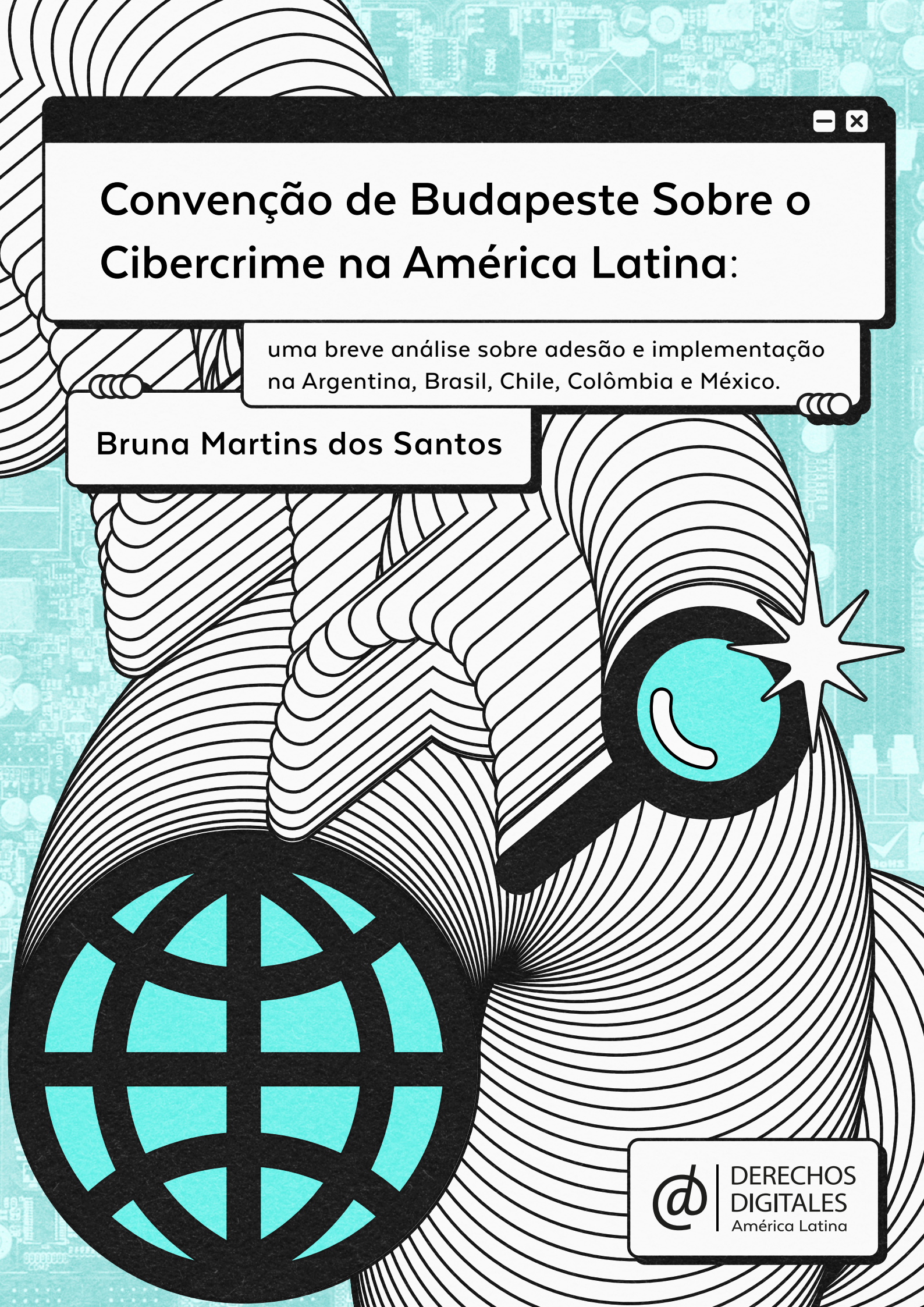
Convenção de Budapeste Sobre o Cibercrime na América Latina:

uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México.

Bruna Martins dos Santos



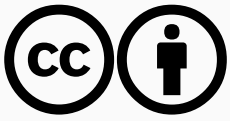
@ DERECHOS DIGITALES América Latina

Este relatório foi realizado pela Derechos Digitales com o apoio do Centro Internacional de Pesquisa para o Desenvolvimento (IDRC).

Desde 2019, a Derechos Digitales faz parte da rede de Centros de Pesquisa de Políticas Cibernéticas (Cyber Policy Research Centres) do IDRC, junto a organizações líderes em questões de tecnologias e políticas públicas no Sul Global.

Edição: **Derechos Digitales**
Autoria: **Bruna Martins dos Santos**
Tradução ao espanhol: **Gonzalo Bernabó**
Layout e capa: **Catalina Viera**
Revisão: **J. Carlos Lara, Michel Roberto de Souza, Jamila Venturini**

**A autora gostaria de agradecer a Cristian León, Secretário-Executivo da Rede Al Sur; Grecia Macías e Luis Fernando García, R3D; J. Carlos Lara, Jamila Venturini e Michel Roberto de Souza, Derechos Digitales; Bárbara Simão, Internetlab; e Carolina Bottero, Fundación Karisma; pelo tempo dedicado às entrevistas e inputs adicionais necessários para a redação do presente relatório.*



Maio de 2022

Índice

I. Introdução

Em novembro de 2001, o Conselho da Europa decidiu abrir para assinaturas o texto da Convenção sobre o Cibercrime. A Convenção de Budapeste, como é conhecida, é, até hoje, um dos principais tratados internacionais vinculantes sobre matéria penal e foi desenvolvida com o objetivo de "intensificar a cooperação internacional e prosseguir uma política criminal comum e proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adopção de legislação adequada e da melhoria da cooperação internacional".[1]

Apesar da abertura para assinaturas ter ocorrido no fim de 2001, há mais de 20 anos atrás, a Convenção continua sendo um dos principais tópicos de conversa quando se fala de uma agenda comum para cooperação Internacional e combate a crimes cometidos no ambiente digital, tendo influenciado legislações por todo o mundo.

Entre os temas tratados pela Convenção sobre o Cibercrime podemos destacar debates sobre (i) criminalização de condutas; (ii) normas para investigação; (iii) produção de provas eletrônicas; e (iv) meios de cooperação internacional, como extradição e assistência jurídica mútua.[2] Mais recentemente, com a positiva e crescente incidência de novas legislações sobre proteção de dados pessoais mundo afora, o debate sobre salvaguardas e proteção de dados aplicado ao campo de segurança pública e persecução penal também entram em cena.

No entanto, o debate não fica concentrado apenas na harmonização das atividades de persecução de delitos cibernéticos de forma transfronteiriça. Uma parte importante das críticas direcionadas à Convenção nos últimos anos tem sido em função do texto promover tipificações penais vazias e genéricas[3] e apresentar desafios de implementação de adequação para seus signatários.

---

1 Conselho da Europa. Convenção sobre o Cibercrime (Convenção de Budapeste). Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention#{

2 Ópice Blum. A Convenção de Budapeste é promulgada sob a forma do Decreto Legislativo n. 37. 22 de Dezembro de 2021. Disponível em: https://opiceblum.com.br/convencao-de-budapeste-e-promulgada-sob-a-forma-do-decreto-legislativo-no-37/

3 Serquera, Maricarmen e Samaniego, Marlene. Desafios de la Armonización de la Convención de Budapest en el Sistema Penal Paraguayo. Derechos Digitales. Junho, 2018. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/minuta_TEDIC.pdf

Em função do exposto, o presente relatório visa comentar alguns pontos principais sobre a Convenção em questão, bem como os desafios de implementação e harmonização dos dispositivos do texto com os sistemas legais e arcabouços jurídicos de países na região latinoamericana. Para a redação do presente relatório foram realizadas uma revisão bibliográfica de materiais relevantes produzidos na região[4] e entrevistas semi-estruturadas com representantes de organizações da sociedade civil que integram a rede *AI Sur*[5] localizadas no Brasil, Argentina, Colômbia, México e Chile.[6]

O documento, portanto, é dividido em sessões que se dedicam a analisar as diferentes situações relativas à adesão - ou não - à Convenção pelos países mencionados acima, bem como possíveis diferenças nos contextos locais. Além disso, as informações obtidas nos estudos de caso individuais e entrevistas realizadas foram utilizadas para formular recomendações dedicadas ao desenho e implementação de políticas públicas sobre o tema, com uma abordagem baseada na proteção de direitos humanos no ambiente digital no centro.

4 Ver, por exemplo, a série de estudos publicada pela Derechos Digitales em colaboração com organizações e especialistas latino-americanos sobre o processo de adequação das normas nacionais à Convenção de Budapeste em: https://www.derechosdigitales.org/tipo_publicacion/publicaciones/

5 A AI Sur é um consórcio de organizações latinoamericanas da sociedade civil e a academia com o objetivo de fortalecer com seu trabalho em parceria os direitos humanos no ambiente digital. Mais informações em: https://www.alsur.lat/pt-br.

6 As entrevistas contaram com representantes das organizações: Derechos Digitales (Chile), R3D (México), InternetLab (Brasil), Fundación Karisma (Colômbia) e Coalizão Direitos na Rede (Brasil).

II. A Convenção de Budapeste sobre Crimes Cibernéticos

a. Principais temas discutidos pela Convenção e sua influência nos debates de cibercrimes ao redor do mundo

A Convenção de Budapeste sobre o Cibercrime é composta por quatro capítulos sobre (a) terminologias, (b) medidas a serem tomadas em nível nacional, (c) cooperação internacional e (d) disposições finais.[7] Um dos pontos principais do texto são as tipificações de crimes cibernéticos que podem ser cometidos contra a confidencialidade de sistemas e dados informáticos, computadores, conteúdos e até violações de direitos autorais.

Apesar de se tratar de um tratado discutido e elaborado no contexto do Conselho da Europa, ao longo dos anos a Convenção de Budapeste tem se consolidado como o principal texto legal sobre cooperação internacional para fins de persecução penal e combate aos cibercrimes.
A lista de signatários conta com 44 Estados-membros do Conselho da Europa e mais alguns Estados não membros, como Argentina, Canadá, Chile, Colômbia, Estados Unidos da América, República Dominicana e Peru.[8]

O memorando explicativo do Tratado traz preocupações a respeito do crescente uso malicioso de meios de comunicação online, bem como a acessibilidade e facilidade que informações são armazenadas em sistemas informáticos, como fatores que aumentaram a disponibilidade dos fluxos de informações, e que os recentes desenvolvimentos nas novas tecnologias e mudanças podem ter contribuído para um relativo aumento na incidência de crimes cibernéticos.[9] No entanto, alguns dos aspectos mais destacados do texto nas atividades comemorativas do seu vigésimo-primeiro aniversário em 2021 foram o potencial de fomento a estruturas de cooperação público-privadas e a harmonização entre legislações e demais estruturas legais e administrativas dedicadas ao combate aos cibercrimes.[10]

---

7 Migalhas. Convenção de Budapeste e crimes cibernéticos no Brasil. Outubro, 2020. Disponível em: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil

8 Conselho da Europa. A convenção de Budapeste e seus Protocolos Adicionais. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention#{%22105166412%22:[0]}

9 Conselho da Europa. Explanatory Report on the Budapest Convention. Disponível em: https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf

10 Conselho da Europa. Benefits. Disponível em: https://www.coe.int/en/web/cybercrime/benefits

Nesse sentido, é importante apontar que apesar do teor punitivista sob o qual a Convenção de Budapeste foi elaborada, sua relevância hoje em dia se dá em função do constante trabalho de atualização e a partir de algum nível de interlocução com outras discussões como as relacionadas com a defesa dos direitos humanos na era digital. E, nos últimos anos, o tratado tem sido de fato consolidado como uma base legal inicial para a definição de estruturas de cooperação internacional, além de um guia para a posterior elaboração de legislações domésticas.

A convenção possui também um Comitê exclusivo - *Cybercrime Convention Committee* (T-CY)[11], que é responsável por discutir melhorias e atualizações para o texto, além de ser composto por todos os países signatários ou que foram convidados a assinar o Tratado. A criação do Comitê T-CY é motivada pelo artigo 46 da Convenção, que reforça a necessidade de um mecanismo de consulta periódica entre os signatários, com o objetivo principal de promover a troca de informações sobre o uso e implementação do texto, processos recentes de inovações tecnológicas e legislativas sobre o combate aos cibercrimes e coleta de evidências digitais e, também, a discussão de possíveis suplementos ou adições ao texto da convenção.[12] Adicionalmente, o colegiado, tem funcionado como um dos grupos intergovernamentais mais relevantes atualmente para a discussão e análise da implementação da Convenção, bem como elaboração de interpretações do texto por meio de notas de orientação (*guidance notes)*[13]. Desde a elaboração da convenção, foram elaboradas notas de orientação em temas como sistemas computacionais, *botnets*, ataques de DDoS, spam, terrorismo, entre outros.

---

11 Cybercrime Convention Committee (T-CY). The Budapest Convention on Cybercrime: benefits and impact in practice. Disponível em: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

12 *Article 46 – Consultations of the Parties*

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

A. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

B. the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

C. consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

13 Conselho da Europa. Guidance Notes on the Convention on Cybercrime. Disponível em: https://www.coe.int/en/web/cybercrime/guidance-notes

Ainda sobre o TC-Y, vale frisar que o comitê é o principal espaço de troca de informações sobre a implementação e uso da convenção e possui mandato para elaborar protocolos adicionais ao texto original com objetivo de articular novos temas e demandas dos estados membros na luta contra o cibercrime. De acordo com o regimento interno do órgão (*Rules of Procedure*[14]), o mandato permite que o colegiado realize avaliações sobre a implementação e impacto da Convenção, adote opiniões e recomendações sobre possíveis interpretações a respeito do texto e discuta a elaboração de instrumentos legais - como convenções e protocolos adicionais - sobre temas afetos a Convenção de Budapeste para submetê-los ao Comitê de Ministros do Conselho da Europa para aprovação.

Um outro ponto relevante a respeito da estrutura da Convenção é a rede 24/7, estabelecida pelo artigo 35[15], que consiste em uma rede de pontos de contato de todos os países signatários e cujos representantes têm que estar disponíveis para prestação de assistência imediata assim que requerido. O objetivo principal da rede mencionada é o estabelecimento de um canal de assistência para fins de investigações, procedimentos referentes a crimes cibernéticos ou até a coleta de evidências eletrônicas. Caso a legislação local autorize, a rede 24/7 também pode ser responsável pela prestação de conhecimentos técnicos, implementação de medidas de preservação/guarda de dados e a coleta de evidências digitais, incluindo informações sobre a localização de suspeitos.

Por fim, vale mencionar que o acesso/adesão ao Convênio também confere aos signatários a possibilidade de realização de atividades de conscientização e capacitação por parte do Comitê Europeu. Em um mundo onde a disputa sobre o regime de acesso a dados localizados no

14 Conselho da Europa. Cybercrime Convention Committee (T-CY) T-CY Rules of Procedure. Outubro, 2020. Disponível em: https://rm.coe.int/t-cy-rules-of-procedure/1680a00f34

15 *Article 35 – 24/7 Network*

Each Party shall designate a point of contact available on a twenty-four hour, seven-day-aweek basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

1. *A. the provision of technical advice;*
   B. the preservation of data pursuant to Articles 29 and 30;
   C. the collection of evidence, the provision of legal information, and locating of suspects.
2. *A. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.*
   B. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.
3. *Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.*

exterior é um tema recorrente, abordado em muitas legislações e projetos de lei em discussão, é relevante que a estrutura facilitada pela Convenção possa promover atividades de capacitação de atores - ainda que essa medida esteja acessível, em grande parte, apenas aos representantes dos Estados signatários.

b. Primeiro Protocolo Adicional

Como fruto do trabalho constante de revisão do T-CY sobre os dispositivos da Convenção, com base no disposto no art. 46 do tratado, em janeiro de 2003, foi publicado o primeiro protocolo adicional que dispõe sobre a incriminação de atos de natureza racista praticada através de sistemas informáticos.[16]que entrou em vigor em 2006. O texto, construído, em sua maior parte, por um comitê de elaboração constituído no contexto do T-CY - e posteriormente submetido à avaliação dos estados membros - 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 xenofobia na Internet.

Acerca das questões procedimentais em torno da atuação do TC-Y e seu papel na elaboração de protocolos adicionais à Convenção de Budapeste, vale esclarecer que o colegiado pode debater sugestões de protocolos adicionais e elaborar rascunhos dos textos. No entanto, a decisão de adoção de um determinado protocolo ou convenção adicional ao tratado principal precisa ser referendada pelo Comitê de Ministros do Conselho da Europa e posteriormente à sua aprovação o texto é aberto para a adesão dos estados signatários da convenção - a adesão à protocolos adicionais à Convenção de Budapeste não é realizada de forma automática por todos os países signatários, portanto.

16 Conselho da Europa. Details of Treaty No.189. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189

De acordo com o memorando explicativo[17] tdo texto, a aproximação de partes distantes do mundo por meio das recentes mudanças tecnológicas, comerciais e econômicas, seriam a razão para uma maior incidência e crescimento acelerado da disseminação de conteúdos de discriminação racial, xenofobia e outras formas de intolerancia no ambiente online. Em função disso, o texto apresenta uma definição para "material racista e xenófobo" (artigo 2º) e tem o objetivo de apresentar soluções comuns para reprimir a disseminação desses tipos de conteúdo por meio de sistemas informáticos.

A divisão do protocolo é feita conforme a tabela abaixo:

Tabela 1 - Resumo do Primeiro Protocolo Adicional à Convenção de Budapeste

Temas	Artigos
Dispositivos Comuns e questões gerais	Capítulo I – Disposições Comuns
	Capítulo II – Medidas a serem tomadas no nível nacional — Disseminação de conteúdo racista e xenofóbico por sistemas — Ameaças com motivações racistas e xenófobas — Insultos com motivações racistas e xenófobas — Negação, minimização, aprovação ou justificativas de genocídios e crimes contra a humanidade
Relação entre a Convenção de Budapeste e o Protocolo Adicional	Capítulo III – Relações entre a Convenção e o Protocolo
Dispositivos Finais	Capítulo IV – Disposições finais

Por fim, vale destacar que um aspecto importante sobre o primeiro protocolo adicional é a tentativa de estabelecimento de uma dinâmica equilibrada entre a liberdade de expressão dos usuários da Internet e uma luta efetiva contra a disseminação e prática de racismo e xenofobia no ambiente digital.

17 Conselho da Europa. Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. 2003. Disponível em: https://rm.coe.int/1680989b1c

c. Segundo Protocolo Adicional

O segundo protocolo adicional diz respeito a uma empreitada de atualização dos dispositivos da Convenção que é relativamente mais recente, uma vez que foi adotado em dezembro de 2021 pelos Estados membros do Comitê Europeu.[18]

O texto surgiu mais uma vez de uma decisão do T-CY sobre a necessidade de enrijecimento das regras —conforme destacado em seu memorando explicativo—[19], especialmente no que diz respeito à divulgação de informações de registro de nomes de domínio, medidas de cooperação direta com provedores de serviços para obtenção de informações de usuários, meios eficazes para obtenção de informações de usuários e dados de tráfego, cooperação imediata em emergências, ferramentas de assistência mútua, bem como salvaguardas para a preservação dos direitos humanos no ambiente digital.

O contexto de criação do segundo protocolo adicional é, no entanto, relativamente mais complexo do que o primeiro. Com vistas a oferecer suplementos para o texto da convenção de Budapeste, o TC-Y criou dois grupos Ad Hocs dedicados exclusivamente ao acesso fronteiriço a dados e questões de jurisdição territorial (*Transborder Group*, criado em 2012[20]) e acesso a dados armazenados em nuvens (*Cloud Evidence Group*, criado em 2015[21]). No ano de 2016, o final das discussões do *Cloud Evidence Group* acabou por concluir que existia uma dita dificuldade dos Estados em obter acesso a dados privados em função de questões como territorialidades, computação em nuvem e alcance de jurisdições.[22] Em função das limitações discutidas no colegiado, a conclusão acabou sendo pela elaboração de um novo protocolo adicional que foi discutido entre os anos de 2017 a 2021.

18 Conselho da Europa. New Treaties. Disponível em: https://www.coe.int/en/web/conventions/new-treaties

19 Conselho da Europa. Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. 2022. Disponível em: https://rm.coe.int/1680a49c9d

20 Conselho da Europa. Transborder Ad Hoc Group. Disponível em: https://www.coe.int/en/web/cybercrime/tb

21 Conselho da Europa. Cloud Evidence Ad Hoc Group. Disponível em: https://www.coe.int/en/web/cybercrime/ceg

22 inCyber. [Budapest Convention] A second protocol to fight cybercrime. Dezembro, 2021. Disponível em: https://incyber.fr/en/budapest-convention-a-second-protocol-to-fight-cybercrime/

O segundo protocolo é estruturado da seguinte forma:

Tabela 2 - Resumo do Segundo Protocolo Adicional à Convenção de Budapeste

Temas[23]	Artigos
Disposições gerais	Capítulo I - Disposições Gerais
Cooperação aprimorada	Capítulo II - Medidas para o aprimoramento da cooperação — Seção I - Princípios Gerais — Seção II - Procedimentos para a melhoria da cooperação com provedores de serviços e outras partes — Seção III - Procedimentos para a melhoria da cooperação internacional entre autoridades para o compartilhamento de dados — Seção IV - procedimentos sobre Assistência Mútua — Seção V - Procedimentos relativos a atividades de cooperação internacional na ausência de acordos internacionais
Condições, Salvaguardas e direitos	Capítulo III - Condições e Salvaguardas — Proteção de dados pessoais — Salvaguardas — Principios Gerais
Disposições Finais e questões procedimentais	Capítulo IV - Efectos del Protocolo, firma, reservas, etc.

23 Conselho da Europa. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. 2022. Disponível em: https://rm.coe.int/1680a49dab

De acordo com o CoE, o segundo protocolo surge como uma atualização necessária para tornar a Convenção de Budapeste um instrumento mais eficiente ao passo que revisita questões como acesso transfronteiriço a dados e cooperação legal mútua, e estabelece parâmetros mais claros para cooperação direta entre autoridades e provedores de serviços digitais - inclusive no nível dos provedores de serviços referentes a infraestrutura da internet.[24]

No entanto, nos últimos anos o debate em torno do segundo protocolo adicional tem mobilizado vários setores, em especial a sociedade civil internacional, em função da tentativa do Comitê Europeu de estabelecer regras novas de aplicação da lei que seguem na contramão dos princípios de proteção de dados pessoais e privacidade.[25]

O texto do segundo protocolo adicional foi objeto de grande mobilização da sociedade e várias cartas que reivindicavam questões como mais espaço para uma participação qualificada dos setores interessados, mais tempo para a discussão do texto, entre outras. Em abril de 2018, 94 organizações da sociedade civil assinaram uma carta solicitando mais transparência para as negociações do segundo Protocolo adicional, e que o Comitê convidasse especialistas da sociedade civil para participar das discussões e processo de elaboração do texto.[26] Para as organizações, além da ausência de transparência e devidas garantias de participação no processo, era preocupante a tentativa do Segundo Protocolo Adicional de padronização do acesso transfronteiriço a dados pessoais por autoridades policiais e judiciais.

Em maio de 2021, foram publicadas mais cartas da sociedade civil sobre o processo. A primeira, de 06 de maio, trazia alertas a respeito do ritmo açodado das discussões nas últimas rodadas de elaboração do texto, e que a ausência de tempo hábil para analisar e revisar o texto era um fator que limitava a participação qualificada do setor.[27] No final do mesmo mês, uma nova carta assinada por 43 organizações da sociedade civil – inclusive a Derechos Digitales e várias organizações

---

24 CCDCOE. Battling Cybercrime Through the New Additional Protocol to the Budapest Convention. 2021. Disponível em: https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/

25 Electronic Frontier Foundation. Global Law Enforcement Convention Weakens Privacy & Human Rights. Junho, 2021. Disponível em: https://www.eff.org/deeplinks/2021/06/global-law-enforcement-convention-weakens-privacy-human-rights

26 Global civil society letter to the Council of Europe: Cybercrime negotiations and transparency. Abril, 2018. Disponivel em: https://edri.org/files/letter-cybercrimenegotiations-and-transparency_20180403_EN.pdf

27 Carta da Sociedade Civil. 6th round of consultation on the Cybercrime Protocol and civil society participation. Maio, 2021. Disponível em: https://rm.coe.int/0900001680a25788

latino-americanas – foi enviada ao Comitê de Ministros do CoE reivindicando mais tempo para uma análise qualificada do rascunho final do texto antes do encerramento do processo de consultas aos setores interessados.[28]

Apesar dos reiterados pedidos por mais transparência e ampla participação da sociedade civil nas negociações do texto[29], o texto foi disponibilizado em consulta pública por apenas duas semanas e após a coleta de inputs foi finalizado - mais um fator que demonstra a pressa do debate e baixa adesão às demandas colocadas pela sociedade civil.[30]

Sobre o ponto da participação setorial no processo de elaboração do segundo protocolo adicional, vale mencionar que a avaliação de organizações como a *Electronic Frontier Foundation* é que - apesar da realização de consultas periódicas do TC-Y com a participação dos setores interessados[31] - o processo teria falhado ao cumprir com princípios multissetoriais de transparência, accountability e inclusão.[32] O monitoramento de acordos e negociações deste tipo por parte de diferentes setores é fundamental para assegurar que sejam ouvidas e consideradas as diversas preocupações em relação à atenção aos direitos humanos a partir do contexto e experiência de implementação da Convenção em cada país.

O texto, aprovado em 17 de dezembro de 2021, tem previsão de ser disponibilizado para a adesão de signatários em maio de 2022.

---

28 Carta da Sociedade Civil. Ensuring Meaningful Consultation in Cybercrime Negotiations. Abril, 2021. Disponível em: https://www.eff.org/files/2021/06/07/final_letter_-_council_of_europe-final.pdf

29 Electronic Frontier Foundation. Nearly 100 Public Interest Organizations Urge Council of Europe to Ensure High Transparency Standards for Cybercrime Negotiations. Abril, 2018. Disponível em: https://www.eff.org/deeplinks/2018/03/nearly-100-public-interest-organizations-urge-council-europe-ensure-high

30 Access Now. Comments on the draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, available at: https://rm.coe.int/0900001680a25783; EDPB, contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime. Disponível em: https://edpb.europa.eu/system/files/2021-05/edpb_contribution052021_6throundconsultations_budapestconvention_en.pdf.

31 Conselho da Europa. Consultations with civil society, data protection authorities and industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime 6th round of consultations [closed]. Disponível em: https://www.coe.int/en/web/cybercrime/protocol-consultations

32 Electronic Frontier Foundation. Civil Society Groups Seek More Time to Review, Comment on Rushed Global Treaty for Intrusive Cross Border Police Powers. Junho, 2021. Disponível em: https://www.eff.org/deeplinks/2021/06/civil-society-groups-seek-more-time-review-comment-rushed-global-treaty-intrusive

III. A Convenção de Budapeste nos países da América Latina e discussões correntes sobre o tema

a. Argentina

A adesão da Argentina à Convenção de Budapeste foi realizada mesmo ante os alertas da sociedade civil e academia sobre a amplitude e ambiguidade do texto e suas considerações sobre os riscos que representava às atividades de pesquisa de segurança informática desenvolvidas no país.[33] Especialistas no país alertaram sobre um aumento da insegurança jurídica para a realização de atividades de investigação penal no campo dos cibercrimes em função de dispositivos abertos e genéricos presentes, também na Lei n. 26.388, de delitos informáticos, uma vez que ambos os textos não estão ilesos de interpretações arbitrárias e potencial abuso por parte de autoridades.[34]

Apesar dos alertas, em 2018, na ocasião da sanção da Lei n. 27.411[35], o País internalizou os dispositivos da Convenção de Budapeste em seu ordenamento jurídico. A adesão argentina, porém, foi feita com ressalvas em função de dispositivos que representavam potencial conflito com a legislação nacional. Deixa de fora, portanto, dispositivos majoritariamente

33 Infobae. Argentina se suma a la Convención de Budapest para tratar delitos informáticos. Junho, 2018. Disponível em: https://www.infobae.com/tecno/2018/05/13/argentina-se-suma-a-la-convencion-de-budapest-para-tratar-delitos-informaticos/

34 Infobae. Argentina se suma a la Convención de Budapest para tratar delitos informáticos. Junho, 2018. Disponível em: https://www.infobae.com/tecno/2018/05/13/argentina-se-suma-a-la-convencion-de-budapest-para-tratar-delitos-informaticos/

35 Presidencia de la Nación. Argentina. Ley 27411, Convenio sobre ciberdelito del Consejo de Europa. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798

relacionados a medidas relativas a pornografia infantil e questões jurisdicionais (os seguintes dispositivos: 6.1.b[36], 9.1.d[37], 9.2.b[38], 9.2.c[39], 9.1.e[40], 22.1.d[41] e 29.4[42]).

O país tem reportado uma participação ativa no Comitê T-CY e celebrou a aprovação do 2º Protocolo Adicional da Convenção de Budapeste ao declarar que "para prevenir e processar o crime cibernético, é essencial ter mecanismos e instrumentos adequados que permitam e facilitem a cooperação e assistência internacional."[43]

---

36 *Article 6 – Misuse of devices*
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:(...)
B. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches

37 *Article 9 – Offences related to child pornography*
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:(...)
D. procuring child pornography through a computer system for oneself or for another person;

38 *Article 9 – Offences related to child pornography*
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:(....)
B. a person appearing to be a minor engaged in sexually explicit conduct;

39 *Article 9 – Offences related to child pornography*
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:(....)
C. realistic images representing a minor engaged in sexually explicit conduct

40 *Article 9 – Offences related to child pornography*
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:(...)
E. possessing child pornography in a computer system or on a computer-data storage medium.

41 *Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:(..)*
D. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

42 *Article 29 – Expedited preservation of stored computer data*
4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

43 Ministerio de Seguridad. Ciberdelito: Se aprobó el texto del 2° Protocolo Adicional del Convenio de Budapest. Argentina. Maio, 2021. Disponível em: https://www.argentina.gob.ar/noticias/ciberdelito-se-aprobo-el-texto-del-2deg-protocolo-adicional-del-convenio-de-budapest

Tabela 3 - Quadro-resumo - Argentinaa

O país é parte ou observador? Parte[44]

Data de adesão e ratificação? Tratado ratificado em 05 de junho de 2018, e com data de entrada em vigor da convenção a partir de 01 de outubro do mesmo ano.

Apresentou Reservas? Sim, a lei argentina que internaliza os dispositivos do tratado deixa de fora dispositivos majoritariamente relacionados a medidas relativas a pornografia infantil e questões jurisdicionais (os seguintes dispositivos:: 6.1.b[45], 9.1.d[46], 9.2.b[47], 9.2.c[48], 9.1.e[49], 22.1.d[50] e 29.4[51]).[52]

---

44 Conselho da Europa. Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

45 *Article 6 – Misuse of devices*
1.Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:(...)
B. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

46 *Article 9 – Offences related to child pornography*
1.Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:(...)
D. procuring child pornography through a computer system for oneself or for another person;

47 *Article 9 – Offences related to child pornography*
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:(....)
B. a person appearing to be a minor engaged in sexually explicit conduct;

48 *Article 9 – Offences related to child pornography*
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:(....)
C. realistic images representing a minor engaged in sexually explicit conduct

49 *Article 9 – Offences related to child pornography*
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:(...)
E. possessing child pornography in a computer system or on a computer-data storage medium.

50 *Article 22 – Jurisdiction*
1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:(..)
D. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

51 *Article 29 – Expedited preservation of stored computer data*
4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

52 Conselho da Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185). Disponível em: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=ARG

Tabela 3 - Quadro-resumo - Argentina

O país possui uma Lei própria sobre combate a cibercrimes e cooperação internacional? Desde qual ano? Atualmente o país possui um conjunto de leis e regras a respeito do ambiente digital, e que lidam com questões relativas à Proteção de Dados pessoais, tipificações de condutas praticadas no ambiente digital, proteção à propriedade intelectual e uma lei adicional, conforme descrito acima, que aprova o texto da Convenção de Budapeste e dita os caminhos para a sua aplicação. Leis relevantes: a. Lei 25.326[53] Lei de Proteção de Dados Pessoais, b. Lei 26.388[54], Alterações ao Código Penal , c. Lei 27.411[55], Aprova o texto da Convenção de Budapeste e d. Lei 11.723[56], Lei de Propriedade Intelectual.

53 Presidencia de la Nación. Argentina. Ley 25.326, Protección de Los Datos Personales. Infoleg. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

54 Presidencia de la Nación. Argentina. Ley 27411, Convenio sobre Ciberdelito del Consejo de Europa. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

55 Presidency of the Nation. Argentina. Law 27411, Council of Europe Convention on Cybercrime. Available at: https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798

56 Presidencia de la Nación. Argentina. Ley 11.723 - Régimen Legal de la Propiedad Intelectual. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

b. Brasil

Apesar de ser há mais de 20 anos uma demanda de setores como Ministérios, agências governamentais, Ministério Público e uma parte do Congresso Nacional, a adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético somente foi aprovada em dezembro de 2021[57] e aguarda o início do processo de implementação.

Discussões em torno do tema tem sido bastante presentes no cenário legislativo brasileiro e antecedem a aprovação de leis chave sobre o ambiente digital promulgadas no país como o Marco Civil da Internet[58] e a Lei Geral de Proteção de Dados Pessoais[59], bem como algumas leis ordinárias[60] que implicaram em alterações ao Código Penal Brasileiro para incluir tipificações sobre crimes cibernéticos. Nos anos 2000, um projeto de lei substitutivo a outros projetos de lei referentes a crimes na área de informática apresentado pelo Senador Eduardo Azeredo (PL da Câmara nº 89, de 2003[61]) já tentava promover algum nível de harmonização entre as tipificações e discussões presentes na Convenção de Budapeste contra o Cibercrime. Esse texto foi arduamente combatido por entidades da sociedade civil, ativistas e academia em função das tipificações genéricas e ambivalentes que tentava introduzir no ordenamento jurídico brasileiro. Em resposta, foi proposta uma lei orientada à proteção e garantia de direitos no ambiente digital que resultaria, em 2011, no envio de uma das primeiras versões do texto do Marco Civil da Internet[62] à Câmara dos Deputados.[63]

---

57 Governo Federal, Ministério da Justiça e Segurança Pública. Aprovada adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético. Dezembro, 2021. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/aprovada-adesao-do-brasil-a-convencao-de-budapeste-sobre-o-crime-cibernetico

58 Presidência da República do Brasil. Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Abril, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

59 Presidência da República do Brasil. Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD). Agosto, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

60 Exemplos relevantes de atualizações realizadas nos últimos anos na legislação penal brasileira para lidar com combate aos crimes cibernéticos são a lei 12.737, de 30 de novembro de 2012, e a Lei n. 14.155, de 27 de maio de 2021.

61 Safernet Brasil. PL sobre Crimes Cibernéticos: Projeto de Lei Substitutivo do Senador Eduardo Azeredo (PSDB-MG). Disponível em: https://www.safernet.org.br/site/institucional/projetos/obsleg/pl-azeredo

62 Câmara dos Deputados. Projeto de lei n. 2126/2011, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255

63 Brito Cruz, Francisco de Carvalho. Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet. Dissertação de mestrado. Faculdade de Direito da Universidade de São Paulo. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2019/04/dissertacao_Francisco_Carvalho_de_Brito_Cruz.pdf. Arnoudo, Daniel. O Brasil e o Marco Civil da Internet. Instituto Igarapé. Disponível em: https://igarape.org.br/marcocivil/pt/.

Ainda sobre o Marco Civil da Internet, vale destacar que o texto continuou prosperando como a principal legislação sobre Internet no país, especialmente em função da sua abordagem baseada nos direitos dos usuários da Internet e também por sua elaboração ter contado com a participação dos mais diversos setores da sociedade brasileira. Sobre o tema específico de investigações online e guarda de dados, o MCI traz dispositivos sobre guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet. Em 2018, seguindo o exemplo de elaboração normativa com a participação da sociedade, o país aprovou a lei n. 13.709/2018, ou a Lei Geral de Proteção de Dados Pessoais[64], responsável por estabelecer regras básicas para a execução das atividades de tratamento de dados pessoais no país.

No judiciário, um julgamento pelo Supremo Tribunal Federal (STF) vai selar uma controvérsia sobre o Acordo de Assistência Judiciário-Penal (MLAT), firmado entre Brasil e Estados Unidos. A dúvida a ser decidida pelo STF é se as autoridades brasileiras, inclusive o judiciário, poderiam pedir diretamente às empresas de tecnologia no exterior dados e informações, dessa forma, dispensando os procedimentos de cooperação jurídica internacional para obtenção de conteúdos de aplicativos na internet que estejam no exterior. Em 2020, o STF realizou uma audiência pública para ouvir especialistas sobre o tema[65], quando se fez referência em vários momentos a conceitos trazidos pela Convenção de Budapeste, assim como à necessidade de respeito aos direitos humanos.[66]

No final de 2019, o país recebeu o convite para ser signatário da Convenção com um prazo máximo de 3 anos para completar o processo. Menos de 2 anos depois, em dezembro de 2021, foi promulgado o Decreto Legislativo n. 37 de 2021[67] , que “Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001”, sem sugestões de reservas ao texto da Convenção.

64 Presidência da República do Brasil. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

65 STF. Audiência pública n. 29. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf

66 O caso está marcado para julgamento em maio de 2022. STF. ADC 51. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379

67 Senado Federal. Projeto de Decreto Legislativo n. 255 de 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/150258

Apesar de celebrado por algumas autoridades governamentais e pelo setor privado[68], o processo levantou muitas preocupações da sociedade civil brasileira[69]–[70] a respeito de temas como (i) a aprovação em prazo menor do que o previsto; (ii) celebração sem quaisquer discussões multissetoriais sobre o tema; (iii) a ausência de uma lei geral de proteção de dados dedicada às atividades de persecução penal e segurança pública[71]; e (iv) ter sido aprovado durante o processo de rediscussão do Código de Processo Penal brasileiro que contém seções dedicadas exclusivamente a regulação das atividades de investigação online, coleta de dados e cooperação entre autoridades e empresas.

Adicionalmente, outro ponto chave questionado foi o caráter de adesão total e irrestrito à Convenção, ignorando dispositivos do Tratado sobre a "necessidade de alinhamento entre seu conteúdo e as normas internas dos signatários e com instrumentos internacionais de direitos humanos"[72] e mecanismos como declarações (art. 40 da Convenção) e reservas (art. 42). Tais mecanismos existem justamente para facilitar o processo de conformidade doméstica e fomentar o exercício da soberania de cada país que desejar integrar o grupo de signatários. Nesse sentido, a celeridade sob a qual o processo de adesão do Estado brasileiro foi realizado é um fator de muita preocupação, uma vez que pode ter inviabilizado quaisquer análises de conformidade com o ordenamento jurídico brasileiro em face de legislações que foram aprovadas no país nos últimos anos.

Abaixo segue uma tabela destacando pontos de dois dos principais projetos de lei em trâmite no Congresso Brasileiro sobre temas relacionados à Convenção de Budapeste:

68 Brasscom. Empresas de tecnologia defendem a adesão do Brasil à Convenção de Budapeste. Disponível em: https://brasscom.org.br/empresas-de-tecnologia-defendem-adesao-do-brasil-a-convencao-de-budapeste/

69 Coalizão Direitos na Rede. Carta aos membros do Senado Federal sobre a Convenção de Budapeste. Outubro, 2021. Disponível em: https://direitosnarede.org.br/2021/10/21/carta-aos-membros-do-senado-federal-sobre-a-convencao-de-budapeste/

70 Rodrigues, Gustavo. A Convenção de Budapeste sobre o Cibercrime e as controvérsias sobre a adesão brasileira. Instituto de Referência em Internet e Sociedade, IRIS. Novembro, 2021. Disponível em: https://irisbh.com.br/a-convencao-de-budapeste-sobre-o-cibercrime-e-as-controversias-sobre-a-adesao-brasileira/

71 Eilberg, Daniela e outros. Os cuidados com a Convenção de Budapeste. Jota. Julho, 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

72 Artigo 15, da Convenção de Budapeste sobre o Cibercrime.

Tabela 4 - Projetos de Lei no Brasil	
Projetos de Lei	**Pontos relevantes**
PL 2630/2020, que Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet [73]	— Determina que os provedores de aplicações na Internet que atuam no Brasil devem ter sede e nomear representantes legais no país.[74] — Cria um novo tipo penal sobre a promoção ou financiamento do uso de contas automatizadas e outros meios para a disseminação de conteúdo inverídico (desinformação) ou passível de sanção criminal.
PL 8045/10, que trata do Código de Processo Penal [75]–[76]	— Cria alternativas para o tema de medidas cautelares como a utilização de mecanismos tal qual o monitoramento eletrônico e bloqueio de endereço eletrônico.[77] — Visa aumentar as hipóteses de cabimento de interceptação telefônica. — Altera a parte sobre provas eletrônicas, permitindo o monitoramento de investigados, interceptação de dados em repouso e outros. — Aborda hipóteses de cooperação jurídica internacional para a instrução ou produção de provas.

Além dos projetos de lei destacados acima, vale dizer que o país também tem analisado a possibilidade de elaboração e aprovação de uma Lei Geral de Proteção de Dados Pessoais aplicável ao campo da segurança pública[78]. Um anteprojeto de lei foi elaborado por uma comissão de juristas criada pelo presidente da Câmara dos Deputados[79] e foca uma parte considerável das suas disposições na dicotomia entre o estabelecimento de salvaguardas e garantias proteção de direitos dos indivíduos versus a realização de investigações no ambiente digital. Contudo, esse anteprojeto ainda não foi apresentado como projeto de lei.

---

73 Câmara dos Deputados. Projeto de lei n. 2630/2020, que Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Abril, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2256735

74 Relatório do Grupo de Trabalho destinado a elaborar parecer ao Projeto de Lei n. 2630/2020. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/aperfeicoamento-da-legislacao-brasileira-internet/documentos/outros-documentos/relatorio-adotado-do-grupo-de-trabalho

75 Câmara dos Deputados. Projeto de lei n. 8045/10, que trata do Código de Processo Penal, Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

76 Câmara dos Deputados. Parecer do relator da Comissão Especial de análise do projeto de lei do Código de Processo Penal, João Campos. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1998270&filename=Parecer-PL804510-26-04-2021

77 Câmara dos Deputados. Veja os principais pontos da reforma do Código de Processo Penal. Disponível em: https://www.camara.leg.br/noticias/210377-veja-os-principais-pontos-da-reforma-do-codigo-de-processo-penal/

78 Supremo Tribunal de Justiça. Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. Novembro, 2021. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx

79 O Anteprojeto de Lei, na versão apresentada pela Comissão de Juristas, pode ser acessado aqui: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf

Tabela 5 - Quadro-resumo - Brasil

O país é parte ou observador? Atualmente o país tem o status de observador da Convenção. No entanto, o convite para adesão chegou em 2019.[80]

Data de adesão e ratificação? O processo de Adesão foi formalizado pelo Congresso Brasileiro em dezembro de 2021 com a edição do Decreto Legislativo n. 37 de 2021[81]. A data de ratificação ainda não está confirmada, pois o processo depende de uma última fase de atuação do executivo e confirmação da ratificação.

Apresentou Reservas? Não.

O país possui uma Lei própria sobre combate a cibercrimes e cooperação internacional? Desde qual ano? Sim, desde 1999 o país tem debatido a criação de uma lei dedicada exclusivamente ao combate de crimes cibernéticos. Apesar do projeto de lei 84/99 (PL Azeredo) ter sido o primeiro a ser debatido de forma mais categórica, atualmente o país tem um conjunto de leis sobre o tema de combate a cibercrimes:

— Lei 14.197/2021 - Lei de Defesa do Estado Democrático de Direito[82]
— Lei 12.737/2012 - Dispõe sobre a tipificação criminal de delitos informáticos[83]

Debates atuais importantes sobre cibercrimes, cooperação internacional e fluxos de dados para fins de condução de investigações?
— PL 8045/10, que altera o Código de Processo Penal[84]
— Debates em torno de uma PL para uma Lei Geral de Proteção de Dados para a Segurança Pública, ainda não apresentado mas que contou com um grupo de trabalho de juristas no congresso.[85]

80 Conselho da Europa. Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

81 Diário Oficial. Decreto Legislativo n. 37 de 2021. Dezembro, 2021. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/12/2021&jornal=515&pagina=7&totalArquivos=188

82 Presidência da República do Brasil. Lei nº 14.197, de 1º de setembro de 2021, que Acrescenta o Título XII na Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), relativo aos crimes contra o Estado Democrático de Direito; e revoga a Lei nº 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), e dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Setembro, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14197.htm#:~:text=359%2DR.,a%208%20(oito)%20anos

83 Presidência da República do Brasil. Lei nº 12.737, de 30 de novembro de 2012, que Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Novembro, 2012. Disponível em: http://planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

84 Câmara dos Deputados. Projeto de Lei n. 8045/2010, sobre o Código de Processo Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

85 Supremo Tribunal de Justiça. Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. Novembro, 2021. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx

c. Chile

A adesão do Chile à Convenção de Budapeste foi formalizada ao Conselho da Europa em abril de 2017, dias antes da promulgação do Decreto n. 83/2017, que "*promulga el convenio sobre la ciberdelincuencia*".[86] A necessidade de reforçar o compromisso assumido em nível nacional de garantir a segurança cibernética no país (via Política Nacional de Cibersegurança) e ser parte de um sistema rápido e eficaz de cooperação internacional, bem como estabelecer canais de troca de conhecimento sobre o combate aos crimes cibernéticos estão entre as principais razões alegadas pelo Governo Chileno para a adesão ao tratado.[87]

A respeito das reservas apresentadas, vale mencionar que no caso chileno o documento de acesso a Convenção de Budapeste depositado no Conselho da Europa deixou de fora, dispositivos majoritariamente relacionados a medidas relativas à possibilidade de aplicação da lei doméstica, pornografia infantil e questões jurisdicionais (os seguintes dispositivos: 6.1[88], 9.2.b[89], 9.2.c[90], 9.4[91], 22.1.b[92] e 29.4[93]). Assim como a Argentina, o país também se reserva o direito de recusar pedidos de assistência internacional em casos onde a conduta não é tipificada na lei chilena.

---

86 BCN Chile. Decreto 83, promulga el convenio sobre la ciberdelincuencia. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=1106936

87 Ministério de Relações Exteriores do Chile. Chile deposita el instrumento de adhesión al Convenio de Budapest sobre la Ciberdelincuencia. Abril, 2017. Disponível em: https://www.minrel.gov.cl/chile-deposita-el-instrumento-de-adhesion-al-convenio-de-budapest-sobre/minrel_old/2017-04-21/175923.html

88 *Article 6 – Misuse of devices*
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right

89 *Article 9 – Offences related to child pornography*
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: (...)
B. a person appearing to be a minor engaged in sexually explicit conduct; c. realistic images representing a minor engaged in sexually explicit conduct.

90 *Article 9 – Offences related to child pornography*
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: (...)
C. realistic images representing a minor engaged in sexually explicit conduct.

91 *Article 9 – Offences related to child pornography*
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d and e, and 2, sub-paragraphs b and c.

92 *Article 22 – Jurisdiction*
1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:(..)
B. on board a ship flying the flag of that Party; or

93 *Article 29 – Expedited preservation of stored computer data*
4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

Importante mencionar que recentemente o país aprovou um projeto de lei dedicado à modernização da Lei 19223/92, que "tipifica condutas penais relativas à informática, criando novos delitos". O texto do projeto de lei em questão se dedica, também, a atualizar outros textos legais vigentes no país com o objetivo de promover um melhor nível de adequação à Convenção de Budapeste.[94]

Conforme exposto, o Projeto de Lei, Boletim n. 12.192-25[95], estabelece regras sobre crimes de informática, revoga a Lei n. 19.223 e modifica outros órgãos jurídicos para adaptá-los à Convenção de Budapeste. O texto tem recebido bastante pressão por parte do Governo para uma célere aprovação.[96] Dentre os pontos rechaçados na etapa final de discussão do texto se encontrava a possibilidade de modificação do Código Penal para permitir que o Ministério Público pudesse solicitar dados de cidadãos a qualquer momento, sem ordem judicial ou mecanismo específico de transparência e prestação de contas, o que foi fortemente contestado por representantes da sociedade civil, academia e associações empresariais.[97]

94 Senado de la República de Chile. Proyecto que moderniza normas sobre delitos informáticos será analizado por una Comisión Mixta. Outubro de 2021. Disponível em: https://www.senado.cl/proyecto-que-moderniza-normas-sobre-delitos-informaticos-sera-analizado

95 Boletín 12192-25, que estabelece regras sobre crimes de informática, revoga a Lei nº 19.223 e modifica outros órgãos jurídicos para adaptá-los à Convenção de Budapeste. Disponível em: http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=12192-25

96 Derechos Digitales. En rechazo a la modificación del Código Procesal Penal que habilita la vigilancia sin controles ni contrapesos legales. Janeiro, 2022. Disponível em: https://www.derechosdigitales.org/17623/en-rechazo-a-la-modificacion-del-codigo-procesal-penal-que-habilita-la-vigilancia-sin-controles-ni-contrapesos-legales/

97 Derechos Digitales. En rechazo a la modificación del Código Procesal Penal que habilita la vigilancia sin controles ni contrapesos legales. Janeiro, 2022. Disponível em: https://www.derechosdigitales.org/17623/en-rechazo-a-la-modificacion-del-codigo-procesal-penal-que-habilita-la-vigilancia-sin-controles-ni-contrapesos-legales/

Tabela 7 - Projetos de Lei no Chile	
Projeto de Lei	**Pontos relevantes**
PL 12192-25, que "busca modificar a norma vigente (Lei n.19.223) que tipifica condutas relativas à sistemas informáticos".	— Visa promover um maior nível de adequação entre a legislação chilena dedicada ao combate de cibercrimes e a Convenção de Budapeste; — Promovia mudanças processuais, rechaçadas, que incluíam: * Uma relativa redução do controle das atividades estatais de investigação ao passo que visava introduzir mecanismos de solicitação de dados de cidadãos sem salvaguardas suficientes; * Uma flexibilização de medidas investigativas invasivas vigentes no sistema penal chileno, entre elas uma alteração ao artigo 219 do Código de Processo Penal que fala sobre interceptação de comunicações privadas; * Alternativas para introduzir no sistema processual penal chileno a possibilidade de coleta de dados de indivíduos sem uma ordem judicial específica que autorize o ato.

As mudanças propostas e rechaçadas para a legislação chilena no caso do PL12.192-25 seguiam, portanto, uma tendência preocupante de instrumentalização do processo de adequação à Convenção de Budapeste como uma desculpa para reduzir o controle e transparência das atividades de investigação do estado, tendendo à violação da privacidade dos cidadãos.

Tabela 8 - Quadro-resumo - Chile

O país é parte ou observador? Parte.[98]
Data de adesão e ratificação? Tratado ratificado em 20 de abril de 2017 e com entrada em vigor da convenção a partir de primeiro de agosto do mesmo ano.
Apresentou Reservas? Sim, no documento de acesso chileno a Convenção de Budapeste deixou de fora, dispositivos majoritariamente relacionados a medidas relativas à possibilidade de aplicação da lei doméstica, pornografia infantil e questões jurisdicionais (artigos 6.1[99], 9.2.b[100], 9.2.c[101], 9.4[102], 22.1.b[103] and 29.4[104]). JAssim como a Argentina, o país também se reserva o direito de recusar pedidos de assistência internacional em casos em que a conduta não é tipificada na lei chilena.[105]
O país possui uma Lei própria sobre combate a cibercrimes e cooperação internacional? Desde qual ano? Lei 19223/92, que tipifica figuras penais relativas a crimes informáticos.[106]
Debates atuais importantes sobre cibercrimes, cooperação internacional e fluxos de dados para fins de condução de investigações? PL n. 12.192-25, que estabelece regras sobre crimes de informática, revoga a Lei n. 19.223 e modifica outros órgãos jurídicos para adaptá-los à Convenção de Budapeste[107] - [108], aprovado em março de 2022.

98 Conselho da Europa. Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

99 *Article 6 – Misuse of devices*
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right

100 *Article 9 – Offences related to child pornography*
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: (...)
B. a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct.

101 *Article 9 – Offences related to child pornography*
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: (...)
C. realistic images representing a minor engaged in sexually explicit conduct.

102 *Article 9 – Offences related to child pornography*
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d and e, and 2, sub-paragraphs b and c.

103 *Article 22 – Jurisdiction*
1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:(..)
B. on board a ship flying the flag of that Party; or

104 *Article 29 – Expedited preservation of stored computer data*
4. A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

105 Conselho da Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185) - Chile. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=Chi

106 Biblioteca del Congreso Nacional de Chile. Ley 19223 Tipifica figuras penales relativas a la Informatica. May, 1993. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=30590

107 Camara de Diputadas y Diputados de Chile. Proyecto de Ley Modifica la ley N° 19.223 que Tipifica Figuras Penales Relativas a la Informática incorporando un nuevo delito. Disponível em: https://www.camara.cl/verDoc.aspx?prmID=14367&prmTIPO=INICIATIVA

108 https://noticias.usm.cl/2021/10/15/ley-de-delitos-informaticos/

d. Colômbia

No caso colombiano, a discussão e elaboração de políticas públicas para temas afetos a crimes cibernéticos têm favorecido perspectivas relativas à defesa e segurança cibernética e visa facilitar o uso de informações em processos judiciais e para prevenir ou antecipar a consumação de crimes cibernéticos, como aponta a *Fundación Karisma.*[109] Em 2018, a organização apontava que o país necessitava de uma política pública para matérias criminais mais compreensiva e precisava resolver as precariedades presentes na Lei n. 1.273/2009[110] - que institui no país a noção de preservação de dados e sistemas de informação, assim como comunicações - antes de avançar nas negociações sobre aderir à Convenção de Budapeste.

No entanto, o país promulgou a Lei n. 1928, de 24 de julho de 2018, que aprova o texto da Convenção de Budapeste sobre o Cibercrime.[111] Já o instrumento de adesão à Convenção de Budapeste foi depositado ante o Conselho da Europa em março de 2020.[112] No caso colombiano, as reservas apresentadas tratam da possibilidade do país aplicar as medidas mencionadas nos artigos 20 (coleta em tempo real de dados em trânsito) e 21 (interceptação de dados de conteúdo) da Convenção de acordo com seu regulamento interno em matéria de dados pessoais e proteção do direito à privacidade.

Dentre as motivações apontadas pelo governo para a adesão estavam o crescimento da incidência dos crimes cibernéticos nos primeiros meses da pandemia da Covid-19 e a necessidade de mais instrumentos para lidar com cibercrimes por meio da cooperação internacional entre países.[113] A facilitação de investigação de cibercrimes de natureza transnacional por meio da

109 Derechos Digitales and Fundación Karisma. Convenio de Budapest; Aplicación en Colombia frente a derechos humanos. Junho de 2018. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/minuta_karisma.pdf

110 Universidad Técnica Federico Santa María. Ley de delitos informáticos. Outubro, 2021. Disponível em: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

111 Vlex. Ley 1928 del 24 de Julio de 2018 Senado. Julho, 2018. Disponível em: https://vlex.com.co/vid/ley-1928-24-julio-737603069

112 Gobierno de Colombia, Cancillería de Colombia. Colombia se adhiere al Convenio de Budapest contra la ciberdelincuencia. Março, 2020. Disponível em: https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

113 MINTIC. Adhesión al Convenio de Budapest contra la ciberdelincuencia, clave para Colombia en tiempos de Coronavirus. 07 de abril de 2020. Disponível em: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126496:Adhesion-al-Convenio-de-Budapest-contra-la-ciberdelincuencia-clave-para-Colombia-en-tiempos-de-Coronavirus

formalização de canais de troca de informações entre os países signatários da Convenção, somada à possibilidade de acesso aos projetos e programas de acesso e transferência de conhecimento sobre os temas da Convenção foram alguns dos outros benefícios alegados pelo governo colombiano.[114]

A respeito da adequação do ordenamento jurídico colombiano à Convenção de Budapeste, no entanto, restam algumas dúvidas sobre possíveis limites e salvaguardas que poderiam ser introduzidos a fim de evitar abusos e má interpretações por parte das autoridades estatais. Nesse sentido, vale reforçar um ponto ressaltado pela Fundación Karisma sobre a necessidade de se fomentar o uso proporcional do direito penal como resposta ao cibercrime por meio da criação das leis equilibradas e o exame de tipos penais genéricos no âmbito interpretativo, a partir de normas já existentes e de padrões internacionais de direitos humanos.[115]

114 MINTIC. Adhesión al Convenio de Budapest contra la ciberdelincuencia, clave para Colombia en tiempos de Coronavirus. 07 de abril de 2020. Disponível em: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126496:Adhesion-al-Convenio-de-Budapest-contra-la-ciberdelincuencia-clave-para-Colombia-en-tiempos-de-Coronavirus

115 Derechos Digitales and Fundación Karisma. Convenio de Budapest; Aplicación en Colombia frente a derechos humanos. Junho 2018. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/minuta_karisma.pdf

Tabela 8 - Quadro-resumo - Colômbia

O país é parte ou observador? Parte, convite realizado em 2019. [116]

Data de adesão e ratificação? Data de adesão:16.03.2020, com entrada em vigor da convenção em 01 de julho de 2020.

Apresentou Reservas? Sim, as reservas apresentadas visam permitir ao país aplicar as medidas mencionadas nos artigos 20 (coleta em tempo real de dados em trânsito) e 21 (interceptação de dados de conteúdo) da Convenção de acordo com seu regulamento interno em matéria de dados pessoais e proteção do direito à privacidade.[117]

O país possui uma Lei própria sobre combate a cibercrimes e cooperação internacional? Desde qual ano?

- Lei n. 1273/2009[118]
- Lei n. 1928/2019[119]

Debates atuais importantes sobre cibercrimes, cooperação internacional e fluxos de dados para fins de condução de investigações? Em março de 2021 o Ministério das Tecnologias da informação e comunicações publicou a Resolução n. 500/2021, que estabelece "diretrizes e padrões para a estratégia de segurança digital e o modelo de segurança e privacidade como viabilizador da política de Governo Digital".[120]

116 Conselho da Europa. Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty treaty no=185

117 Conselho da Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185) - Colombia. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=COL

118 Diário Oficial, Colombia. Ley 1273 de 2009, que modifica o Código Penal. Disponível em: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

119 Vlex. Ley 1928 del 24 de Julio de 2018 Senado. Julho, 2018. Disponível em: https://vlex.com.co/vid/ley-1928-24-julio-737603069

120 Republica de Colombia, MINTIC. Resolución número 00500 de marzo 10 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital". Março, 2021. Disponível em: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

e. México

O México representa um caso particular, pois figura apenas como observador da Convenção, não tendo ainda formalizado sua adesão, apesar de ter solicitado a entrada em 2006. A ausência de formalização, porém, não impediu que a Convenção também tivesse algum nível de influência na discussão local sobre o combate aos crimes cibernéticos. Assim como nos demais países da região, denota-se no México reiteradas tentativas de transposição de dispositivos específicos para o ordenamento jurídico nacional e essa tem sido a força-motriz para projetos de lei dedicados à atualização da legislação mexicana sobre cibercrimes.

O país possui um arcabouço jurídico próprio aplicável a determinados casos de crimes cibernéticos e que é composto pelo Código Penal[121], Lei de Segurança Nacional[122] e algumas outras normas esparsas.[123]

Para os especialistas entrevistados durante a elaboração do presente relatório, haveria uma linha perigosa de legitimação dos textos da convenção e utilização da justificativa de necessidade de implementação do seu texto para a produção de leis mais duras, dedicadas a implementar mais medidas de controle e vigilância no processo penal, além de tipos penais vagos, imprecisos e amplos de maneira deliberada. Nesse sentido, no tangente à adesão do México, alguns fatores de risco apontados poderiam ser um eventual fortalecimento das capacidades e competências de um estado autoritário, e ainda mais iniciativas legislativas que acabariam por legitimar os já existentes abusos do sistema processual penal mexicano.[124] Caso o país seguisse com o processo de adesão à Convenção de Budapeste, uma atenção ainda maior de todos os setores envolvidos no tema seria necessária, especialmente para ajudar a dirimir eventuais ambiguidades entre o texto do Tratado frente ao sistema mexicano e ao Sistema Interamericano de Direitos Humanos. Alguns dos temas de atenção seriam: proteção de whistleblowers, garantia do direito à liberdade de expressão, o uso de materiais com copyright.

---

121 Justia México. Código Penal Federal. Disponível em: https://mexico.justia.com/federales/codigos/codigo-penal-federal/

122 Diário Oficial da Federação do México. Ley de Seguridad Nacional. Disponível em: http://www.ordenjuridico.gob.mx/Federal/PE/APF/APC/SEGOB/Leyes/L-11.pdf

123 Covarrubias, Jersain Llamas. El estatus de México y el Convenio sobre la Ciberdelincuencia de Budapest. Setembro, 2020. Foro Jurídico. Disponível em: https://forojuridico.mx/el-estatus-de-mexico-y-el-convenio-sobre-la-ciberdelincuencia-de-budapest/

124 Entrevista realizada com Grecia Macías e Luis Fernando Garcia, Advogada e Diretor-Executivo da Rede en Defensa de los Derechos Digitales - R3D.

Pesquisa realizada pela organização mexicana R3D com apoio da Derechos Digitales, em junho de 2018, apontou algumas incongruências persistentes entre a legislação mexicana e a Convenção, especialmente em função da insegurança jurídica gerada pelas tipificações amplas e genéricas de crimes cibernéticos dispostas no Tratado.[125] A organização aponta também que após uma eventual adesão do país à Convenção, seria necessário uma análise profunda sobre questões como competências jurisdicionais, nível e instância de implementação, e até a possível elaboração de uma nova lei especial ou modificação de leis vigentes nas entidades federativas do país a fim de promover uma maior harmonização e garantir a exata aplicação da Lei Penal.[126]

Atualmente, o país tem discutido - ao menos - 13 propostas de leis dedicadas ao campo da segurança cibernética e que se dedicam a instituir no país uma Lei de Segurança Cibernética com tipificações de condutas como delitos cibernéticos, ameaça cibernética, a criação de uma agência nacional de segurança cibernética e outras discussões.[127] Adicionalmente, vale destacar que em 2017 foi editada uma Estratégia Nacional de Segurança Cibernética (ENCS)[128] para o país, como um documento orientador do estado mexicano e que traz como objetivos principais o a. fomento da colaboração entre diferentes setores, b. a necessidade de análise e mapeamento dos riscos e ameaças no ciberespaço, c. promover o uso responsável das tecnologias da informação e comunicação, entre outros.

Ainda sobre a ENCS, vale frisar que organizações da sociedade civil - como a R3D - reforçaram a importância da adoção de uma abordagem com base em direitos humanos, e reivindicaram que a Estratégia deveria ser discutida abertamente com a sociedade justamente por propor modificações à marcos legais e jurídicos com que tipificam crimes cibernéticos, o que poderia representar uma ameaça ao exercício de liberdades e direitos na Internet.[129] Mais recentemente, o país iniciou a discussão de uma reforma constitucional em matéria de

125 Centeno, Danya. México y el Convenio de Budapest: posibles incompatibilidades. R3D y Derechos Digitales. Junho, 2018. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf

126 Centeno, Danya. México y el Convenio de Budapest: posibles incompatibilidades. R3D y Derechos Digitales. Junho, 2018. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf

127 El Economista. Expertos comparan iniciativas de ley de ciberseguridad en México. Fevereiro, 2022. Disponível em: https://www.eleconomista.com.mx/tecnologia/Expertos-comparan-iniciativas-de-ley-de-ciberseguridad-en-Mexico-20220208-0067.html

128 Governo do México. Estratégia Nacional de Ciberseguridad. 2017. Disponível em: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

129 R3D. Expertos consideran incongruente la estrategia nacional de ciberseguridad por falta de controles a la vigilancia estatal. Agosto, 2017. Disponível em: https://r3d.mx/2017/08/07/expertos-consideran-incongruente-la-estrategia-nacional-de-ciberseguridad-por-falta-de-controles-a-la-vigilancia-estatal/

cibersegurança com o objetivo de permitir que o Congresso mexicano tenha a competencia de elaborar "leis de segurança nacional, incluindo segurança cibernética e proteção dos direitos humanos no ciberespaço, estabelecendo os requisitos e limites para as investigações correspondentes".[130] Sobre o tema, organizações da sociedade civil também alertaram, em carta enviada ao Congresso Mexicano em 2021, que o texto também apresentava riscos uma vez que "a ambiguidade e amplitude do que se considera conduta que ameace a segurança nacional nos impediria de ter clareza e certeza sobre o alcance, conteúdo e limitações do exercício do poder e restrição do Estado aos direitos e liberdades da sociedade".[131]

130 Artigo 19 México, R3D, Aimée Vega Montiel – CEIICH UNAM e Laboratorio Feminista de Derechos Digitales. Reforma constitucional en materia de Ciberseguridad podría explotarse para censurar y arremeter contra manifestaciones legítimas de la sociedad. Abril, 2021. Disponível em: https://articulo19.org/reforma-constitucional-en-materia-de-ciberseguridad-podria-explotarse-para-censurar-y-arremeter-contra-manifestaciones-legitimas-de-la-sociedad/

131 Artigo 19 México, R3D, Aimée Vega Montiel – CEIICH UNAM e Laboratorio Feminista de Derechos Digitales. Reforma constitucional en materia de Ciberseguridad podría explotarse para censurar y arremeter contra manifestaciones legítimas de la sociedad. Abril, 2021. Disponível em: https://articulo19.org/reforma-constitucional-en-materia-de-ciberseguridad-podria-explotarse-para-censurar-y-arremeter-contra-manifestaciones-legitimas-de-la-sociedad/

Tabela 9 - Quadro-resumo - México
O país é parte ou observador? Observador da Convenção[132]
Data de adesão e ratificação? O país não é signatário.
Apresentou Reservas? O país não é signatário.
O país possui uma Lei própria sobre combate a cibercrimes e cooperação internacional? Desde qual ano? Sim, em 1999 o Congresso iniciou uma primeira leva de reformas ao seu Código Penal responsável por inserir o tema dos cibercrimes no texto da lei. Além disso, atualmente, o país possui dispositivos sobre o tema em seu Código Penal, Lei de Segurança Nacional e uma Estratégia Nacional de Segurança Cibernética, anunciada pelo Presidente mexicano em 2017.
Debates atuais importantes sobre cibercrimes, cooperação internacional e fluxos de dados para fins de condução de investigações? Existe um atual debate sobre uma reforma das leis que regem o Sistema Nacional de Segurança Pública sob a iniciativa da reforma constitucional em matéria de cibersegurança.[133] [134]

132 Conselho da Europa. Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

133 IT Masters Mag. Delitos informáticos en México, ¿qué dice la Ley? Setembro, 2020. Disponível em: https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/

134 Em setembro de 2019, a Comissão de Segurança Pública da Câmara dos Deputados aprovou dois pareceres para reformar as Leis Gerais do Sistema Nacional de Segurança Pública em matéria de cibersegurança e Segurança Nacional em matéria de inteligência.

IV. O debate sobre Cibercrimes além da Convenção de Budapeste

Apesar de ser um dos principais textos sobre o tema, a Convenção de Budapeste sobre o Cibercrime não é a única das iniciativas recentes discutidas mundo afora a respeito. No decorrer dos últimos anos, cada vez mais foros e espaços como a Organização das Nações Unidas (ONU), Organização para a Cooperação e Desenvolvimento Econômico (OCDE) vêm discutindo o combate aos cibercrimes e maneiras para fomentar mais canais de cooperação entre autoridades. Essas discussões incluem pensar como permitir e solicitar o acesso à dados de indivíduos investigados dentro de balizas e salvaguardas que estejam em conformidade com padrões internacionais de direitos humanos.

Em dezembro de 2019, a Assembleia Geral da ONU aprovou em uma resolução[135] a criação de um Comitê ad hoc para elaboração de um novo tratado internacional para combater os crimes cibernéticos, apesar de objeções de países como Estados Unidos e blocos como o da União Europeia.[136] A Resolução[137] determina que o Comitê será composto por especialistas de todas as regiões do mundo e buscará elaborar uma nova Convenção sobre o combate ao uso de tecnologias para fins criminais, levando em consideração os instrumentos internacionais e esforços existentes nos níveis nacional, regional e internacional.

Entidades da sociedade civil com atuação internacional expuseram preocupação com a celeridade do processo e a falta de evidências sobre sua necessidade. Em uma carta direcionada ao Comitê ad hoc em 2019, as mesmas organizações alertaram sobre a falta de um objetivo claro e bem definido para o texto do Tratado em questão, apontando que o emprego de termos e definições genéricas abre a possibilidade de criminalização de comportamentos online que atualmente são protegidos por padrões e normas de direitos humanos internacionais.[138]

---

135 Organização das Nações Unidas. Resolução da Assembleia Geral sobre o combate o uso de informações e tecnologias de comunicação para fins criminais. Dezembro, 2019. Disponível em: https://undocs.org/A/Res/74/247

136 Observador. ONU avança para tratado internacional de combate ao cibercrime com objeções da UE e EUA. Dezembro, 2019. Disponível em: https://observador.pt/2019/12/28/onu-avanca-para-tratado-internacional-de-combate-ao-cibercrime-com-objecoes-da-ue-e-eua/

137 Organização das Nações Unidas. Resolução da Assembleia Geral sobre o combate o uso de informações e tecnologias de comunicação para fins criminais. Dezembro, 2019. Disponível em: https://undocs.org/A/Res/74/247

138 Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online. Novembro, 2019. Disponível em: https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human

O tratado ventilado pela ONU é uma proposta antiga verbalizada por países como a Rússia[139] como um novo instrumento global capaz de substituir a Convenção de Budapeste. Além das preocupações sobre a origem da iniciativa - que nas suas primeiras versões também recebeu apoio da regimes autoritários como a China, Camboja e outros países.[140] Um outro ponto levantado como preocupante por entidades do terceiro setor é a falta de transparência e espaços de participação social comum nas discussões realizadas no âmbito das Nações Unidas - que segue com muitas limitações para a participação de entidades que não possuem status ECOSOC.[141]

Além dos debates realizados pela ONU, vale mencionar também as recentes discussões realizadas pela OCDE sobre acesso governamental a dados pessoais. O debate, realizado exclusivamente no âmbito do Comitê de Política de Economia Digital - CDEP e no contexto da recente revisão da implementação das Diretrizes de Privacidade de 1980 da OCDE, identificou o *acesso governamental irrestrito a dados pessoais mantidos pelo setor privado como uma questão crucial para a governança de dados e a proteção de direitos e como uma barreira potencial para permitir o livre fluxo de dados com confiança*.[142]

No entanto, em dezembro de 2021 a iniciativa que visava a elaboração de princípios de alto nível ou orientação para os países membros da OCDE a respeito de acesso governamental confiável a dados pessoais armazenados pelo setor privado foi interrompida até segunda ordem pela OCDE em função de desacordos e ausência de consenso entre os países que compõem o CDEP[143]–[144]

139 Brown, Deborah. Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. HRW. Agosto, 2021. Disponível em: https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights

140 Brown, Deborah. Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. HRW. Agosto, 2021. Disponível em: https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights

141 Carta ao Comitê AD HOC de Cybercrime. Disponível em: https://direitosnarede.org.br/2022/01/25/carta-ao-comite-ad-hoc-de-cybercrime/

142 OCDE. Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy. Dezembro, 2020. Disponível em: https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm

143 Theodore Christakis, Kenneth Propp, Peter Swire. Towards OECD Principles for Government Access to Data. Lawfare Blog. Dezembro, 2021. Disponível em: https://www.lawfareblog.com/towards-oecd-principles-government-access-data

144 Joint Business Statement on the OECD Committee on Digital Economy Policy's work to develop an instrument setting out high-level principles or policy guidance for trusted government access to personal data held by the private sector. Junho, 2021. Disponível em: https://iccwbo.org/content/uploads/sites/3/2021/05/2021-05-04-joint-business-hl-statement-on-govt-access-to-private-sector-data.pdf

Já no âmbito da Organização dos Estados Americanos (OEA), desde 1999, foi criado um Grupo de Trabalho sobre Delitos Cibernéticos pela Reunião de Ministros da Justiça ou de Outros Ministros ou Procuradores-Gerais das Américas (REMJA), um foro político e técnico em matéria de justiça e cooperação jurídica internacional. O objetivo desse Grupo de Trabalho é fortalecer a cooperação internacional na prevenção, investigação e julgamento de crimes cibernéticos, facilitar o intercâmbio de informação e experiências dos membros, além de recomendar ações necessárias para o fortalecimento da cooperação dos Estados membros nesse tema. Dentre outras, esse Grupo também promove a recomendação de adesão dos Estados à Convenção de Budapeste e estimula o desenvolvimento por parte dos Estados de estratégias nacionais sobre crimes cibernéticos.[145] Ademais de proporcionar programas de capacitação,[146] o grupo consolida o desenvolvimento do tema em cada Estado, publica um Portal Interamericano de Cooperação em Matéria de Delito Cibernético,[147] além de facilitar o intercâmbio de informações consolidadas sobre as autoridades.[148]

145 https://rm.coe.int/3148-1-1-forum-programa-de-la-conferencia-es/168076e137
146 http://www.oas.org/es/sla/dlc/cyber-es/programa-capacitacion.asp
147 https://oas.org/es/sla/dlc/cyber-es/homePortal.asp
148 https://oas.org/es/sla/dlc/cyber-es/desarrollo-pais.asp

V. Conclusão e Recomendações

O quadro de implementação e discussão dos processos de adesão em países como Chile, Brasil, Argentina, Colômbia e México tende a ser bastante semelhante em aspectos como (a) ausência de participação dos setores interessados de forma relevante, (b) rapidez na discussão de leis e decretos de promulgação sem transparência e com celeridade, (c) utilização da necessidade de adequação à Convenção de Budapeste para a promoção de reformas compreensivas da legislação penal e processual penal vigentes e que oferecem riscos para os direitos dos cidadãos como o direito à privacidade, direito à proteção de dados, e devido processo legal.

Apesar da Convenção de Budapeste ser um texto de altíssima relevância para matérias de cooperação internacional em matéria penal, o fato do texto ter sido desenvolvido em um sistema jurídico e político diferente do vigente nos países latinoamericanos torna o processo de adequação relativamente mais custoso para os países da região e requer uma atenção ainda maior a observância de padrões desenvolvidos no sistema interamericano de proteção de direitos humanos.

Nesse sentido, como parte final do presente documento, apresentamos recomendações para diferentes setores sobre os respectivos processos de adesão e implementação da Convenção de Budapeste na região, bem como sobre a participação em discussões futuras sobre temas como cooperação internacional, acesso governamental a dados de investigados e combate aos cibercrimes.

Aos Estados e governos nacionais

1. Realização de discussões multissetoriais sobre o processo de adesão dos países ao grupo de signatários da Convenção a fim de facilitar um mapeamento sobre riscos e incongruências do texto com o Ordenamento Jurídico local, bem como uma discussão franca e propositiva sobre a apresentação de possíveis reservas e o processo de implementação do Tratado Internacional;

2. Realizar uma análise de adequação da Convenção de Budapeste e de seus protocolos, de acordo com os direitos humanos e fundamentais reconhecidos pelo Estado, evitando sua utilização apenas como uma base comum para a discussão de possíveis avenidas no combate aos cibercrimes.

3. Evitar de realizar a simples cópia dos tipos penais abordados no texto da Convenção, pois gera dúvidas sobre sua aplicação;

4. Garantir o pleno respeito aos direitos fundamentais de seus cidadãos reconhecidos nas respectivas Constituições e Leis vigentes, para a aplicação da Convenção e realização de atividades de persecução penal no ambiente digital por meio do estabelecimento de salvaguardas claras e específicas;

5. Incluir todos os setores interessados em discussões futuras sobre novas tipificações para crimes cibernéticos, mecanismos de cooperação jurídica internacional, investigações e outros. O modelo de participação multissetorial deve ser levado em consideração também na discussão das questões relativas à Convenção de Budapeste, assim como na maioria dos processos de elaboração de políticas dedicadas à Internet.

6. Os países Latinoamericanos têm a obrigação de assegurar que os compromissos assumidos estejam refletidos na adesão e implementação da Convenção de Budapeste, por isso não podem, nessa discussão, ignorar as obrigações de direitos humanos que sustentam o sistema interamericano de direitos humanos.

7. Evitar a linha punitivista e preocupante do direito penal como via única. A tradição dos países da América do Sul com abusos na atividade policial e violações de direitos humanos por parte de regimes autoritários deveria ser o principal motivo para a consideração e discussão de salvaguardas para a proteção de direitos humanos no ambiente digital para o continente.

Aos setores não governamentais

8. Alertar a sociedade sobre possíveis e eventuais abusos governamentais na implementação da Convenção de Budapeste sobre o Cibercrime, bem como na execução de atividades persecução penal no ambiente Digital por parte do Estado;

9. Conduzir atividades de capacitação de cidadãos, organizações do terceiro setor e academia sobre os principais instrumentos de cooperação internacional vigentes, bem como aspectos da sua implementação.

10. Conduzir atividades de monitoramento e atuação em incidência legislativa diante da preocupante instrumentalização do processo de adequação à Convenção de Budapeste como pretexto para reduzir o controle e transparência das atividades de investigação do estado, com violações às garantias fundamentais e à privacidade dos cidadãos.

11. Documentar os processos de participação na nas discussões sobre novas tipificações para crimes cibernéticos, mecanismos de cooperação jurídica internacional, investigações e outros.

12. Explorar novas linhas de investigação e estudos complementares na América Latina sobre a importância e os desenvolvimentos regionais de formas de institucionalização de combate a cibercrimes, incluída a realização de acordos bilaterais para assistência judiciária em matéria penal (MLAT) e cooperação jurídica internacional.

Anexo I - Tabela de Análise do Status dos Países

	O país é parte ou observador?	Data de adesão e ratificação?	Apresentou Reservas?	O país possui uma Lei própria sobre combate a cibercrimes e cooperação internacional? Desde qual ano?
Argentina	Parte [149]	Tratado ratificado em 05 de junho de 2018, e com data de entrada em vigor da convenção a partir de 01 de outubro do mesmo ano.	Sim, a lei argentina que internaliza os dispositivos do tratado deixa de fora, portanto, dispositivos majoritariamente relacionados a medidas relativas a pornografia infantil e questões jurisdicionais (os seguintes dispositivos: 6.1.b, 9.1.d, 9.2.b, 9.2.c, 9.1.e, 22.1.d e 29.4) [150]-[151]	— Lei 25.326 [152], Lei de Proteção de Dados Pessoais — Lei 26.388 [153], Alterações ao Código Penal — Lei 27.411 [154], Aprova o texto da Convenção de Budapeste Convention — Lei 11.723 [155], Lei de Propriedade Intelectual

149 Conselho da Europa. Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

150 Conselho da Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185). Disponível em: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=ARG

151 Conselho da Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185). Disponível em: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=ARG

152 Presidencia de la Nación. Argentina. Ley 25.326, Protección de Los Datos Personales. Infoleg. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

153 Presidencia de la Nación. Argentina. Ley 26.388, Código Penal. Infoleg. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

154 Presidencia de la Nación. Argentina. Ley 27411, Convenio sobre ciberdelito del consejo de europa. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798

155 Presidencia de la Nación. Argentina. Ley 11.723 - Régimen legal de la propiedad intelectual. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

	O país é parte ou observador?	Data de adesão e ratificação?	Apresentou Reservas?	O país possui uma Lei própria sobre combate a cibercrimes e cooperação internacional? Desde qual ano?	Debates atuais importantes sobre cibercrimes, cooperação internacional e fluxos de dados para fins de condução de investigações?
Brasil	Atualmente o país tem o status de observador da Convenção. No entanto, o convite para adesão chegou em 2019 [156]	O processo de Adesão foi formalizado pelo Congresso Brasileiro em dezembro de 2021 com a edição do Decreto Legislativo n. 37 de 2021. [157] A data de ratificação ainda não está confirmada, pois o processo depende de uma última fase de atuação do executivo e confirmação da ratificação.	Não	Sim, desde 1999 o país tem debatido a criação de uma lei dedicada exclusivamente ao combate de crimes cibernéticos. Apesar do projeto de Lei 84/99 (PL Azeredo) ter sido o primeiro a ser debatido de forma mais categórica, atualmente o país tem um conjunto de leis sobre o tema de combate a cibercrimes: — L14197 - Lei de Defesa do Estado Democrático de Direito [158] — 12.737/2012 - Dispõe sobre a tipificação criminal de delitos informáticos. [159]	— Reforma do Código de Processo Penal [160] — Debates em torno de uma Lei Geral de Proteção de Dados para a Segurança Pública, ainda não apresentada mas que contou com um grupo de trabalho de juristas no congresso. [161] — Projeto de Lei das Fake News. [162]

156 Conselho da Europa. Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

157 Diário Oficial. Decreto Legislativo n. 37 de 2021. Dezembro, 2021. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/12/2021&jornal=515&pagina=7&totalArquivos=188

158 Presidência da República do Brasil. Lei nº 14.197, de 1º de setembro de 2021, que Acrescenta o Título XII na Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), relativo aos crimes contra o Estado Democrático de Direito; e revoga a Lei nº 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), e dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Setembro, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14197.htm#:~:text=359%2DR.,a%208%20(oito)%20anos

159 Presidência da República do Brasil. Lei nº 12.737, de 30 de novembro de 2012, que Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Novembro, 2012. Disponível em: http://planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

160 Câmara dos Deputados. Projeto de Lei n. 8045/2010, sobre o Código de Processo Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

161 Supremo Tribunal de Justiça. Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. Novembro, 2021. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx

162 Câmara dos Deputados. Projeto de lei n. 2630/2020, que Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Abril, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2256735

	O país é parte ou observador?	Data de adesão e ratificação?	Apresentou Reservas?	O país possui uma Lei própria sobre combate a cibercrimes e cooperação internacional? Desde qual ano?	Debates atuais importantes sobre cibercrimes, cooperação internacional e fluxos de dados para fins de condução de investigações?
Chile	Parte [163]	Tratado ratificado em 20 de abril de 2017 e com entrada em vigor da convenção a partir de primeiro de agosto do mesmo ano.	Sim, no documento de acesso chileno a Convenção de Budapeste deixou de fora, dispositivos majoritariamente relacionados a medidas relativas à possibilidade de aplicação da lei doméstica, pornografia infantil e questões jurisdicionais (artigos 6.1, 9.2.b, 9.2.c, 9.4, 22.1.b e 29.4). Assim como a Argentina, o país também se reserva o direito de recusar pedidos de assistência internacional em casos onde a conduta não é tipificada na lei chilena. [164]	Ley 19223/92, que tipifica figuras penais relativas a crimes informáticos. [165] Boletim de Lei nº 12.192-25, que estabelece regras sobre crimes de informática, revoga a Lei nº 19.223 e modifica outros órgãos jurídicos para adaptá-los à Convenção de Budapeste. [166]	Boletim de Lei nº 12.192-25, que estabelece regras sobre crimes de informática, revoga a Lei nº 19.223 e modifica outros órgãos jurídicos para adaptá-los à Convenção de Budapeste. [167] - [168]

163 Conselho da Europa. Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

164 Conselho da Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185) - ChileColombia. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=Chihttps://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=COL

165 Biblioteca del Congreso Nacional de Chile. Ley 19223 Tipifica figuras penales relativas a la Informatica. May, 1993. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=30590

166 Senado, Proyecto de Ley Establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest. Disponível em: https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=12192-25

167 Camara de Diputadas y Diputados de Chile. Proyecto de Ley Modifica la ley N° 19.223 que Tipifica Figuras Penales Relativas a la Informática incorporando un nuevo delito. Disponível em: https://www.camara.cl/verDoc.aspx?prmID=14367&prmTIPO=INICIATIVA

168 https://noticias.usm.cl/2021/10/15/ley-de-delitos-informaticos

	O país é parte ou observador?	Data de adesão e ratificação?	Apresentou Reservas?	O país possui uma Lei própria sobre combate a cibercrimes e cooperação internacional? Desde qual ano?	Debates atuais importantes sobre cibercrimes, cooperação internacional e fluxos de dados para fins de condução de investigações?
Colômbia	Parte, convite realizado em 2019. [169]	16.03.2020, com entrada em vigor da convenção em 01 de julho de 2020.	Sim, as reservas apresentadas visam permitir ao país aplicar as medidas mencionadas nos artigos 20 (coleta em tempo real de dados em trânsito) e 21 (interceptação de dados de conteúdo) da Convenção de acordo com seu regulamento interno em matéria de dados pessoais e proteção do direito à privacidade. [170]	— Lei n. 1273/2009 [171] — Lei n. 1928/2019 [172]	Em março de 2021 o Ministério das Tecnologias da informação e comunicações publicou a Resolução n. 500/2021, que estabelece "diretrizes e padrões para a estratégia de segurança digital e a modelo de segurança e privacidade como viabilizador da política de Governo Digital". [173]

169 Conselho da Europa. Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty treaty no=185

170 Conselho da Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185) - Colombia. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=COL

171 Diário Oficial, Colombia. Ley 1273 de 2009, que modifica o Código Penal. Disponível em: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

172 Vlex. Ley 1928 del 24 de Julio de 2018 Senado. Julho, 2018. Disponível em: https://vlex.com.co/vid/ley-1928-24-julio-737603069

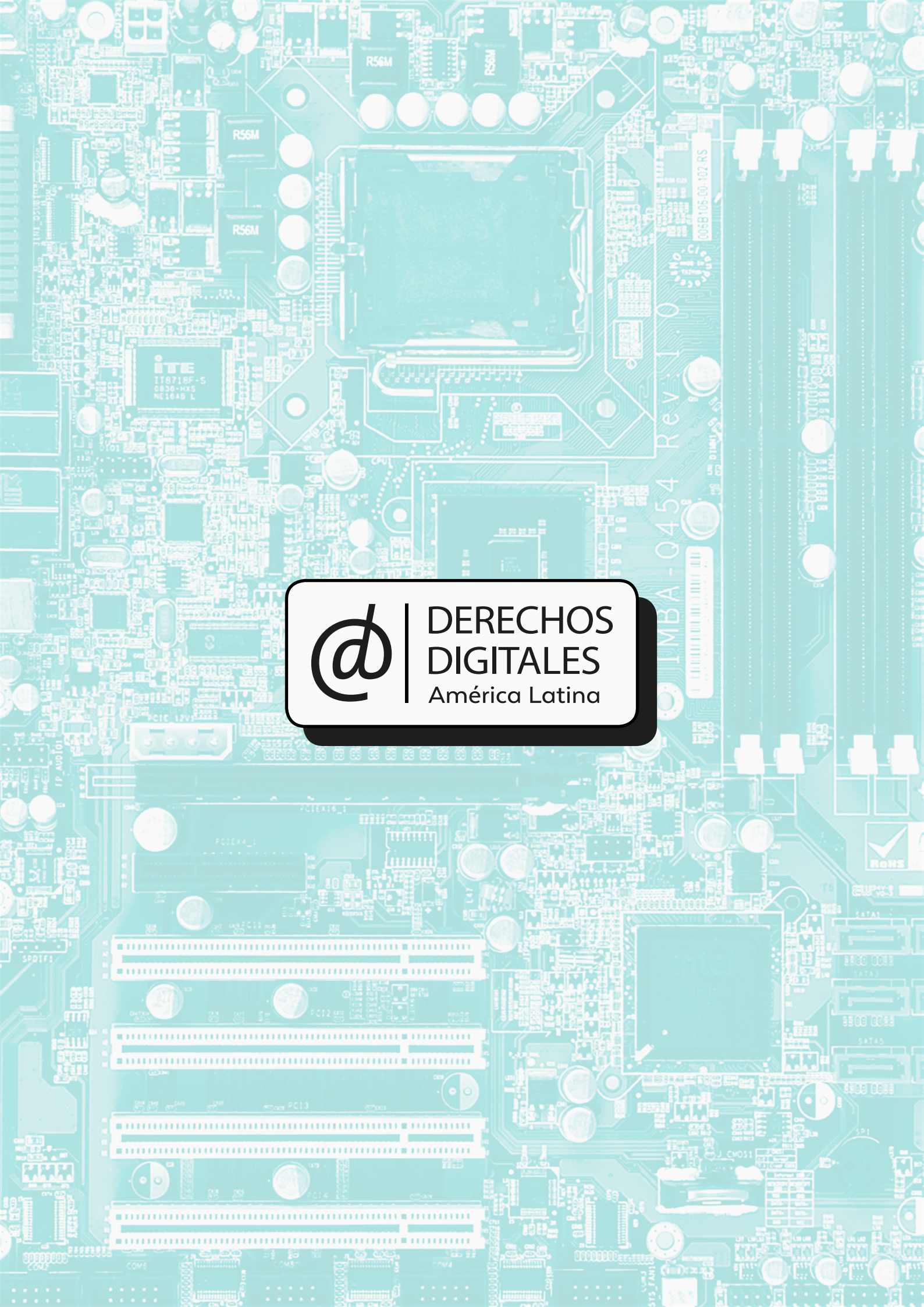
173 Republica de Colombia, MINTIC. RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital". Março, 2021. Disponível em: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

	O país é parte ou observador?	Data de adesão e ratificação?	Apresentou Reservas?	O país possui uma Lei própria sobre combate a cibercrimes e cooperação internacional? Desde qual ano?	Debates atuais importantes sobre cibercrimes, cooperação internacional e fluxos de dados para fins de condução de investigações?
México	Observador da Convenção[174]	Não se aplica	Não se aplica	Sim, em 1999 o Congresso iniciou uma primeira leva de reformas ao seu Código Penal responsável por inserir o tema dos cibercrimes no texto da lei. Além disso, atualmente, o país possui dispositivos sobre o tema em seu Código Penal, Lei de Segurança Nacional e uma Estratégia Nacional de Segurança Cibernética, anunciada pelo Presidente mexicano em 2017.	Existe um atual debate sobre uma reforma das leis que regem o Sistema Nacional de Segurança Pública.[175]-[176]

174 Conselho da Europa. Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

175 IT Masters Mag. Delitos informáticos en México, ¿qué dice la Ley? Setembro, 2020. Disponível em: https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/

176 Em setembro de 2019, a Comissão de Segurança Pública da Câmara dos Deputados aprovou dois pareceres para reformar as Leis Gerais do Sistema Nacional de Segurança Pública em matéria de cibersegurança e Segurança Nacional em matéria de inteligência.


DERECHOS
DIGITALES
América Latina