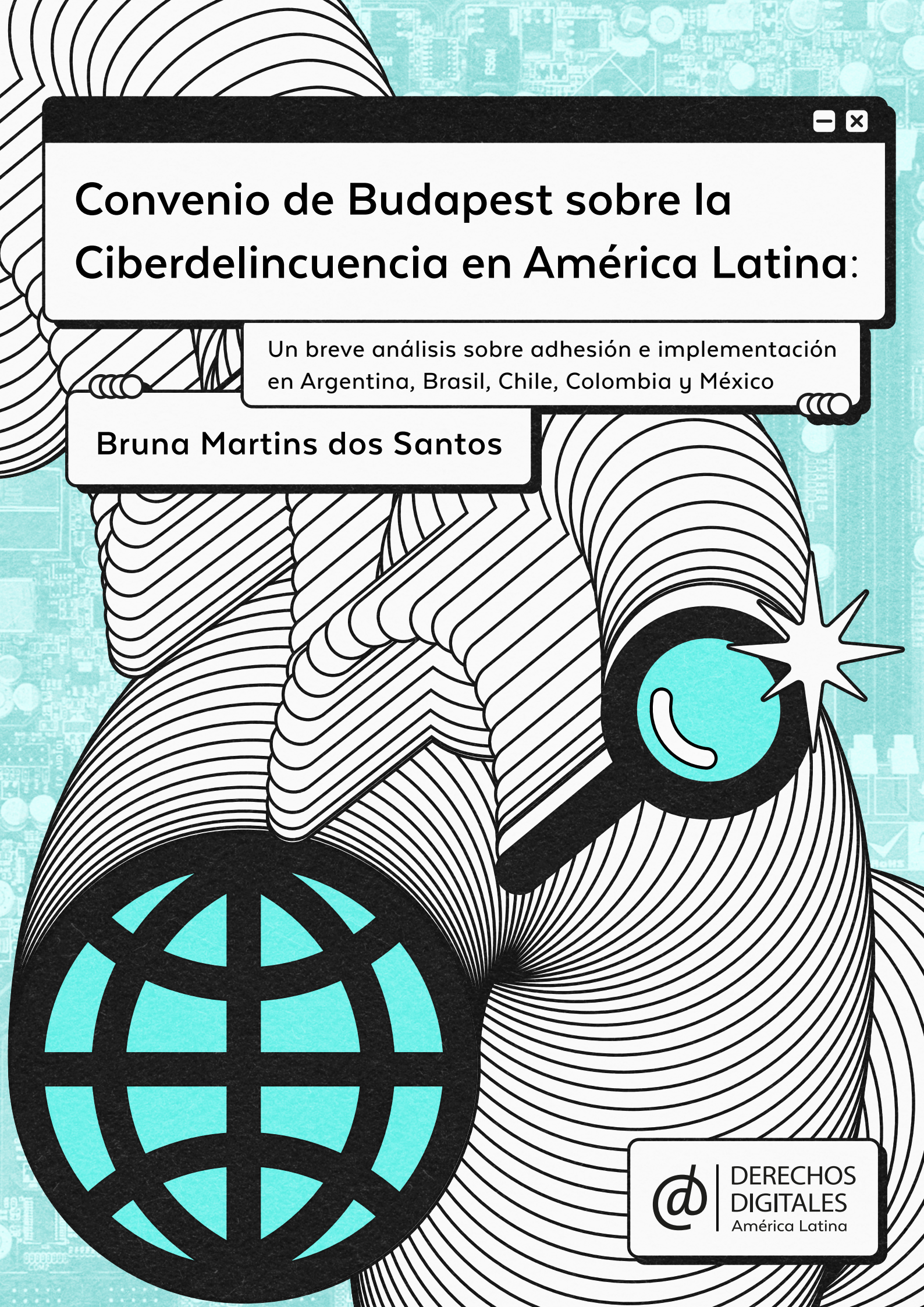
Convenio de Budapest sobre la Ciberdelincuencia en América Latina:

Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México

Bruna Martins dos Santos



DERECHOS DIGITALES
América Latina

Este reporte fue realizado por Derechos Digitales, con el apoyo del International Development Research Centre (IDRC).

Desde 2019, Derechos Digitales es parte de la red de Cyber Policy Research Centres de IDRC, junto a organizaciones líderes en temas de tecnologías y políticas públicas en el Sur Global.

Texto por **Bruna Martins dos Santos**
Traducción: **Gonzalo Bernabó**
Diseño y diagramación por **Catalina Viera**
Revisión por: **J. Carlos Lara, Michel Roberto de Souza, Jamila Venturini**

La autora quisiera agradecer a Cristian León, Secretario-Ejecutivo de la Red Al Sur; Grecia Macías y Luis Fernando García, R3D; J. Carlos Lara, Jamila Venturini y Michel Roberto de Souza, Derechos Digitales; Bárbara Simão, InternetLab; y Carolina Botero, Fundación Karisma; por el tiempo dedicado a las entrevistas y las aportaciones adicionales necesarias para la redacción del presente informe.

Mayo de 2022

Contenido

I. Introducción

En noviembre de 2001, el Consejo de Europa decidió abrir a la firma el texto del Convenio sobre la Ciberdelincuencia. El Convenio de Budapest, como se conoce, es hasta la fecha uno de los principales tratados internacionales vinculantes en materia penal y se elaboró con el objetivo de intensificar la cooperación internacional y "aplicar una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional". [1]

A pesar de que la apertura de firmas se produjo a finales de 2001, hace más de 20 años, el Convenio sigue siendo uno de los principales temas de discusión cuando se habla de una agenda común para la cooperación internacional y la lucha contra los delitos cometidos en el ámbito digital, habiendo influenciado legislaciones en todo el mundo.

Entre los temas abordados por el Convenio sobre la Ciberdelincuencia podemos destacar los debates sobre (i) criminalización de conductas; (ii) normas de investigación; (iii) producción de pruebas electrónicas; y (iv) medios de cooperación internacional, como la extradición y la asistencia jurídica mutua[2]. Más recientemente, con la positiva y creciente incidencia de nuevas legislaciones sobre protección de datos personales a nivel mundial, el debate sobre las garantías y la protección de datos aplicada al ámbito de la seguridad pública y la persecución penal también ha entrado en escena.

Sin embargo, el debate no se centra únicamente en la armonización de las actividades de persecución de delitos cibernéticos de forma transfronteriza. Una parte importante de las críticas dirigidas al Convenio en los últimos años ha sido en relación a que el texto promueve tipificaciones penales vacías y genéricas[3] y presenta desafíos de implementación de la adecuación para sus signatarios.

---

1 Consejo de Europa. Convenio sobre Ciberdelincuencia (Convenio de Budapest). Disponible en: 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 (El Convenio de Budapest se promulga bajo la forma de Decreto Legislativo n.37). 22 de Diciembre de 2021. Disponible en: https://opiceblum.com.br/convencao-de-budapeste-e-promulgada-sob-a-forma-do-decreto-legislativo-no-37/

3 Serquera, Maricarmen y Samaniego, Marlene. Desafíos de la Armonización de la Convención de Budapest en el Sistema Penal Paraguayo. Derechos Digitales. Junio, 2018. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/minuta_TEDIC.pdf

En función de lo expuesto, el presente informe pretende comentar algunos de los puntos principales del Convenio en cuestión, así como los desafíos de la implementación y armonización de las disposiciones del texto con los sistemas jurídicos y marcos legales de los países de la región latinoamericana. Para la elaboración del presente informe se ha realizado una revisión bibliográfica de materiales relevantes producidos en la región[4] y entrevistas semiestructuradas con representantes de organizaciones de la sociedad civil que integran la red *Al Sur*[5] localizadas en Brasil, Argentina, Colombia, México y Chile[6].

El documento, por tanto, se divide en sesiones dedicadas a analizar las diferentes situaciones de adhesión -o no- al Convenio por parte de los países arriba mencionados, así como las posibles diferencias en los contextos locales. A su vez, la información obtenida en los estudios de casos individuales y en las entrevistas realizadas fue utilizada para formular recomendaciones dedicadas al diseño e implementación de políticas públicas en la materia, con un enfoque basado en la protección de los derechos humanos en el ámbito digital como centro.

4 Ver, por ejemplo, la serie de estudios publicada por Derechos Digitales en colaboración con organizaciones y especialistas latino-americanos sobre el proceso de adecuación de las normas nacionales al Convenio de Budapest en https://www.derechosdigitales.org/tipo_publicacion/publicaciones/

5 Al Sur es un consorcio de organizaciones latinoamericanas de la sociedad civil y académica con el objetivo de fortalecer con su trabajo en equipo los derechos humanos en el ambiente digital. Más información en: https://www.alsur.lat/pt-br.

6 Las entrevistas contaron con representantes de las organizaciones: Derechos Digitales (Chile), R3D (México), InternetLab (Brasil), Fundación Karisma (Colombia) y Coalizão Direitos na Rede (Brasil).

II. El Convenio de Budapest sobre Delitos Cibernéticos

a. Principales temas discutidos por el Convenio y su influencia en los debates de ciberdelitos alrededor del mundo

El Convenio de Budapest sobre la Ciberdelincuencia se compone de cuatro capítulos sobre (a) terminología, (b) medidas que deben adoptarse a nivel nacional, (c) cooperación internacional y (d) disposiciones finales[7]. Uno de los puntos principales del texto son las tipificaciones de los ciberdelitos que se pueden cometer contra la confidencialidad de los sistemas y datos informáticos, computadoras, contenidos e incluso violaciones de los derechos de autor.

A pesar de ser un tratado debatido y redactado en el contexto del Consejo de Europa, con el paso de los años el Convenio de Budapest se ha consolidado como el principal texto legal sobre cooperación internacional con fines de persecución penal y lucha contra los ciberdelitos. La lista de firmantes incluye 44 Estados miembros del Consejo de Europa y algunos Estados no miembros, como Argentina, Canadá, Chile, Colombia, Estados Unidos de América, República Dominicana y Perú.[8]

El memorándum explicativo del Tratado conlleva preocupaciones respecto al creciente uso malicioso de medios de comunicación *online*, así como a la accesibilidad y facilidad con la que las informaciones son almacenadas en sistemas informáticos, como factores que han aumentado la disponibilidad de los flujos de información, y que la evolución reciente de las nuevas tecnologías y los cambios pueden haber contribuido a un aumento relativo de la incidencia de los delitos cibernéticos.[9] Sin embargo, algunos de los aspectos más destacados del texto en las actividades conmemorativas de su vigésimo primer aniversario en 2021 fueron el potencial para fomentar las estructuras de cooperación público-privada y la armonización entre las legislaciones y otras estructuras legales y administrativas dedicadas a la lucha contra los ciberdelitos.[10]

---

7 Migalhas. Convençao de Budapeste e crimes cibernéticos no Brasil. Octubre, 2020. Disponible en: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil

8 Consejo de Europa. El Convenio de Budapest y sus Protocolos Adicionales. Disponible en: https://www.coe.int/en/web/cybercrime/the-budapest-convention#{%22105166412%22:[0]}

9 Consejo de Europa. Explanatory Report on the Budapest Convention. Disponible en: https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf

10 Consejo de Europa. Benefits. Disonible en: https://www.coe.int/en/web/cybercrime/benefits

En este sentido, es importante señalar que a pesar del tenor punitivo bajo el cual fue elaborado el Convenio de Budapest, su relevancia hoy en día se debe al constante trabajo de actualización y a partir de cierto nivel de interlocución con otras discusiones como las relacionadas con la defensa de los derechos humanos en la era digital. Y en los últimos años, el tratado se ha consolidado de hecho como una base legal inicial para la definición de las estructuras de cooperación internacional, así como una guía para la posterior elaboración de legislaciones nacionales.

El Convenio también cuenta con un Comité específico - *Cybercrime Convention Committee* (T-CY)[11] - que es responsable de debatir las mejoras y actualizaciones del texto, y está compuesto por todos los países que han firmado o han sido invitados a firmar el Tratado. La creación del Comité T-CY está motivada por el artículo 46 del Convenio, que refuerza la necesidad de un mecanismo de consulta periódica entre los firmantes, con el objetivo principal de promover el intercambio de información sobre el uso y la implementación del texto, los procesos recientes de innovaciones tecnológicas y legislativas sobre la lucha contra los ciberdelitos y la recopilación de pruebas digitales, y también la discusión de posibles suplementos o adiciones al texto del convenio.[12] Asimismo, el colegiado ha funcionado como uno de los grupos intergubernamentales más relevantes actualmente para el debate y el análisis de la implementación de del Convenio, así como para la elaboración de interpretaciones del texto mediante notas orientativas (*guidance notes*[13]). Desde la creación del convenio, se han elaborado notas orientativas sobre temas como los sistemas informáticos, botnets, ataques DDoS, spam, terrorismo, entre otros.

11 Cybercrime Convention Committee (T-CY). The Budapest Convention on Cybercrime: benefits and impact in practice. Disponible en: 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 Consejo de Europa. Guidance Notes on the Convention on Cybercrime. Disponible en: https://www.coe.int/en/web/cybercrime/guidance-notes

Aún en relación al TC-Y, vale la pena mencionar que el Comité es el principal espacio de intercambio de información sobre la implementación y uso del Convenio y tiene el mandato para elaborar protocolos adicionales al texto original para articular nuevas cuestiones y demandas de los estados miembros en la lucha contra la ciberdelincuencia. De acuerdo con el reglamento interno del órgano (*Rules of Procedure*[14]), el mandato permite al colegiado realizar evaluaciones sobre la aplicación y el impacto del Convenio, adoptar opiniones y recomendaciones sobre posibles interpretaciones respecto del texto y debatir la elaboración de instrumentos legales —como convenios y protocolos adicionales— sobre cuestiones relacionadas con el Convenio de Budapest para someterlos a la aprobación del Comité de Ministros del Consejo de Europa.

Otro punto relevante en cuanto a la estructura del Convenio es la red 24/7, establecida por el artículo 35[15], que consiste en una red de puntos de contacto en todos los países firmantes y cuyos representantes tienen que estar disponibles para prestar asistencia inmediata tan pronto como les sea requerida. El objetivo principal de la citada red es establecer un canal de asistencia a efectos de investigaciones, procedimientos relativos a crímenes cibernéticos o incluso la recolección de pruebas electrónicas. Si la legislación local lo permite, la red 24/7 también puede ser la responsable de proporcionar conocimientos técnicos, aplicar medidas de preservación/protección de datos y recopilar pruebas digitales, incluso información sobre la ubicación de los sospechosos.

---

14 Consejo de Europa. Cybercrime Convention Committee (T-CY) T-CY Rules of Procedure. Octubre, 2020. Disponíble en: 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.*

Por último, cabe mencionar que el acceso/adhesión al Convenio también ofrece a los firmantes la posibilidad de llevar a cabo actividades de concientización y capacitación por parte del Comité Europeo. En un mundo en el que la disputa sobre el régimen de acceso a los datos localizados en el extranjero es un tema recurrente, abordado en muchas legislaciones y proyectos de ley en discusión, es relevante que la estructura facilitada por el Convenio pueda promover actividades de capacitación para los actores, incluso si esta medida es accesible, en gran medida, solo para los representantes de los Estados signatarios.

b. Primer Protocolo Adicional

Como resultado de la constante labor de revisión de las disposiciones del Convenio por parte del T-CY, sobre la base de lo dispuesto en el artículo 46 del tratado, en enero de 2003, se publicó el primer protocolo adicional, que se refiere a la incriminación de los actos de carácter racista cometidos a través de sistemas informáticos[16], y que entró en vigor en 2006. El texto, elaborado en su mayor parte por un comité de redacción constituido en el contexto del T-CY —y posteriormente sometido a la evaluación de los Estados miembros— tiene como principal objetivo promover una mayor armonización entre legislaciones relevantes en el ámbito del derecho criminal sobre la lucha contra el racismo y la xenofobia en internet.

En cuanto a las cuestiones de procedimiento en torno a la actuación del TC-Y y su papel en la elaboración de protocolos adicionales al Convenio de Budapest, conviene aclarar que el colegiado puede debatir sugerencias de protocolos adicionales y elaborar borradores de los textos. Sin embargo, la decisión de adopción de un determinado protocolo o convenio adicional al tratado principal debe ser refrendada por el Comité de Ministros del Consejo de Europa y, tras su aprobación, el texto queda abierto a la adhesión de los Estados signatarios del convenio - por tanto, la adhesión a los protocolos adicionales al Convenio de Budapest no es realizada de forma automática por todos los Estados signatarios.

16 Consejo de Europa. Details of Treaty No.189. Disponible en: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189

De acuerdo con el memorando explicativo[17] del texto, el acercamiento de partes distantes del mundo a través de los recientes cambios tecnológicos, comerciales y económicos, sería el motivo de una mayor incidencia y crecimiento acelerado de la difusión de contenidos de discriminación racial, xenofobia y otras formas de intolerancia en el ámbito online. En función de eso, el texto ofrece una definición para "material racista y xenófobo" (artículo 2) y tiene como objetivo presentar soluciones comunes para reprimir la difusión de este tipo de contenidos a través de los sistemas informáticos.

La división del protocolo está hecha según la tabla siguiente:

Tabla 1 - Resumen del Primer Protocolo Adicional al Convenio de Budapest

Temas	Artículos
Disposiciones Comunes y cuestiones generales	Capítulo I - Disposiciones Comunes
Disposiciones comunes y cuestiones generales	Capítulo II – Medidas a ser tomadas a nivel nacional — Difusión de contenidos racistas y xenófobos por sistemas — Amenazas por motivos racistas y xenófobos — Insultos por motivos racistas y xenófobos — Negación, minimización, aprobación o justificación de genocidios y crímenes contra la humanidad
Relación entre el Convenio de Budapest y el Protocolo Adicional	Capítulo III - Relaciones entre el Convenio y el Protocolo
Disposiciones Finales	Capítulo IV – Disposiciones finales

Por último, cabe destacar que un aspecto importante sobre el primer protocolo adicional es el intento de establecer una dinámica equilibrada entre la libertad de expresión de los usuarios de Internet y una lucha eficaz contra la difusión y la práctica del racismo y la xenofobia en el ámbito digital.

17 Consejo de 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. Disponible en: https://rm.coe.int/1680989b1c

c. Segundo Protocolo Adicional

El segundo protocolo adicional se refiere a un esfuerzo de actualización de las disposiciones del Convenio que es relativamente más reciente, ya que fue adoptado en diciembre de 2021 por los Estados miembros del Comité Europeo[18].

El texto surgió una vez más de una decisión del T-CY sobre la necesidad de endurecer las normas –como se destaca en su memorando explicativo–[19], especialmente en lo que dice respecto a la divulgación de informaciones de registro de nombres de dominio, medidas de cooperación directa con proveedores de servicios para la obtención de informaciones de usuarios, medios eficaces para la obtención de informaciones de usuarios y datos de tráfico, cooperación inmediata en casos de emergencia, herramientas de asistencia mutua, así como salvaguardias para la preservación de los derechos humanos en el ámbito digital.

El contexto para la creación del segundo protocolo adicional es, sin embargo, relativamente más complejo que el primero. Con el fin de aportar complementos al texto del Convenio de Budapest, el TC-Y creó dos grupos Ad Hoc dedicados exclusivamente al acceso fronterizo a los datos y cuestiones de jurisdicción territorial (Transborder Group[20], creado en 2012) y el acceso a los datos almacenados en las nubes (Cloud Evidence Group, creado en 2015[21]). En el año 2016, el final de los debates del Cloud Evidence Group llegó a la conclusión de que existía una supuesta dificultad de los Estados para acceder a los datos privados en función de cuestiones como la territorialidad, la computación en la nube y el alcance de las jurisdicciones[22]. Debido a las limitaciones discutidas en el colegiado, la conclusión terminó siendo la elaboración de un nuevo protocolo adicional que fue discutido entre 2017 y 2021.

18 Consejo de Europa. New Treaties. Disponible en: https://www.coe.int/en/web/conventions/new-treaties
19 Consejo de Europa. Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. 2022. Disponible en: https://rm.coe.int/1680a49c9d
20 Consejo de Europa. Transborder Ad Hoc Group. Disponible en: https://www.coe.int/en/web/cybercrime/tb
21 Consejo de Europa. Cloud Evidence Ad Hoc Group. Disponible en: https://www.coe.int/en/web/cybercrime/ceg
22 inCyber. [Budapest Convention] A second protocol to fight cybercrime. Diciembre, 2021. Disponible en: https://incyber.fr/en/budapest-convention-a-second-protocol-to-fight-cybercrime/

El segundo protocolo está estructurado de la siguiente manera:

Tabla 2 - Resumen del Segundo Protocolo Adicional al Convenio de Budapest

Temas[23]	Artículos
Disposiciones generales	Capítulo I - Disposiciones Generales
Cooperación mejorada	Capítulo II - Medidas para el mejoramiento de la cooperación — Sección I - Principios Generales — Sección II - Procedimientos para el mejoramiento de la cooperación con proveedores de servicios y otras partes — Sección III - Procedimientos para el mejoramiento de la cooperación internacional entre autoridades para el intercambio de datos — Sección IV - procedimientos para Asistencia Mutua — Sección V - Procedimientos relativos a actividades de cooperación internacional en ausencia de acuerdos internacionales
Condiciones, Salvaguardas y derechos	Capítulo III - Condiciones y Salvaguardas — Protección de datos personales — Salvaguardas — Principios Generales
Disposiciones Finales y asuntos de procedimiento	Capítulo IV - Efectos del Protocolo, firma, reservas, etc.

23 Consejo de Europa. Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas. 2022. Disponible en: https://rm.coe.int/1680a49dab

De acuerdo con el CdE, el segundo protocolo surge como una actualización necesaria para convertir el Convenio de Budapest en un instrumento más eficaz al tiempo que revisa cuestiones como el acceso transfronterizo a los datos y la cooperación legal mutua, y establece parámetros más claros para la cooperación directa entre las autoridades y los proveedores de servicios digitales, inclusive en el nivel de los proveedores de servicios de infraestructura de internet.[24]

Sin embargo, en los últimos años el debate en torno al segundo protocolo adicional ha movilizado a diversos sectores, en particular a la sociedad civil internacional, debido al intento del Comité Europeo de establecer nuevas normas de aplicación de la ley que van a contramano de los principios de protección de datos personales y privacidad.[25]

El texto del segundo protocolo adicional fue objeto de una gran movilización de la sociedad y de varias cartas que reclamaban cuestiones como más espacio para una participación cualificada de los sectores interesados, más tiempo para la discusión del texto, entre otras. En abril de 2018, 94 organizaciones de la sociedad civil firmaron una carta solicitando más transparencia para las negociaciones del segundo Protocolo adicional, y que el Comité invitase a especialistas de la sociedad civil a participar en los debates y en el proceso de redacción del texto.[26] Para las organizaciones, además de la falta de transparencia y de las debidas garantías de participación en el proceso, resulta preocupante el intento del Segundo Protocolo Adicional de estandarización del acceso transfronterizo de datos personales por parte de las autoridades policiales y judiciales.

En mayo de 2021 se publicaron más cartas de la sociedad civil sobre el proceso. La primera, fechada el 6 de mayo, advertía sobre el ritmo acelerado de las discusiones en las últimas fases de elaboración del texto, y que la falta de tiempo para analizar y revisar el texto era un factor que limitaba la participación cualificada del sector.[27] A finales del mismo mes, una nueva carta firmada por 43 organizaciones de la

---

24 CCDCOE. Battling Cybercrime Through the New Additional Protocol to the Budapest Convention. 2021. Disponible en: 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. Junio, 2021. Disponible en: 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. Disponible en: https://edri.org/files/letter-cybercrimenegotiations-and-transparency_20180403_EN.pdf

27 Carta de la Sociedad Civil. 6th round of consultation on the Cybercrime Protocol and civil society participation. Mayo, 2021. Disponible en: https://rm.coe.int/0900001680a25788

sociedad civil -entre ellas Derechos Digitales y varias organizaciones latinoamericanas- fue enviada al Comité de Ministros del CdE exigiendo más tiempo para un análisis cualificado del borrador final del texto antes del cierre del proceso de consulta con los sectores interesados.[28]

A pesar de las reiteradas peticiones de mayor transparencia y amplia participación de la sociedad civil en las negociaciones del texto[29], éste fue puesto a disposición para consulta pública durante sólo dos semanas y después de que la recopilación de inputs estuviera finalizada - un factor más que demuestra la premura del debate y la escasa adherencia a las demandas planteadas por la sociedad civil.[30]

En cuanto a la participación sectorial en el proceso de elaboración del segundo protocolo adicional, cabe mencionar que la evaluación de organizaciones como la Electronic Frontier Foundation es que, a pesar de la realización de consultas periódicas por parte del TC-Y con la participación de los sectores interesados[31], el proceso habría fallado en el cumplimiento de los principios multisectoriales de transparencia, rendición de cuentas e inclusión.[32] El monitoreo de este tipo de acuerdos y negociaciones por parte de los diferentes sectores es fundamental para asegurar que sean escuchadas y consideradas las diversas preocupaciones en relación a la atención de los derechos humanos a partir del contexto y la experiencia de la implementación del Convenio en cada país.

Está previsto que el texto, aprobado el 17 de diciembre de 2021, se ponga a disposición para la adhesión de los firmantes en mayo de 2022.

---

28 Carta de la Sociedad Civil. Ensuring Meaningful Consultation in Cybercrime Negotiations. Abril, 2021. Disponible en: 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. Disponible en: 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. Disponible en: https://edpb.europa.eu/system/files/2021-05/edpb_contribution052021_6throundconsultations_budapestconvention_en.pdf.

31 Consejo de 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].
Disponible en: 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. Junio, 2021. Disponible en: https://www.eff.org/deeplinks/2021/06/civil-society-groups-seek-more-time-review-comment-rushed-global-treaty-intrusive

III. El Convenio de Budapest en los países de América Latina y debates actuales sobre el tema

a. Argentina

La adhesión de Argentina al Convenio de Budapest se llevó a cabo incluso ante las advertencias de la sociedad civil y el mundo académico sobre la amplitud y ambigüedad del texto y sus consideraciones sobre los riesgos que suponía para las actividades de investigación en seguridad informática desarrolladas en el país.[33] Especialistas en el país advirtieron sobre el aumento de la inseguridad jurídica para la realización de actividades de investigación penal en el ámbito de los ciberdelitos debido a las disposiciones abiertas y genéricas presentes, también en la Ley 26.388, de delitos informáticos, ya que ambos textos no están exentos de interpretaciones arbitrarias y potenciales abusos por parte de las autoridades.[34]

A pesar de las advertencias, en 2018, con motivo de la sanción de la Ley Nº 27.411[35], el país internalizó las disposiciones del Convenio de Budapest en su ordenamiento jurídico. La adhesión de Argentina, sin embargo, se hizo con reservas debido a las disposiciones que representaban un conflicto potencial con la legislación nacional. Deja fuera, por tanto,

33 Infobae. Argentina se suma a la Convención de Budapest para tratar delitos informáticos. Junio, 2018. Disponible en: 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. Junio, 2018. Disponible en: 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. Disponible en: https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798

las disposiciones relacionadas mayormente a las medidas relativas a la pornografía infantil y a las cuestiones jurisdiccionales (las siguientes disposiciones: 6.1.b[36], 9.1.d[37], 9.2.b[38], 9.2.c[39], 9.1.e[40], 22.1.d[41] y 29.4[42]).

El país ha informado de su participación activa en el Comité T-CY y ha celebrado la adopción del 2º Protocolo Adicional al Convenio de Budapest afirmando que "Para prevenir y perseguir el delito cibernético es fundamental contar con mecanismos e instrumentos adecuados que permitan y faciliten la cooperación y asistencia 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. Mayo, 2021. Disponible en: https://www.argentina.gob.ar/noticias/ciberdelito-se-aprobo-el-texto-del-2deg-protocolo-adicional-del-convenio-de-budapest

Tabla 3 - Cuadro-resumen - Argentina

¿El país es parte u observador? Parte[44]

¿Fecha de adhesión y ratificación? Tratado ratificado el 05 de junio de 2018, y con fecha de entrada en vigor del convenio a partir del 01 de octubre del mismo año.

¿Presentó Reservas? Sí, la ley argentina que internaliza las disposiciones del tratado deja fuera las disposiciones relacionadas mayormente con las medidas relativas a la pornografía infantil y las cuestiones jurisdiccionales (las siguientes disposiciones: 6.1.b[45], 9.1.d[46], 9.2.b[47], 9.2.c[48], 9.1.e[49], 22.1.d[50] y 29.4[51]).[52]

---

44 Consejo de Europa. Chart of signatures and ratifications of Treaty 185. Disponible en: 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 Consejo de Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185). Disponible en: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=ARG

Tabla 3 - Cuadro-resumen - Argentina

¿El país posee su propia ley sobre ciberdelincuencia y cooperación internacional? ¿Desde qué año? En la actualidad, el país cuenta con un conjunto de leyes y normas relativas al ámbito digital, que abordan cuestiones relacionadas con la Protección de Datos personales, tipificación de conductas practicadas en el ámbito digital, protección de la propiedad intelectual y una ley adicional, como la descrita anteriormente, que aprueba el texto del Convenio de Budapest y dicta las vías para su aplicación. Leyes relevantes: a. Ley 25.326[53], Ley de Protección de Datos Personales, b. Ley 26.388[54], Modificaciones al Código Penal, c. Ley 27.411[55], Aprueba el texto del Convenio de Budapest y d. Ley 11.723[56], Ley de Propiedad Intelectual.

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

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

55 Presidencia de la Nación. Argentina. Ley 27411, Convenio sobre Ciberdelito del Consejo de Europa. Disponible en: 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. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

b. Brasil

A pesar de ser, desde hace más de 20 años, una demanda de sectores como Ministerios, agencias gubernamentales, el Ministerio Público federal y una parte del Congreso Nacional, la adhesión de Brasil al Convenio de Budapest sobre la Ciberdelincuencia sólo se aprobó en diciembre de 2021[57] y espera el inicio del proceso de implementación.

Las discusiones en torno al tema han estado bastante presentes en el escenario legislativo brasileño y anteceden a la aprobación de leyes clave sobre el ámbito digital promulgadas en el país como el Marco Civil de Internet[58] y la Ley General de Protección de Datos Personales[59] así como algunas leyes ordinarias[60] que implicaron cambios en el Código Penal brasileño para incluir tipificaciones sobre delitos cibernéticos. En los años 2000, un proyecto de ley sustitutivo de otros proyectos de ley relacionados con los delitos informáticos presentado por el senador Eduardo Azeredo (PL de la Cámara nº 89 de 2003[61]) ya intentaba promover algún nivel de armonización entre las tipificaciones y discusiones presentes en el Convenio de Budapest contra la Ciberdelincuencia. Este texto fue fuertemente combatido por entidades de la sociedad civil, activistas y académicos debido a las tipificaciones genéricas y ambivalentes que pretendía introducir en el sistema jurídico brasileño. En respuesta, se propuso una ley destinada a la protección y garantía de los derechos en el ámbito digital que desembocaría, en 2011, en el envío de una de las primeras versiones del texto del Marco Civil de Internet[62] a la Cámara de Diputados.[63]

---

57 Gobierno Federal, Ministerio de Justicia y Seguridad Pública. Aprobada la adhesión de Brasil al Convenio de Budapest sobre la Ciberdelincuencia. Diciembre de 2021. Disponible en: https://www.gov.br/mj/pt-br/assuntos/noticias/aprovada-adesao-do-brasil-a-convencao-de-budapeste-sobre-o-crime-cibernetico

58 Presidencia de la República de Brasil. Ley nº 12.965, de 23 de abril de 2014, que establece princípios, garantías, derechos y deberes para el uso de Internet en Brasil. Abril, 2014. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

59 Presidencia de la República de Brasil. Ley nº 13.709, de 14 de agosto de 2018, Ley General de Protección de Datos Personales (LGPD). Agosto, 2018. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

60 Ejemplos relevantes de las actualizaciones realizadas en los últimos años en la legislación penal brasileña para abordar la lucha contra la ciberdelincuencia son la ley 12.737, de 30 de novembro de 2012, y 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). Disponible en: https://www.safernet.org.br/site/institucional/projetos/obsleg/pl-azeredo

62 Cámara de Diputados. Projeto de ley n. 2126/2011, que establece principios, garantías, derechos y deberes para el uso de Internet en Brasil. Disponible en: 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. Disponible en: 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. Disponible en: https://igarape.org.br/marcocivil/pt/.

Aún en el Marco Civil de Internet (MCI), cabe destacar que el texto continuó prosperando como la principal legislación de internet en el país, especialmente por su abordaje basado en los derechos de los usuarios de internet y también porque su elaboración contó con la participación de los más diversos sectores de la sociedad brasileña. Sobre el tema específico de las investigaciones online y el almacenamiento de datos, el MCI contiene disposiciones sobre el almacenamiento y la disponibilidad de los registros de conexión y acceso a las aplicaciones de Internet. En 2018, siguiendo el ejemplo de elaboración normativa con la participación de la sociedad, el país aprobó la ley n. 13.709/2018, o Ley General de Protección de Datos Personales[64], responsable de establecer las reglas básicas para la ejecución de las actividades de tratamiento de datos personales en el país.

En el ámbito judicial, una sentencia del Supremo Tribunal Federal (STF) sellará una controversia sobre el Acuerdo de Asistencia Judicial en Materia Penal (MLAT), firmado entre Brasil y Estados Unidos. La duda que debe decidir el STF es si las autoridades brasileñas, incluido el poder judicial, pueden solicitar directamente a las empresas de tecnología en el extranjero datos e informaciones, prescindiendo así de los procedimientos de cooperación jurídica internacional para la obtención de contenidos de aplicaciones de internet que se encuentren en el extranjero. En 2020, el STF celebró una audiencia pública para escuchar a expertos en la materia[65], en la que se hizo referencia en varios momentos a los conceptos aportados por el Convenio de Budapest, así como a la necesidad de respetar los derechos humanos.[66]

A finales de 2019, el país recibió la invitación para convertirse en signatario del Convenio con un plazo máximo de 3 años para completar el proceso. Menos de 2 años después, en diciembre de 2021, se promulgó el Decreto Legislativo Nº 37 de 2021[67], que "Aprueba el texto del Convenio sobre la Ciberdelincuencia, celebrado en Budapest el 23 de noviembre de 2001", sin que se sugieran reservas al texto del Convenio.

64 Presidencia de la República de Brasil. Ley General de Protección de Datos Personales. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

65 STF. Audiencia pública n. 29. Disponible en: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf

66 El caso está previsto para ser juzgado en mayo de 2022. STF. ADC 51. Disponible en: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379

67 Senado Federal. Proyecto de Decreto Legislativo n. 255 de 2021. Disponible en: https://www25.senado.leg.br/web/atividade/materias/-/materia/150258

A pesar de ser celebrado por algunas autoridades gubernamentales y por el sector privado[68], el proceso suscitó muchas preocupaciones por parte de la sociedad civil brasileña[69]- [70] respecto a cuestiones como (i) la aprobación en un plazo menor de lo previsto; (ii) celebrarse sin ningún debate multisectorial sobre el tema; (iii) la ausencia de una ley general de protección de datos dedicada a las actividades de persecución penal y de seguridad pública[71]; y (iv) haber sido aprobado durante el proceso de rediscusión del Código Procesal Penal brasileño, que contiene secciones dedicadas exclusivamente a regular las actividades de investigación online, recopilación de datos y cooperación entre autoridades y empresas.

Asimismo, otro punto clave que se cuestionó fue el carácter de adhesión total e irrestricta al Convenio, ignorando las disposiciones del Tratado sobre la "necesidad de alineamiento entre su contenido y las normas internas de los signatarios y con instrumentos internacionales de derechos humanos"[72] y mecanismos como declaraciones (art. 40 del Convenio) y reservas (art. 42). Tales mecanismos existen justamente para facilitar el proceso de conformidad interna y fomentar el ejercicio de la soberanía de cada país que desee integrar el grupo de signatarios. En este sentido, la celeridad con la que se llevó a cabo el proceso de adhesión del Estado brasileño es un factor de gran preocupación, ya que puede haber hecho inviable cualquier análisis de conformidad con el ordenamiento jurídico brasileño a la luz de las legislaciones que fueron aprobadas en el país en los últimos años.

A continuación se presenta un cuadro en el que se destacan los puntos de dos de los principales proyectos de ley en curso en el Congreso brasileño sobre cuestiones relacionadas con el Convenio de Budapest:

---

68 Brasscom. Empresas de tecnologia defendem a adesão do Brasil à Convenção de Budapeste. Disponible en: 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. Octubre, 2021. Disponible en: 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. Noviembre, 2021. Disponible en: 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. Julio, 2021. Disponible en: 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 Artículo 15, del Convenio de Budapest sobre el Ciberdelito.

Tabla 4 - Proyectos de Ley en Brasil	
Proyectos de Ley	**Puntos relevantes**
PL 2630/2020, Que instituye la Ley Brasileña de Libertad, Responsabilidad y Transparencia en Internet [73]	— Determina que los proveedores de aplicaciones de Internet que operan en Brasil deben tener sede y nombrar representantes legales en el país.[74] — Crea un nuevo tipo penal sobre la promoción o financiación del uso de cuentas automatizadas y otros medios para difundir contenidos no veraces (desinformación) o susceptibles de sanción penal.
CPL 8045/10, acerca del Código de Procedimiento Penal.[75]-[76]	— Crea alternativas para el tema de las medidas cautelares como el uso de mecanismos como el monitoreo electrónico y el bloqueo de dirección electrónica.[77] — Busca aumentar las posibilidades de que se utilice la interceptación telefónica. — Modifica la parte relativa a las pruebas electrónicas, permitiendo el monitoreo de personas investigadas, la interceptación de datos en reposo y otros. — Aborda las posibilidades de cooperación jurídica internacional para la instrucción o producción de pruebas.

Además de los proyectos de ley destacados anteriormente, cabe decir que el país también ha estado analizando la posibilidad de elaborar y aprobar una Ley General de Protección de Datos Personales aplicable al ámbito de la seguridad pública[78]. Un anteproyecto de ley ha sido elaborado por una comisión de juristas creada por el presidente de la Cámara de Diputados[79] y centra una parte considerable de sus disposiciones en la dicotomía entre el establecimiento de salvaguardias y garantías que protejan los derechos de las personas versus la realización de investigaciones en el entorno digital. Con todo, este anteproyecto aún no se ha presentado como proyecto de ley.

73 Cámara de Diputados. Projeto de ley n. 2630/2020, por la que se establece la Ley Brasilera de Libertad, Responsabilidad y Transparencia en Internet. Abril, 2020. Disponible en: https://www.camara.leg.br/propostas-legislativas/2256735

74 Informe del Grupo de Trabajo destinado a elaborar la opinión sobre el proyecto de ley 2630/2020. Disponible en: 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 Cámara de Diputados. Proyecto de ley n. 8045/10, que trata del Código de Proceso Penal, Disponible en: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

76 Cámara de Diputados. Informe del Relator de la Comisión Especial para el Análisis del Proyecto de Ley del Código Procesal Penal, João Campos. Disponible en: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1998270&filename=Parecer-PL804510-26-04-2021

77 Cámara de Diputados. Vea los principales puntos de la reforma de la Ley de Enjuiciamiento Criminal. Disponible en: https://www.camara.leg.br/noticias/210377-veja-os-principais-pontos-da-reforma-do-codigo-de-processo-penal/

78 Supremo Tribunal de Justicia. La Comisión entrega a la Cámara un proyecto de ley sobre el tratamiento de datos personales en el ámbito penal. Noviembre de 2021. Disponible en: 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 El Anteproyecto de Ley, en la versión presentada por la Comisión de Juristas, puede consultarse aquí: 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

Tabla 5 - Cuadro-resumen - Brasil

¿El país es parte u observador? Actualmente, el país tiene estatus de observador en la Convención. Sin embargo, la invitación para la adhesión llegó en 2019.[80]

¿Fecha de adhesión y ratificación? El proceso de Adhesión fue formalizado por el Congreso de Brasil en diciembre de 2021 con la edición del Decreto Legislativo Nº 37 de 2021[81]. La fecha de ratificación aún no está confirmada, ya que el proceso depende de una última fase de actuación del ejecutivo y de la confirmación de la ratificación.

¿Presentó Reservas? No.

¿El país posee su propia ley sobre ciberdelincuencia y cooperación internacional? ¿Desde qué año? Sí, desde 1999 se debate en el país la creación de una ley dedicada exclusivamente a la lucha contra los delitos cibernéticos. Aunque el proyecto de ley 84/99 (PL Azeredo) fue el primero en ser debatido de forma más categórica, actualmente el país cuenta con un conjunto de leyes sobre el tema de la lucha contra los ciberdelitos:

— Ley 14.197/2021 - Ley de Defensa del Estado Democrático de Derecho[82]
— Ley 12.737/2012 - Dispone sobre la tipificación criminal de delitos informáticos[83]

Debates actuales importantes sobre ciberdelitos, cooperación internacional y flujo de datos para fines de conducción de investigaciones

— PL 8045/10, que altera el Código de Proceso Penal[84]
— Debates en torno a un PL para una Ley General de Protección de Datos para la Seguridad Pública, que aún no se ha presentado pero que ha contado con un grupo de trabajo de juristas en el congreso.[85]

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

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

82 Presidencia de la República de Brasil. Ley nº 14.197, de 1 de septiembre de 2021, que añade el Título XII a la Parte Especial del Decreto-Ley nº 2.848, de 7 de diciembre de 1940 (Código Penal), sobre los delitos contra el Estado Democrático de Derecho; y deroga la Ley nº 7.170, de 14 de diciembre de 1983 (Ley de Seguridad Nacional) y las disposiciones del Decreto-Ley nº 3.688, de 3 de octubre de 1941 (Ley de Contravenciones Criminales). Septiembre de 2021. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14197.htm#:~:text=359%2DR.,a%208%20(oito)%20anos

83 Presidencia de la República de Brasil. Ley nº 12.737, de 30 de noviembre de 2012, que Dispone sobre la tipificación penal de los delitos informáticos; modifica el Decreto-Ley nº 2.848, de 7 de diciembre de 1940 - Código Penal; y dicta otras disposiciones. Noviembre de 2012. Disponible en: http://planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

84 Cámara de Diputados. Proyecto de Ley n. 8045/2010, sobre el Código de Procesamiento Penal. Disponible en: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

85 Supremo Tribunal de Justicia. Comisión entrega a Cámara anteproyecto sobre tratamiento de datos personales en el área criminal. Noviembre, 2021. Disponible en: 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

La adhesión de Chile al Convenio de Budapest fue formalizada ante el Consejo de Europa en abril de 2017, días antes de la promulgación del Decreto Nº 83/2017, que "promulga el convenio sobre ciberdelincuencia".[86] La necesidad de reforzar el compromiso asumido a nivel nacional para garantizar la seguridad cibernética en el país (a través de la Política Nacional de Ciberseguridad) y de formar parte de un sistema rápido y eficaz de cooperación internacional, así como de establecer canales de intercambio de conocimientos sobre la lucha contra los crímenes cibernéticos son algunas de las principales razones alegadas por el Gobierno chileno para adherirse al tratado.[87]

Respecto a las reservas presentadas, cabe mencionar que en el caso chileno el documento de acceso al Convenio de Budapest depositado en el Consejo de Europa dejó fuera, disposiciones relacionadas en su mayoría con medidas relativas a la posibilidad de aplicación de la ley nacional, pornografía infantil y cuestiones jurisdiccionales (las siguientes disposiciones: 6.1[88], 9.2.b[89], 9.2.c[90], 9.4[91], 22.1.b[92] e 29.4[93]). Al igual que Argentina, el país también se reserva el derecho de rechazar las solicitudes de asistencia internacional en los casos en que la conducta no esté tipificada en la legislación chilena.

---

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

87 Ministerio de Relaciones Exteriores de Chile. Chile deposita el instrumento de adhesión al Convenio de Budapest sobre la Ciberdelincuencia. Abril, 2017. Disponible en: 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.

Es importante mencionar que, recientemente, se aprobó en el país un proyecto de ley dedicado a modernizar la Ley 19223/92, que "tipifica las conductas penales relacionadas con la informática, creando nuevos delitos". El texto del proyecto de ley en cuestión se dedica también a actualizar otros textos legales vigentes en el país con el fin de promover un mejor nivel de adecuación al Convenio de Budapest.[94]

Conforme a lo expuesto, el proyecto de ley, boletín Nº 12.192-25[95] establece normas sobre crímenes informáticos, deroga la Ley 19.223 y modifica otros cuerpos jurídicos para adaptarlos al Convenio de Budapest. El texto ha recibido bastantes presiones por parte del Gobierno para una rápida aprobación.[96] Entre los puntos rechazados en la etapa final de discusión del texto se encontraba la posibilidad de modificar el Código Penal para permitir que el Ministerio Público pudiera solicitar datos de los ciudadanos en cualquier momento, sin orden judicial ni mecanismo específico de transparencia y rendición de cuentas, a lo que se opusieron rotundamente representantes de la sociedad civil, el mundo académico y asociaciones empresariales.[97]

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

95 Boletín 12192-25, que establece reglas sobre crímenes de informática, deroga a Ley nº 19.223 y modifica otros órganos jurídicos para adaptarlos al Convenio de Budapest. Disponible en: 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. Enero, 2022. Disponible en: 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. Enero, 2022. Disponible en: https://www.derechosdigitales.org/17623/en-rechazo-a-la-modificacion-del-codigo-procesal-penal-que-habilita-la-vigilancia-sin-controles-ni-contrapesos-legales/

Tabla 6 - Proyectos de Ley en Chile	
Proyectos de Ley	**Puntos relevantes**
PL 12192-25, que "busca modificar la norma vigente (Ley n.19.223) que tipifica conductas relativas a sistemas informáticos".	— Pretende promover un mayor nivel de adecuación entre la legislación chilena dedicada a la lucha contra el cibercrimen y el Convenio de Budapest; — Promovía cambios procesales, rechazados, que incluían: * Una reducción relativa del control de las actividades estatales de investigación al tiempo que pretendía introducir mecanismos de solicitud de datos a los ciudadanos sin las suficientes garantías; * Una flexibilización de medidas de investigación invasivas vigentes en el sistema de justicia penal chileno, entre ellas una modificación del artículo 219 del Código Procesal Penal que habla sobre la interceptación de comunicaciones privadas; * Alternativas para introducir en el sistema procesal penal chileno la posibilidad de recolección de datos de personas sin una orden judicial específica que autorice el acto.

Los cambios propuestos y rechazados para la legislación chilena en el caso del PL12.192-25 seguían, por tanto, una preocupante tendencia a instrumentalizar el proceso de adaptación al Convenio de Budapest como excusa para reducir el control y la transparencia de las actividades de investigación del Estado, tendiendo a la violación de la privacidad de los ciudadanos.

Tabla 7 - Cuadro-resumen - Chile

¿El país es parte u observador? Parte[98]

¿Fecha de adhesión y ratificación? Tratado ratificado el 20 de abril de 2017 y con entrada en vigor del convenio a partir del 1 de agosto del mismo año.

¿Presentó Reservas? Sí, en el documento de acceso chileno al Convenio de Budapest se dejaron de lado disposiciones relacionadas, en su mayoría, con las medidas relativas a la posibilidad de aplicación de la ley nacional, la pornografía infantil y cuestiones jurisdiccionales (artículos 6.1[99], 9.2.b[100], 9.2.c[101], 9.4[102], 22.1.b[103] y 29.4[104]).Al igual que Argentina, el país también se reserva el derecho de rechazar las solicitudes de asistencia internacional en los casos en que la conducta no esté tipificada en la legislación chilena.[105]

¿El país posee su propia ley sobre ciberdelincuencia y cooperación internacional? ¿Desde qué año? Ley 19223/92, que tipifica figuras penales relativas a crímenes informáticos[106]

Debates actuales importantes sobre ciberdelitos, cooperación internacional y flujo de datos para fines de conducción de investigaciones — PL n. 12.192-25, que establece reglas sobre crímenes de informática, deroga la Ley n. 19.223 y modifica otros organismos jurídicos para adaptarlos al Convenio de Budapest[107]-[108], aprobada en marzo de 2022.

98 Consejo de Europa. Chart of signatures and ratifications of Treaty 185. Disponible en: 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 Consejo de Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185) - Chile. Disponible en: 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 Informática. Mayo, 1993. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=30590

107 Cámara 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. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=14367&prmTIPO=INICIATIVA

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

d. Colombia

En el caso colombiano, la discusión y elaboración de políticas públicas para temas relacionados a crímenes cibernéticos han favorecido perspectivas relacionadas con la defensa y seguridad cibernética y apuntan a facilitar el uso de la información en los procesos judiciales y a prevenir o anticipar la consumación de crímenes cibernéticos, como lo señala la *Fundación Karisma*[109]. En 2018, la organización señalaba que el país necesitaba una política pública en materia criminal más integral y que precisaba resolver las precariedades presentes en la Ley n. 1.273/2009[110], que instituye en el país la noción de preservación de los datos y sistemas de información, así como de las comunicaciones, antes de avanzar en las negociaciones de adhesión al Convenio de Budapest.

Sin embargo, el país promulgó la Ley Nº 1928 de 24 de julio de 2018, que aprueba el texto del Convenio de Budapest sobre la Ciberdelincuencia[111]. Ya el instrumento de adhesión al Convenio de Budapest fue depositado ante el Consejo de Europa en marzo de 2020[112]. En el caso colombiano, las reservas presentadas se refieren a la posibilidad del país de aplicar las medidas mencionadas en los artículos 20 (recolección en tiempo real de datos en tránsito) y 21 (interceptación de datos de contenido) del Convenio de acuerdo con su normativa interna en materia de datos personales y protección del derecho a la privacidad.

Entre las motivaciones dadas por el gobierno para la adhesión estaban la creciente incidencia de los delitos cibernéticos en los primeros meses de la pandemia de Covid-19 y la necesidad de contar con más herramientas para hacer frente a los ciberdelitos a través de la cooperación internacional entre países[113]. La facilitación de investigación de ciberdelitos de carácter transnacional a través de la formalización de canales de intercambio de información entre los países firmantes del Convenio, sumado a la

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

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

111 Vlex. Ley 1928 del 24 de Julio de 2018 Senado. Julio, 2018. Disponible en: 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. Marzo, 2020. Disponible en: 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. Disponible en: 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

posibilidad de acceso a los proyectos y programas de acceso y transferencia de conocimiento sobre los temas del Convenio fueron algunos de los otros beneficios alegados por el gobierno colombiano.[114]

En cuanto a la adecuación del ordenamiento jurídico colombiano al Convenio de Budapest, sin embargo, persisten algunas dudas sobre posibles límites y salvaguardias que podrían introducirse para evitar abusos y malas interpretaciones por parte de las autoridades estatales. En este sentido, cabe reforzar un punto destacado por la Fundación Karisma sobre la necesidad de fomentar el uso proporcional del derecho penal como respuesta a la ciberdelincuencia mediante la creación de leyes equilibradas y el examen de tipos penales genéricos en el ámbito interpretativo, a partir de normas ya existentes y estándares internacionales de derechos humanos.[115]

114 MINTIC. Adhesión al Convenio de Budapest contra la ciberdelincuencia, clave para Colombia en tiempos de Coronavirus. 07 de abril de 2020. Disponible en: 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 y Fundación Karisma. Convenio de Budapest; Aplicación en Colombia frente a derechos humanos. Junio de 2018. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/minuta_karisma.pdf

Tabla 8 - Cuadro-resumen - Colombia

¿El país es parte u observador? Parte, invitación realizada en 2019. [116]

¿Fecha de adhesión y ratificación? 16.03.2020, con entrada en vigor del convenio en 01 de julio de 2020.

¿Presentó Reservas? Si, las reservas presentadas pretenden que el país pueda aplicar las medidas mencionadas en los artículos 20 (recolección en tiempo real de datos en tránsito) y 21 (interceptación de datos de contenido) del Convenio de acuerdo con su normativa interna en materia de datos personales y protección del derecho a la privacidad.[117]

¿El país posee su propia ley sobre ciberdelincuencia y cooperación internacional? ¿Desde qué año?

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

Debates actuales importantes sobre ciberdelitos, cooperación internacional y flujo de datos para fines de conducción de investigaciones En marzo de 2021 el Ministerio de Tecnologías de la Información y Comunicaciones publicó la Resolución n. 500/2021, que establece "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".[120]

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

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

118 Diario Oficial, Colombia. Ley 1273 de 2009, que modifica el Código Penal. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

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

120 República 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". Marzo, 2021. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

e. México

México representa un caso particular, puesto que sólo figura como observador del Convenio y aún no ha formalizado su adhesión, a pesar de haber solicitado el ingreso en 2006. La ausencia de formalización, sin embargo, no ha impedido que el Convenio tenga también cierto nivel de influencia en el debate local sobre la lucha contra los delitos cibernéticos. Al igual que en otros países de la región, se han realizado en México reiterados intentos de transposición de disposiciones específicas para el ordenamiento jurídico nacional, y esto ha sido el motor para los proyectos de ley dirigidos a la actualización de la legislación mexicana en materia de ciberdelincuencia.

El país cuenta con un marco jurídico propio aplicable a determinados casos de delitos informáticos y que está constituido por el Código Penal[121], Ley de Seguridad Nacional[122] y algunas otras normas dispersas[123].

Para los especialistas entrevistados durante la elaboración del presente informe, existiría una peligrosa línea de legitimación de los textos del convenio y utilización de la justificación de la necesidad de implementación de su texto para la producción de leyes más duras, dedicadas a implementar más medidas de control y vigilancia en el proceso penal, además de tipos penales vagos, imprecisos y amplios de manera deliberada. En este sentido, respecto a la adhesión de México, algunos factores de riesgo podrían ser un eventual fortalecimiento de las capacidades y competencias de un Estado autoritario, y más aún iniciativas legislativas que terminen legitimando los abusos ya existentes del sistema procesal penal mexicano[124]. En el caso de que el país continuase con el proceso de adhesión al Convenio de Budapest, sería necesaria una atención aún mayor por parte de todos los sectores implicados en el tema, especialmente para ayudar a resolver eventuales ambigüedades entre el texto del Tratado frente al sistema mexicano y el

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

122 Diário Oficial de la Federación Mexicana. Ley de Seguridad Nacional. Disponible en: 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. Septiembre, 2020. Foro Jurídico. Disponible en: https://forojuridico.mx/el-estatus-de-mexico-y-el-convenio-sobre-la-ciberdelincuencia-de-budapest/

124 Entrevista con Grecia Macías y Luis Fernando García, abogada y director ejecutivo de la Red en Defensa de los Derechos Digitales - R3D.

Sistema Interamericano de Derechos Humanos. Algunos de los temas de atención serían: la protección de alertadores (*whistleblowers*), garantías del derecho a la libertad de expresión, y el uso de materiales con derechos de autor.

Una investigación realizada por la organización mexicana R3D con el apoyo de Derechos Digitales en junio de 2018 señaló algunas incongruencias persistentes entre la legislación mexicana y el Convenio, especialmente en función de la inseguridad jurídica generada por las tipificaciones amplias y genéricas de crímenes cibernéticos establecidas en el Tratado[125]. La organización señala también que tras una eventual adhesión del país al Convenio, sería necesario un análisis profundo sobre cuestiones como las competencias jurisdiccionales, el nivel y la instancia de implementación, e incluso la posible elaboración de una nueva ley especial o la modificación de leyes vigentes en las entidades federativas del país a fin de promover una mayor armonización y garantizar la exacta aplicación de la Ley Penal.[126]

Actualmente, el país ha discutido –al menos– 13 propuestas de ley dedicadas al ámbito de la ciberseguridad y que se dedican a instituir en el país una Ley de Seguridad Cibernética con tipificaciones de conductas como delitos cibernéticos, amenazas cibernéticas, la creación de una agencia nacional de seguridad cibernética y otras discusiones.[127] Adicionalmente, vale destacar que en 2017 fue editada una Estrategia Nacional de Ciberseguridad (ENCS)[128] para el país, como un documento orientador del Estado mexicano y que trae como objetivos principales el a. fomento de la colaboración entre los diferentes sectores, b. la necesidad de análisis y mapeo de riesgos y amenazas en el ciberespacio, c. la promoción del uso responsable de las tecnologías de la información y la comunicación, entre otros.

Aún sobre la ENCS, cabe destacar que organizaciones de la sociedad civil –como R3D– han reforzado la importancia de adoptar un enfoque basado en los derechos humanos, y han reivindicado que la Estrategia

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

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

128 Gobierno de México. Estrategia Nacional de Ciberseguridad. 2017. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

debe ser discutida abiertamente con la sociedad precisamente porque propone modificaciones a los marcos legales y jurídicos con los que se tipifican los delitos cibernéticos, lo que podría representar una amenaza para el ejercicio de las libertades y los derechos en Internet.[129] Más recientemente, el país inició la discusión de una reforma constitucional en materia de ciberseguridad con el objetivo de permitir que el Congreso mexicano tenga la competencia para elaborar "*leyes en materia de seguridad nacional, que incluyan la seguridad cibernética y protección de los derechos humanos en el ciberespacio, estableciendo los requisitos y límites a las investigaciones correspondientes*".[130] Sobre el tema, las organizaciones de la sociedad civil también alertaron, en una carta enviada al Congreso Mexicano en 2021, que el texto también presentaba riesgos en tanto que "La ambigüedad y amplitud de lo que se considera como conductas que atentan contra la seguridad nacional impediría tener claridad y certeza sobre los alcances, contenido y limitantes del ejercicio de poder y restricción del Estado hacia los derechos y libertades de la sociedad."[131]

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

130 Artículo 19 México, R3D, Aimée Vega Montiel – CEIICH UNAM y 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. Disponible en: https://articulo19.org/reforma-constitucional-en-materia-de-ciberseguridad-podria-explotarse-para-censurar-y-arremeter-contra-manifestaciones-legitimas-de-la-sociedad/

131 Artículo 19 México, R3D, Aimée Vega Montiel – CEIICH UNAM y 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. Disponible en: https://articulo19.org/reforma-constitucional-en-materia-de-ciberseguridad-podria-explotarse-para-censurar-y-arremeter-contra-manifestaciones-legitimas-de-la-sociedad/

Tabla 9 - Cuadro-resumen - México
¿El país es parte u observador? Observador del Convenio [132]
¿Fecha de adhesión y ratificación? El país no es firmante.
¿Presentó Reservas? El país no es firmante.
¿El país posee su propia ley sobre ciberdelincuencia y cooperación internacional? ¿Desde qué año? Sí, en 1999 el Congreso inició una primera oleada de reformas de su Código Penal encargada de insertar el tema de los ciberdelitos en el texto de la ley. Además, el país cuenta actualmente con disposiciones sobre el tema en su Código Penal, la Ley de Seguridad Nacional y una Estrategia Nacional de Ciberseguridad, anunciada por el Presidente de México en 2017.
Debates actuales importantes sobre ciberdelitos, cooperación internacional y flujo de datos para fines de conducción de investigaciones Existe un debate actual sobre una reforma de las leyes que rigen el Sistema Nacional de Seguridad Pública en el marco de la iniciativa de reforma constitucional en materia de ciberseguridad.[133] [134]

132 Consejo de Europa. Chart of signatures and ratifications of Treaty 185. Disponible en: 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? Septiembre, 2020. Disponible en: https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/

134 En septiembre de 2019, la Comisión de Seguridad Pública de la Cámara de Diputados aprobó dos dictámenes para reformar las Leyes Generales del Sistema Nacional de Seguridad Pública en materia de ciberseguridad y de Seguridad Nacional en materia de inteligencia.

IV. El debate sobre Ciberdelitos más allá del Convenio de Budapest

A pesar de ser uno de los principales textos sobre el tema, el Convenio de Budapest sobre la Ciberdelincuencia no es la única de las iniciativas recientes que se discuten a nivel mundial. En los últimos años, cada vez son más los foros y espacios como la Organización de las Naciones Unidas (ONU) o la Organización para la Cooperación y el Desarrollo Económico (OCDE) que vienen debatiendo la lucha contra los delitos cibernéticos y las formas de fomentar más canales de cooperación entre las autoridades. Estos debates incluyen la reflexión sobre cómo permitir y solicitar el acceso a los datos de individuos investigados dentro de directrices y salvaguardias que estén en consonancia con los estándares internacionales de derechos humanos.

En diciembre de 2019, la Asamblea General de la ONU aprobó en una resolución[135] la creación de un comité ad hoc para la elaboración de un nuevo tratado internacional de lucha contra los delitos cibernéticos, a pesar de las objeciones de países como Estados Unidos y bloques como la Unión Europea[136]. La Resolución[137] determina que el Comité será compuesto por especialistas de todas las regiones del mundo y buscará elaborar un nuevo Convenio sobre el combate al uso de tecnologías con fines delictivos, tomando en consideración los instrumentos internacionales y los esfuerzos existentes a nivel nacional, regional e internacional.

Entidades de la sociedad civil con participación internacional manifestaron su preocupación por la rapidez del proceso y la falta de evidencias sobre la necesidad del mismo. En una carta dirigida al Comité ad hoc en 2019, las mismas organizaciones advirtieron sobre la falta de un objetivo claro y bien definido para el texto del Tratado en cuestión, señalando que el empleo de términos y definiciones genéricas abre la posibilidad de criminalizar conductas online que actualmente están protegidas por los estándares y normas de derechos humanos internacionales.[138]

---

135 Organización de las Naciones Unidas. Resolución de la Asemblea General sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Diciembre, 2019. Disponible en: https://undocs.org/A/Res/74/247

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

137 Organización de las Naciones Unidas. Resolución de la Asemblea General sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Diciembre, 2019. Disponible en: 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. Noviembre, 2019. Disponible en: https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human

El tratado discutido por la ONU es una antigua propuesta expresada por países como Rusia[139] como un nuevo instrumento global capaz de sustituir al Convenio de Budapest. Además de las preocupaciones sobre el origen de la iniciativa, que en sus primeras versiones también recibió el apoyo de regímenes autoritarios como China, Camboya y otros países[140], otro punto planteado como preocupante por entidades del tercer sector es la falta de transparencia y de espacios de participación social comunes en las discusiones realizadas en el ámbito de las Naciones Unidas, que sigue teniendo muchas limitaciones para la participación de las entidades que no poseen el estatus de ECOSOC.[141]

Además de los debates realizados por la ONU, cabe mencionar también los recientes debates llevados a cabo por la OCDE sobre el acceso gubernamental a los datos personales. El debate, realizado exclusivamente en el ámbito del Comité de Política de Economía Digital - CDEP y en el contexto de la reciente revisión de la implementación de las Directrices de Privacidad de 1980 de la OCDE, identificó *el acceso gubernamental irrestricto y desproporcionado a datos personales mantenidos por el sector privado como una cuestión crucial para la gobernanza de datos y la protección de derechos y como una barrera potencial para permitir el libre flujo de datos con confianza.*[142]

Sin embargo, en diciembre de 2021 la iniciativa dirigida a elaborar principios de alto nivel u orientaciones para los países miembros de la OCDE en relación con el acceso fiable de los gobiernos a los datos personales almacenados por el sector privado fue interrumpida hasta nuevo aviso por la OCDE debido a los desacuerdos y la falta de consenso entre los países que integran el CDEP.[143]–[144]

---

139 Brown, Deborah. Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. HRW. Agosto, 2021. Disponible en: 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. Disponible en: 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. Disponible en: 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. Diciembre, 2020. Disponible en: 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. Diciembre, 2021. Disponible en: 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. Junio, 2021. Disponible en: https://iccwbo.org/content/uploads/sites/3/2021/05/2021-05-04-joint-business-hl-statement-on-govt-access-to-private-sector-data.pdf

Ya en el marco de la Organización de Estados Americanos (OEA), en 1999, fue creado un Grupo de Trabajo sobre Ciberdelitos por la Reunión de Ministros de Justicia u Otros Ministros, Fiscales y Procuradores Generales de las Américas (REMJA), un foro político y técnico sobre justicia y cooperación jurídica internacional. El objetivo de este Grupo de Trabajo es fortalecer la cooperación internacional en la prevención, investigación y juzgamiento de delitos cibernéticos, facilitar el intercambio de información y experiencias entre los miembros, y recomendar las acciones necesarias para fortalecer la cooperación entre los estados miembros en esta área. Entre otras cosas, este Grupo también promueve la recomendación de adhesión de los Estados al Convenio de Budapest y fomenta el desarrollo por parte de los Estados de estrategias nacionales sobre delitos cibernéticos.[145] Además de proporcionar programas de capacitación[146], el grupo consolida el desarrollo del tema en cada Estado, publica un Portal Interamericano de Cooperación en Materia de Delito Cibernético[147], además de facilitar el intercambio de informaciones consolidadas sobre las 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. Conclusión y Recomendaciones

El esquema de implementación y discusión de los procesos de adhesión en países como Chile, Brasil, Argentina, Colombia y México tiende a ser bastante similar en aspectos como (a) la falta de participación de los sectores interesados de manera relevante, (b) la celeridad en la discusión de las leyes y decretos promulgados sin transparencia y con apuro, (c) la utilización de la necesidad de adecuación al Convenio de Budapest para promover reformas integrales de la legislación penal y procesal penal vigente que ponen en riesgo derechos de los ciudadanos como el derecho a la intimidad, el derecho a la protección de datos y el debido proceso legal.

A pesar de ser el Convenio de Budapest un texto de gran relevancia para asuntos de cooperación internacional en materia penal, el hecho de que el texto haya sido desarrollado en un sistema jurídico y político diferente al vigente en los países latinoamericanos hace que el proceso de adaptación sea relativamente más costoso para los países de la región y requiere una atención aún mayor al cumplimiento de los estándares desarrollados en el sistema interamericano de protección de los derechos humanos.

En este sentido, como parte final de este documento, presentamos recomendaciones para los diferentes sectores sobre los respectivos procesos de adhesión e implementación del Convenio de Budapest en la región, así como la participación en futuras discusiones sobre temas como la cooperación internacional, el acceso gubernamental a datos de individuos investigados y la lucha contra los ciberdelitos.

A los Estados y gobiernos nacionales

1. Realización de debates multisectoriales sobre el proceso de adhesión de los países al grupo de signatarios del Convenio a fin de facilitar un mapeo sobre los riesgos e incongruencias del texto con el Ordenamiento Jurídico local, así como una discusión franca y propositiva sobre la presentación de posibles reservas y el proceso de implementación del Tratado Internacional;

2. Realizar un análisis de adecuación del Convenio de Budapest y sus protocolos, de acuerdo con los derechos humanos y fundamentales reconocidos por el Estado, evitando su empleo sólo como base común para la discusión de posibles caminos en la lucha contra los ciberdelitos.

3. Evitar la mera copia de los tipos penales abordados en el texto del Convenio, ya que esto plantea dudas sobre su aplicación;

4. Garantizar el pleno respeto a los derechos fundamentales de sus ciudadanos reconocidos en las respectivas Constituciones y leyes vigentes, para la realización de actividades de persecución penal en el ámbito digital mediante el establecimiento de garantías claras y específicas;

5. Incluir a todos los sectores interesados en futuros debates sobre nuevas tipificaciones para ciberdelitos, mecanismos de cooperación jurídica internacional, investigaciones y otros. El modelo de participación de las múltiples partes interesadas debe tenerse en cuenta también en la discusión de cuestiones relacionadas con el Convenio de Budapest, así como en la mayoría de los procesos de elaboración de políticas dedicadas a Internet.

6. Los países latinoamericanos tienen la obligación de asegurar que los compromisos adquiridos se reflejen en la adhesión e implementación del Convenio de Budapest, por lo que no pueden, en esta discusión, ignorar las obligaciones de derechos humanos que sustentan el sistema interamericano de derechos humanos.

7. Evitar la línea punitivista y preocupante del derecho penal como único camino. La tradición de los países de América del Sur en materia de abusos en la actividad policial y violaciones de los derechos humanos por parte de regímenes autoritarios debería ser el principal motivo para considerar y debatir las garantías de protección de derechos humanos en el ámbito digital para el continente.

A los sectores no gubernamentales

8. Advertir a la sociedad sobre posibles y eventuales abusos gubernamentales en la implementación del Convenio de Budapest sobre Ciberdelincuencia, así como en la ejecución de actividades de persecución penal en el ámbito digital por parte del Estado;

9. Llevar a cabo actividades de capacitación para ciudadanos, organizaciones del tercer sector y el mundo académico sobre los principales instrumentos de cooperación internacional vigentes, así como los aspectos de su implementación.

10. Realizar actividades de monitoreo y actuación sobre la incidencia legislativa ante la preocupante instrumentalización del proceso de adaptación al Convenio de Budapest como pretexto para reducir el control y la transparencia de las actividades de investigación del estado, con violaciones de las garantías fundamentales y de la privacidad de los ciudadanos.

11. Documentar los procesos de participación en los debates sobre las nuevas tipificaciones de los ciberdelitos, los mecanismos de cooperación jurídica internacional, las investigaciones y otros.

12. Explorar nuevas líneas de investigación y estudios complementarios en América Latina sobre la importancia y evolución regionales de las formas de institucionalización de lucha contra el ciberdelito, incluyendo la realización de acuerdos bilaterales de asistencia judicial en materia penal (MLAT) y cooperación jurídica internacional.

Anexo I - Cuadro de análisis sobre la situación de los países

	¿El país es parte u observador?	Fecha de adhesión y ratificación	¿Presentó Reservas?	¿El país posee su propia ley sobre ciberdelincuencia y cooperación internacional? ¿Desde qué año?
Argentina	Parte [149]	Tratado ratificado el 05 de junio de 2018, y con fecha de entrada en vigor del convenio a partir del 01 de octubre del mismo año.	Sí, la ley argentina que internaliza las disposiciones del tratado deja fuera las disposiciones relacionadas mayormente con las medidas relativas a la pornografía infantil y las cuestiones jurisdiccionales (las siguientes disposiciones: 6.1.b, 9.1.d, 9.2.b, 9.2.c, 9.1.e, 22.1.d y 29.4) [150]-[151]	— Ley 25.326 [152], Ley de Protección de Datos Personales — Ley 26.388 [153], Modificaciones al Código Penal — Ley 27.411 [154], Aprueba el texto del Convenio de Budapest — Ley 11.723 [155], Ley de Propiedad Intelectual

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

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

151 Consejo de Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185). Disponible en: 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. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

153 Presidencia de la Nación. Argentina. Ley 26.388, Código Penal. Infoleg. Disponible en: 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. Disponible en: 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. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

	¿El país es parte u observador?	Fecha de adhesión y ratificación	¿Presentó Reservas?	¿El país posee su propia ley sobre ciberdelincuencia y cooperación internacional? ¿Desde qué año?	Debates actuales importantes sobre ciberdelitos, cooperación internacional y flujo de datos para fines de conducción de investigaciones
Brasil	Actualmente, el país tiene estatus de observador en la Convención. Sin embargo, la invitación para la adhesión llegó en 2019. [156]	El proceso de Adhesión fue formalizado por el Congreso de Brasil en diciembre de 2021 con la edición del Decreto Legislativo nº 37 de 2021. [157] La fecha de ratificación aún no está confirmada, ya que el proceso depende de una última fase de actuación del ejecutivo y de la confirmación de la ratificación.	No	Sí, desde 1999 se debate en el país la creación de una ley dedicada exclusivamente a la lucha contra los delitos cibernéticos. Aunque el proyecto de ley 84/99 (PL Azeredo) fue el primero en ser debatido de forma más categórica, actualmente el país cuenta con un conjunto de leyes sobre el tema de la lucha contra los ciberdelitos: — L14197 - Ley de Defensa del Estado Democrático de Derecho [158] — 12.737/2012 - Dispone sobre la tipificación criminal de delitos informáticos [159]	— Reforma del Código de Proceso Penal [160] — Debates en torno a una Ley General de Protección de Datos para la Seguridad Pública, aún no presentada pero que ha contado con un grupo de trabajo de juristas en el congreso. [161] — Proyecto de Ley de las Fake News. [162]

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

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

158 Presidencia de la República de Brasil. Ley nº 14.197, de 1 de septiembre de 2021, que añade el Título XII a la Parte Especial del Decreto-Ley nº 2.848, de 7 de diciembre de 1940 (Código Penal), sobre los delitos contra el Estado Democrático de Derecho; y deroga la Ley nº 7.170, de 14 de diciembre de 1983 (Ley de Seguridad Nacional) y las disposiciones del Decreto-Ley nº 3.688, de 3 de octubre de 1941 (Ley de Contravenciones Criminales). Septiembre, 2021. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14197.htm#:~:text=359%2DR.,a%208%20(oito)%20anos

159 Presidencia de la República de Brasil. Ley nº 12.737, de 30 de noviembre de 2012, que Dispone sobre la tipificación criminal de delitos informáticos; modifica el Decreto-Ley nº 2.848, de 7 de diciembre de 1940 - Código Penal; y dicta otras medidas. Novembro, 2012. Disponible en: http://planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

160 Cámara de Diputados. Proyecto de Ley n. 8045/2010, sobre el Código de Proceso Penal. Disponible en: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

161 Supremo Tribunal de Justicia. Comisión entrega a la Cámara anteproyecto sobre tratamiento de datos personales en el área criminal. Noviembre, 2021. Disponible en: 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 Cámara de Diputados. Proyecto de ley n. 2630/2020, que Instituye la Ley Brasilera de Libertad, Responsabilidad y Transparencia en Internet. Abril, 2020. Disponible en: https://www.camara.leg.br/propostas-legislativas/2256735

	¿El país es parte u observador?	Fecha de adhesión y ratificación	¿Presentó Reservas?	¿El país posee su propia ley sobre ciberdelincuencia y cooperación internacional? ¿Desde qué año?	Debates actuales importantes sobre ciberdelitos, cooperación internacional y flujo de datos para fines de conducción de investigaciones
Chile	Parte [163]	Tratado ratificado el 20 de abril de 2017 y con entrada en vigor del convenio a partir del 1 de agosto del mismo año.	Sí, en el documento de acceso chileno al Convenio de Budapest se dejaron de lado disposiciones relacionadas, en su mayoría, con las medidas relativas a la posibilidad de aplicación de la ley nacional, la pornografía infantil y cuestiones jurisdiccionales (Artículos 6.1, 9.2.b, 9.2.c, 9.4, 22.1.b e 29.4). Al igual que Argentina, el país también se reserva el derecho de rechazar las solicitudes de asistencia internacional en los casos en que la conducta no esté tipificada en la legislación chilena. [164]	Ley 19223/92, que tipifica figuras penales relativas a crímenes informáticos [165] Boletín Nº 12192-25, proyecto de ley que 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. [166]	Boletín de Ley nº 12.192-25, que establece reglas sobre crímenes de informática, deroga la Ley n. 19.223 y modifica otros organismos jurídicos para adaptarlos al Convenio de Budapest [167]_ [168]

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

164 Consejo de Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185) - ChileColombia. Disponible en: 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 Informática. Mayo, 1993. Disponible en: 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. Disponible en: https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=12192-25

167 Cámara 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. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=14367&prmTIPO=INICIATIVA

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

	¿El país es parte u observador?	Fecha de adhesión y ratificación	¿Presentó Reservas?	¿El país posee su propia ley sobre ciberdelincuencia y cooperación internacional? ¿Desde qué año?	Debates actuales importantes sobre ciberdelitos, cooperación internacional y flujo de datos para fines de conducción de investigaciones
Colombia	Parte, invitación realizada en 2019. [169]	16.03.2020, con entrada en vigor del convenio en 01 de julio de 2020.	Si, las reservas presentadas pretenden que el país pueda aplicar las medidas mencionadas en los artículos 20 (recolección en tiempo real de datos en tránsito) y 21 (interceptación de datos de contenido) del Convenio de acuerdo con su normativa interna en materia de datos personales y protección del derecho a la privacidad. [170]	— Ley n. 1273/2009 [171] — Ley n. 1928/2019 [172]	En marzo de 2021 el Ministerio de Tecnologías de la Información y Comunicaciones publicó la Resolución n. 500/2021, que establece "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". [173]

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

170 Consejo de Europa. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185) - Colombia. Disponible en: 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 el Código Penal. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

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

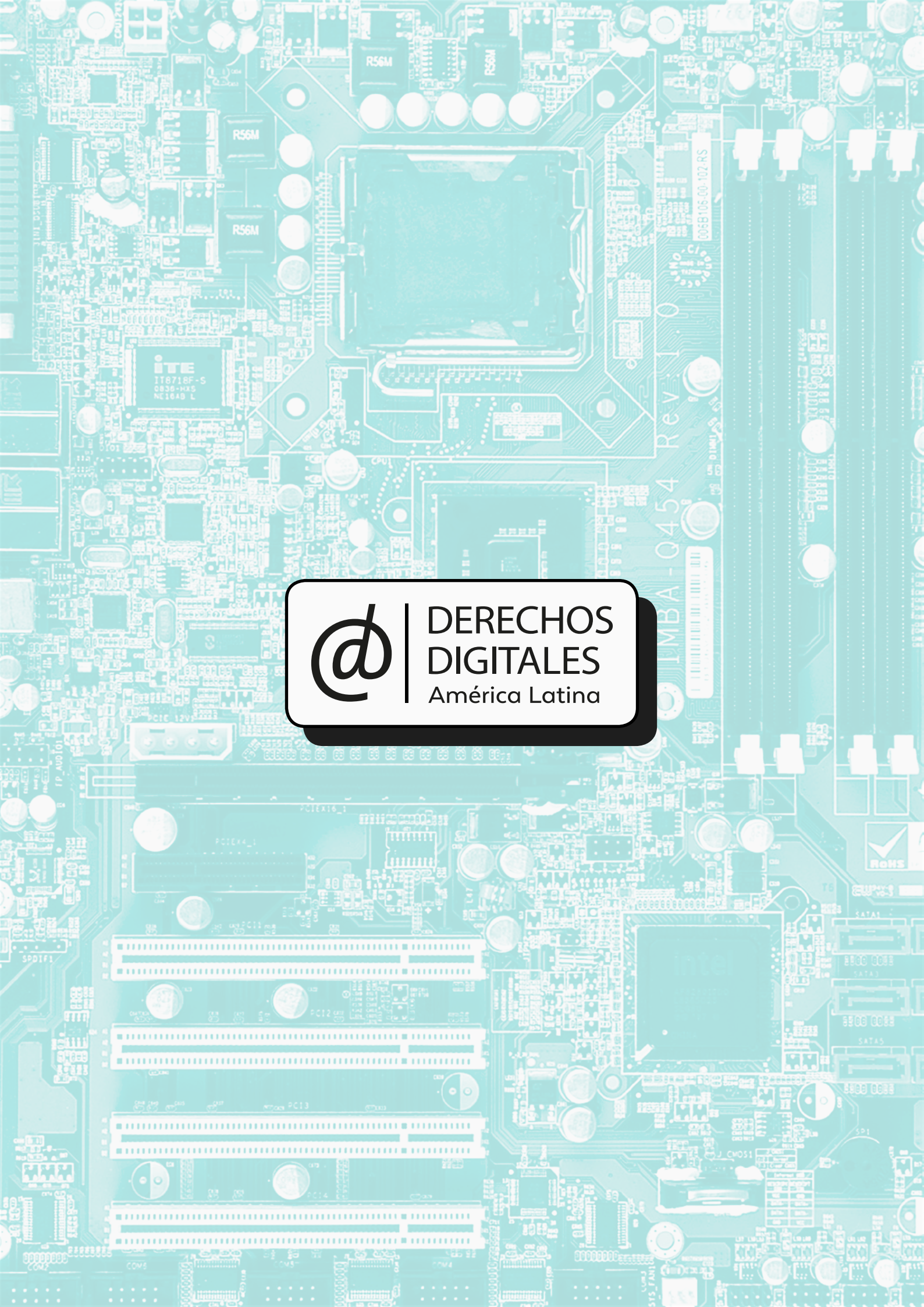
173 República de Colombia, MINTIC. RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital". Marzo, 2021. Disponible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

	¿El país es parte u observador?	Fecha de adhesión y ratificación	¿Presentó Reservas?	¿El país posee su propia ley sobre ciberdelincuencia y cooperación internacional? ¿Desde qué año?	Debates actuales importantes sobre ciberdelitos, cooperación internacional y flujo de datos para fines de conducción de investigaciones
México	Observador del Convenio[174]	(No es aplicable)	(No es aplicable)	Sí, en 1999 el Congreso inició una primera oleada de reformas de su Código Penal encargada de insertar el tema de los ciberdelitos en el texto de la ley. Además, el país cuenta actualmente con disposiciones sobre el tema en su Código Penal, la Ley de Seguridad Nacional y una Estrategia Nacional de Ciberseguridad, anunciada por el Presidente de México en 2017.	Existe un debate actual sobre una reforma de las leyes que rigen el Sistema Nacional de Seguridad Pública en el marco de la iniciativa de reforma constitucional en materia de ciberseguridad[175]_[176]

174 Consejo de Europa. Chart of signatures and ratifications of Treaty 185. Disponible en: 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? Septiembre, 2020. Disponible en: https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/

176 En septiembre de 2019, la Comisión de Seguridad Pública de la Cámara de Diputados aprobó dos dictámenes para reformar las Leyes Generales del Sistema Nacional de Seguridad Pública en materia de ciberseguridad y de Seguridad Nacional en materia de inteligencia.


DERECHOS
DIGITALES
América Latina