Budapest Convention on Cybercrime in Latin America:

A brief analysis of adherence and implementation in Argentina, Brazil, Chile, Colombia and Mexico.

Bruna Martins dos Santos

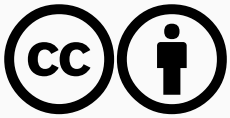
DERECHOS DIGITALES
América Latina

This report was prepared by Derechos Digitales, with support from the International Development Research Centre (IDRC).

Since 2019, Derechos Digitales has been part of the IDRC's Cyber Policy Research Centres, together with leading organizations in technology and public policy issues in the Global South.

Edition: **Derechos Digitales**
Author **Bruna Martins dos Santos**
English Translation: **Gonzalo Bernabó**
Layout and cover design: **Catalina Viera**
Revision: **J. Carlos Lara, Michel Roberto de Souza, Jamila Venturini**

**The author would like to thank Cristian León, Executive Secretary of AI Sur network; Grecia Macías and Luis Fernando García, R3D; J. Carlos Lara, Jamila Venturini and Michel Roberto de Souza, Derechos Digitales; Bárbara Simão, InternetLab; and Carolina Botero, Fundación Karisma; for their time dedicated to the interviews and the additional contributions necessary for the writing of this report.*



May 2022

Contents

I. Introduction

In November 2001, the Council of Europe decided to open for signature the text of the Convention on Cybercrime. The Budapest Convention, as it is known, is to date one of the main binding international treaties in criminal matters and was drawn up with the aim of intensifying international cooperation and "pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation". [1]

Although the opening of signatures occurred at the end of 2001, more than 20 years ago, the Convention remains one of the main topics of conversation when talking about a common agenda for international cooperation and the fight against digital crime, having influenced legislation around the world.

Among the issues covered by the Convention on Cybercrime, we can highlight the discussions on (i) criminalization of conducts; (ii) investigative standards; (iii) production of electronic evidence; and (iv) means of international cooperation, such as extradition and mutual legal assistance.[2] More recently, with the positive and growing incidence of new legislation on personal data protection worldwide, the debate on guarantees and data protection applied to the area of public safety and criminal prosecution has also entered the scene.

However, the debate is not only focused on the harmonization of cybercrime prosecution activities in a cross-border manner. An important part of the criticism directed at the Convention in recent years has been that the text promotes empty and generic criminal definitions[3] and presents adequacy implementation challenges for its signatories.

---

1 Council of Europe. Convention on Cybercrime (Budapest Convention). Available at: 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 (The Budapest Convention is promulgated in the form of the Legislative Decree n. 37). December 22nd, 2021. Available at: https://opiceblum.com.br/convencao-de-budapeste-e-promulgada-sob-a-forma-do-decreto-legislativo-no-37/

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

In light of the above, this report aims to discuss some of the main points of the Convention, as well as the challenges of implementation and harmonization of the provisions of the text with the legal systems and legal frameworks of the countries of the latin American region. For the elaboration of this report, a bibliographic review of relevant materials produced in the region has been carried out.[4] and semi-structured interviews with representatives of civil society organizations that integrate the network *Al Sur*[5] llocated in Brazil, Argentina, Colombia, Mexico and Chile.[6]

The document is therefore divided into sessions dedicated to analyzing the different situations of accession–or not-to the Convention by the countries mentioned above, as well as possible differences in local contexts. In turn, the information obtained from the individual case studies and the interviews conducted was used to formulate recommendations dedicated to the design and implementation of public policies on the subject, with an approach based on the protection of human rights in the digital sphere at its core.

4 See, for example, the series of studies published by Derechos Digitales in collaboration with Latin American organizations and specialists on the process of adapting national standards to the Budapest Convention at: https://www.derechosdigitales.org/tipo_publicacion/publicaciones/

5 Al Sur is a consortium of Latin American civil society and academic organizations with the objective of strengthening human rights in the digital environment through teamwork. More information at: https://www.alsur.lat/pt-br.

6 The interviews counted with representatives of the following organizations: Derechos Digitales (Chile), R3D (México), InternetLab (Brazil), Fundación Karisma (Colombia) and Coalizão Direitos na Rede (Brazil).

II. The Budapest Convention on Cybercrime

a. Main issues discussed by the Convention and its influence on cybercrime debates around the world

The Budapest Convention on Cybercrime consists of four chapters on (a) terminology, (b) measures to be adopted at the national level, (c) international cooperation and (d) final provisions.[7] One of the main points of the text are the typifications of cybercrimes that can be committed against the confidentiality of computer systems and data, computers, content and even copyright violations.

Despite being a treaty discussed and drafted in the context of the Council of Europe, over the years the Budapest Convention has established itself as the main legal text on international cooperation for the purpose of prosecution and combating cybercrime. The list of signatories includes 44 member states of the Council of Europe and some non-member states, such as Argentina, Canada, Chile, Colombia, United States of America, Dominican Republic and Peru.[8]

The explanatory memorandum to the Treaty raises concerns regarding the increasing malicious use of online media, as well as the accessibility and ease with which information is stored in computer systems as factors that have increased the availability of information flows, and that recent developments in new technologies and changes may have contributed to a relative increase in the ocurrence of cybercrime.[9] However, some of the highlights of the text in the commemorative activities of its twenty-first anniversary in 2021 were the potential for fostering public-private cooperation structures and harmonization between legislations and other legal and administrative structures dedicated to fighting cybercrime.[10]

---

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

8 Council of Europe. The Budapest Convention and its Protocols. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention#{%22105166412%22:[0]}

9 Council of Europe. Explanatory Report on the Budapest Convention. Available at: https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf

10 Council of Europe. Benefits. Available at: https://www.coe.int/en/web/cybercrime/benefits

In this regard, it is important to mention that despite the punitive character under which the Budapest Convention was drafted, it owes its relevance today to the constant work of updating and from a certain level of dialogue with other discussions such as those related to the defense of human rights in the digital era. And in recent years, the treaty has in fact established itself as an initial legal basis for the definition of international cooperation structures, as well as a guide for the subsequent drafting of national legislation.

The Convention also has a specific Committee, the *Cybercrime Convention Committee* (T-CY)[11], that is responsible for discussing improvements and updates to the text, and is composed of all countries that have signed or have been invited to sign the Treaty. The creation of the T-CY Committee is motivated by Article 46 of the Convention, which reinforces the need for a regular consultation mechanism between the signatories, with the main objective of promoting the exchange of information on the use and implementation of the text, the recent processes of technological and legislative innovations on the fight against cybercrime and the collection of digital evidence, and also the discussion of possible supplements or additions to the text of the convention.[12] Likewise, the collective body has functioned as one of the most relevant intergovernmental groups for the discussion and analysis of the implementation of the Convention, as well as for the elaboration of interpretations of the text through *guidance notes.*[13] Since the creation of the convention, guidance notes have been prepared on topics such as computer systems, botnets, DDoS attacks, spam, terrorism, among others.

Still in relation to the TC-Y, it is worth mentioning that the Committee is the main space for the exchange of information on the implementation and use of the Convention and has the mandate to elaborate additional protocols to

11 Cybercrime Convention Committee (T-CY). The Budapest Convention on Cybercrime: benefits and impact in practice. Available at: 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 Council of Europe. Guidance Notes on the Convention on Cybercrime. Available at: https://www.coe.int/en/web/cybercrime/guidance-notes

the original text to articulate new issues and demands of member states in the fight against cybercrime. According to the body's *Rules of Procedure*[14], he mandate allows the Committee to conduct assessments on the implementation and impact of the Convention, to adopt opinions and recommendations on possible interpretations of the text and to discuss the elaboration of legal instruments, such as conventions and additional protocols, on matters related to the Budapest Convention for submission to the Committee of Ministers of the Council of Europe for approval.

Another relevant point regarding the structure of the Convention is the 24/7 network, established by the article 35[15], which consists of a network of contact points in all signatory countries and whose representatives must be available to provide immediate assistance as soon as required. The main purpose of this network is to establish a support channel for the purpose of investigations, cybercrime proceedings or even the collection of electronic evidence. If local legislation permits, the 24/7 network may also be responsible for providing technical knowledge, implementing data preservation/protection measures and collecting digital evidence, including information on the location of suspects.

Finally, it is worth mentioning that access/adherence to the Convention also offers signatories the possibility to carry out awareness-raising and training activities by the European Committee. In a world where the dispute over the regime of access to data located abroad is a recurring theme, addressed in many legislations and bills under discussion, it is relevant that the structure provided by the Convention can promote training activities for stakeholders - even if this measure is accessible, to a large extent, only to representatives of the signatory States.

---

14 Council of Europe. Cybercrime Convention Committee (T-CY) T-CY Rules of Procedure. Octubre, 2020. Available at: 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.*

b. First Aditional Protocol

As a result of the constant work on the revision of the provisions of the Convention by the T-CY, on the basis of the provisions of Article 46 of the treaty, in January 2003, the first additional protocol was published, which refers to the incrimination of acts of a racist nature committed through computer systems.[16] which entered into force in 2006. The text, which was largely drafted by a drafting committee set up in the context of the T-CY—and subsequently submitted for evaluation by the member States—is mainly aimed at promoting greater harmonization between relevant legislation in the field of criminal law on the fight against racism and xenophobia on the internet.

Regarding the procedural issues surrounding the action of the TC-Y and its role in the development of additional protocols to the Budapest Convention, it should be clarified that the Committee can discuss suggestions for additional protocols and develop draft texts. However, the decision to adopt a given additional protocol or convention to the main treaty must be endorsed by the Committee of Ministers of the Council of Europe and, after its adoption, the text is open for accession by the signatory States of the convention—therefore, accession to the additional protocols to the Budapest Convention is not automatically realized by all signatory States.

According to the explanatory memorandum of the text[17] the rapprochement of distant parts of the world through recent technological, commercial and economic changes, would be the reason for a greater occurrence and accelerated growth in the dissemination of racially discriminatory content, xenophobia and other forms of intolerance in the online environment. Accordingly, the text provides a definition for “racist and xenophobic material” (Article 2) and aims to present common solutions to repress the dissemination of this type of content through computer systems.

16 Council of Europe. Details of Treaty No.189. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189

17 Council of Europe. 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. Available at: https://rm.coe.int/1680989b1c

The division of the protocol is made according to the following table:

Table 1 - Summary of the First Additional Protocol to the Budapest Convention

Topics	Articles
Common Provisions and General Issues	Chapter I - Common Provisions
	Chapter II - Measures to be taken at national level. — Dissemination of racist and xenophobic content by systems. — Threats on racist and xenophobic grounds — Racist and xenophobic insults — Denial, minimization, approval or justification of genocides and crimes against humanity
Relationship between the Budapest Convention and the Additional Protocol	Chapter III - Relations between the Convention and the Protocol
Final Provisions	Chapter IV - Final Provisions

Finally, it should be noted that an important aspect of the first additional protocol is the attempt to establish a balanced dynamic between the freedom of expression of Internet users and an effective fight against the dissemination and practice of racism and xenophobia in the digital sphere.

c. Second Additional Protocol

The second additional protocol concerns an effort to update the provisions of the Convention which is relatively more recent, having been adopted in December 2021 by the member States of the European Committee.[18]

The text arose once again from a decision by the T-CY on the need to tighten the rules—as highlighted in its explanatory memorandum—[19], especially with regard to the dissemination of domain name registration information, measures for direct cooperation with service providers to obtain user information, effective means for obtaining user information and traffic data, immediate cooperation in emergency cases, mutual assistance tools, as well as safeguards for the preservation of human rights in the digital environment.

The context for the creation of the second additional protocol is, however, relatively more complex than the first. In order to provide complements to the text of the Budapest Convention, the TC-Y created two Ad Hoc Groups dedicated exclusively to border access to data and issues of territorial jurisdiction (Transborder Group, created in 2012[20]) and access to data stored in the clouds (Cloud Evidence Group, established in 2015[21]). In 2016, the Cloud Evidence Group's end of discussions concluded that there was an alleged difficulty for states to access private data based on issues such as territoriality, cloud computing and scope of jurisdictions.[22] Due to the limitations discussed in the collegiate, the conclusion ended up being the elaboration of a new additional protocol that was discussed between 2017 and 2021.

18 Council of Europe. New Treaties. Available at: https://www.coe.int/en/web/conventions/new-treaties

19 Council of Europe. Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. 2022. Available at: https://rm.coe.int/1680a49c9d

20 Council of Europe. Transborder Ad Hoc Group. Available at: https://www.coe.int/en/web/cybercrime/tb

21 Council of Europe. Cloud Evidence Ad Hoc Group. Available at: https://www.coe.int/en/web/cybercrime/ceg

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

The second protocol is structured as follows:

Table 2 - Summary of the Second Additional Protocol to the Budapest Convention

Topics[23]	Articles
General provisions	Chapter I – General Provisions
Improved Cooperation	Chapter II - Measures to improve cooperation — Section I - General Principles — Section II - Procedures for the improvement of cooperation with service providers and other parties. — Section III - Procedures for the improvement of international cooperation between authorities for the exchange of data. — Section IV - Procedures for Mutual Assistance — Section V - Procedures related to international cooperation activities in the absence of international agreements.
Conditions, Safeguards and Rights	Chapter III - Conditions and Safeguards — Protection of personal data — Safeguards — General Principles
Final Provisions and Procedural Issues	Capítulo IV - Efectos del Protocolo, firma, reservas, etc.

23 Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. 2022. Available at: https://rm.coe.int/1680a49dab

According to the CoE, the second protocol comes as a necessary update to make the Budapest Convention a more effective instrument while revising issues such as data access across borders and mutual legal cooperation, and setting clearer parameters for direct cooperation between authorities and digital service providers - including at the level of Internet infrastructure service providers.[24]

However, in recent years, the debate around the second additional protocol has mobilized various sectors, in particular international civil society, due to the European Committee's attempt to establish new law enforcement rules that run counter to the principles of personal data protection and privacy.[25]

The text of the second additional protocol was the subject of a large mobilization of society and several letters demanding issues such as more space for qualified stakeholder participation, more time for discussion of the text, among others. In April 2018, 94 civil society organizations signed a letter requesting more transparency for the negotiations of the second Additional Protocol, and that the Committee invite civil society specialists to participate in the discussions and in the process of drafting the text.[26] For the organizations, in addition to the lack of transparency and proper guarantees of participation in the process, the Second Additional Protocol's attempt to standardize personal data access across borders by law enforcement and judicial authorities was worrying.

In May 2021, more letters from civil society about the process were published. The first, dated May 6, warned about the accelerated pace of discussions in the final stages of drafting the text, and that the lack of time to analyze and review the text was a factor limiting the qualified participation of the sector.[27] At the end of the same month, a new letter signed by 43 civil society organizations - among them Derechos Digitales and several Latin American organizations - was sent to the CoE

---

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. June, 2021. Available at: 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. April, 2018. Available at: https://edri.org/files/letter-cybercrimenegotiations-and-transparency_20180403_EN.pdf

27 Civil Society Letter. 6th round of consultation on the Cybercrime Protocol and civil society participation. May, 2021. Available at: https://rm.coe.int/0900001680a25788

Committee of Ministers demanding more time for a qualified analysis of the final draft of the text before the consultation process with stakeholders closes.[28]

Despite repeated calls for greater transparency and broad civil society participation in the negotiations of the text[29], it was made available for public consultation for only two weeks and after the collection of inputs had been finalized - a further factor demonstrating the haste of the debate and the lack of adherence to the demands made by civil society.[30]

With regard to sectoral participation in the process of drafting the second additional protocol, it is worth mentioning that the assessment of organizations such as the Electronic Frontier Foundation is that -despite regular consultations by the TC-Y with the participation of stakeholders[31]- the process would have failed to comply with the multi-sectoral principles of transparency, accountability and inclusiveness.[32] The monitoring of this type of agreements and negotiations by the different sectors is fundamental to ensure that the different concerns regarding the attention to human rights are heard and considered based on the context and experience of the implementation of the Convention in each country.

It is expected that the text, approved on December 17, 2021, will be made available for accession by signatories in May 2022.

---

28 Civil Society Letter. Ensuring Meaningful Consultation in Cybercrime Negotiations. Abril, 2021. Available at: 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. April, 2018. Available at: 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. Available at: https://edpb.europa.eu/system/files/2021-05/edpb_contribution052021_6throundconsultations_budapestconvention_en.pdf.

31 Council of Europe. 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].
Available at: 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. June, 2021. Available at: https://www.eff.org/deeplinks/2021/06/civil-society-groups-seek-more-time-review-comment-rushed-global-treaty-intrusive

III. The Budapest Convention in Latin American countries and current debates on the topic

a. Argentina

Argentina's accession to the Budapest Convention took place even in the face of warnings from civil society and the academic world about the breadth and ambiguity of the text and their considerations about the risks it posed to computer security research activities carried out in the country.[33] Specialists in the country warned about the increased legal insecurity for the execution of criminal investigation activities in the field of cybercrime due to the open and generic provisions existing, also in Law 26.388, for computer crimes, since both texts are not exempt from arbitrary interpretations and potential abuses from the authorities.[34]

Despite the warnings, in 2018, on the occasion of the enactment of the Law Nº 27.411[35], the country internalized the provisions of the Budapest Convention into its legal system. Argentina's accession, however, was made with reservations due to provisions that represented a potential conflict with national legislation. It therefore leaves out the provisions

33 Infobae. Argentina se suma a la Convención de Budapest para tratar delitos informáticos. (Argentina joins the Budapest Convention to deal with cybercrime). June, 2018. Available at: 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. (Argentina joins the Budapest Convention to deal with cybercrime). June, 2018. Available at: https://www.infobae.com/tecno/2018/05/13/argentina-se-suma-a-la-convencion-de-budapest-para-tratar-delitos-informaticos/

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

relating mainly to measures concerning child pornography and jurisdictional issues (the following provisions: 6.1.b[36], 9.1.d[37], 9.2.b[38], 9.2.c[39], 9.1.e[40], 22.1.d[41] and 29.4[42]).

The country has reported its active participation in the T-CY Committee and welcomed the adoption of the 2nd Additional Protocol to the Budapest Convention stating that "In order to prevent and prosecute cybercrime, it is essential to have adequate mechanisms and instruments that enable and facilitate international cooperation and assistance."[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 Ministry of Security. Cybercrime: The text of the 2nd Additional Protocol to the Budapest Convention was approved. Argentina. May, 2021. Available at: https://www.argentina.gob.ar/noticias/ciberdelito-se-aprobo-el-texto-del-2deg-protocolo-adicional-del-convenio-de-budapest

Table 3 - Summary Chart - Argentina

Is the country part or observer? Part[44]

Date of accession and ratification? Treaty ratified on June 05, 2018, and with date of entry into force of the convention as of October 01 of the same year.

Submitted Reservations? Yes, the Argentine law internalizing the provisions of the treaty leaves out the provisions mostly related to measures concerning child pornography and jurisdictional issues (the following provisions: 6.1.b[45], 9.1.d[46], 9.2.b[47], 9.2.c[48], 9.1.e[49], 22.1.d[50] and 29.4[51]).[52]

---

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

Table 3 - Summary Chart - Argentina

Does the country have its own law on cybercrime and international cooperation?
Since what year? Currently, the country has a set of laws and regulations related to the digital environment, which address issues related to the Protection of Personal Data, criminalization of behaviors practiced in the digital environment, protection of intellectual property and an additional law, as described above, which approves the text of the Budapest Convention and dictates the ways for its implementation. Relevant laws: a. Law 25.326[53], Personal Data Protection Law, b. Law 26.388[54], Amendments to the Criminal Code, c. Law 27.411[55], Approves the text of the Budapest Convention and d. Law 11.723[56], Intellectual Property Law.

53 Presidency of the Nation. Argentina. Law 25.326, Personal Data Protection. Infoleg. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

54 Presidency of the Nation. Argentina. Law 26.388, Penal Code. Infoleg. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

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

56 Presidency of the Nation. Argentina. Ley 11.723 - Régimen Legal de la Propiedad Intelectual. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

b. Brazil

Despite being, for more than 20 years, a demand from sectors such as Ministries, government agencies, Public Ministry and part of the National Congress, Brazil's accession to the Budapest Convention on Cybercrime was only approved in December 2021[57] and awaits the beginning of the implementation process.

Discussions on the subject have been quite present in the Brazilian legislative scenario and precede the approval of key laws on the digital sphere enacted in the country, such as the Civil Internet Framework[58] and the General Law on Personal Data Protection,[59] as well as some ordinary laws[60] that involved changes in the Brazilian Criminal Code to include characterizations on cybercrime. In the 2000s, a bill substituting other bills related to cybercrime introduced by Senator Eduardo Azeredo (Bill of the Chamber No. 89 of 2003[61]) already attempted to promote some level of harmonization between the typifications and discussions present in the Budapest Convention against Cybercrime. This text was strongly opposed by civil society entities, activists and academics due to the generic and ambivalent types of criminalization that it intended to introduce into the Brazilian juridical system. In response, a law aimed at protecting and guaranteeing rights in the digital sphere was proposed, which led, in 2011, to one of the first versions of the text of the Civil Framework for the Internet[62] being sent to the Chamber of Deputies.[63]

57 Federal Government, Ministry of Justice and Public Security. Approved Brazil's adhesion to the Budapest Convention on Cybercrime. December, 2021. Available at: https://www.gov.br/mj/pt-br/assuntos/noticias/aprovada-adesao-do-brasil-a-convencao-de-budapeste-sobre-o-crime-cibernetico

58 Presidency of the Republic of Brazil. Law nº 12.965, april 23, 2014, which establishes principles, guarantees, rights and duties for Internet use in Brazil. April, 2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

59 Presidency of the Republic of Brazil. Law nº 13.709, august 14, 2018, General Personal Data Protection Law . August, 2018. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

60 Relevant examples of updates made in recent years in Brazilian criminal legislation to deal with cybercrime are the law 12.737, de 30 de novembro de 2012, and 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). Available at: https://www.safernet.org.br/site/institucional/projetos/obsleg/pl-azeredo

62 Chamber of Deputies. Bill 2126/2011, which establishes principles, guarantees, rights, and duties for Internet use in Brazil. Available at: 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. Available at: https://igarape.org.br/marcocivil/pt/.

Still in the Internet Civil Framework (MCI), it is worth noting that the text continued to prosper as the main Internet legislation in the country, especially because of its approach based on the rights of Internet users and also because its drafting involved the participation of the most diverse sectors of Brazilian society. On the specific subject of online research and data storage, the MCI contains provisions on the storage and availability of records of connection and access to Internet applications. In 2018, following the example of regulatory elaboration with the participation of society, the country approved law n. 13,709/2018, or General Law on Personal Data Protection[64], responsible for establishing the basic rules for the execution of personal data processing activities in the country.

In the judicial sphere, a decision of the Federal Supreme Court (FSC) will seal a controversy over the Mutual Legal Assistance Treaty in Criminal Matters (MLAT), signed between Brazil and the United States. The doubt to be decided by the FSC is whether brazilian authorities, including the judiciary, can directly request data and information from technology companies abroad, thus dispensing with international legal cooperation procedures for obtaining content from internet applications located abroad. In 2020, the FSC held a public hearing to listen to experts in the field[65], in which they referred at various times to the concepts provided by the Budapest Convention, as well as the need to respect human rights.[66]

At the end of 2019, the country received the invitation to become a signatory to the Convention with a maximum term of 3 years to complete the process. Less than 2 years later, in December 2021, Legislative Decree No. 37 of 2021[67] was enacted, that "Approves the text of the Convention on Cybercrime, concluded in Budapest on November 23, 2001", with no reservations suggested to the text of the Convention.

64 Presidency of the Republic of Brazil. Personal Data Protection General Law. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

65 FSC. Public hearing n. 29. Available at: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf

66 The case is scheduled for trial in May 2022. STF. ADC 51. Available at: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379

67 Federal Senate. Projeto de Decreto Legislativo n. 255 de 2021. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/150258

Despite being celebrated by some government authorities and the private sector[68], the process raised many concerns on the part of brazilian civil society[69]- [70]regarding issues such as (i) approval in a shorter time frame than expected; (ii) held without any multisectoral debate on the subject; (iii) the absence of a general data protection law dedicated to criminal prosecution and public safety activities;[71] and (iv) and having been approved during the process of rediscussion of the Brazilian Code of Criminal Procedure, which contains sections dedicated exclusively to regulating online research activities, data collection and cooperation between authorities and companies.

Likewise, another key point that was questioned was the nature of total and unrestricted adherence to the Convention, ignoring the provisions of the Treaty on "the need for alignment between its content and the signatories' domestic standards and international human rights instruments"[72] and mechanisms such as declarations (art. 40 of the Convention) and reservations (art. 42). Such mechanisms exist precisely to facilitate the process of internal conformity and encourage the exercise of sovereignty of each country wishing to join the group of signatories. In this sense, the speed with which the Brazilian State's accession process was carried out is a factor of great concern, since it may have made any analysis of conformity with the Brazilian legal system unfeasible in light of the legislation that has been passed in the country in recent years

Below is a table highlighting the points of two of the main bills underway in the Brazilian Congress on issues related to the Budapest Convention:

68 Brasscom. Empresas de tecnologia defendem a adesão do Brasil à Convenção de Budapeste. Available at: 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. October, 2021. Available at: 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. November, 2021. Available at: 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. July, 2021. Available at: 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 Article 15, of the Budapest Convention on Cybercrime.

Table 4 - Bills in Brazil	
Bills	**Relevant points**
Bill 2630/2020, Establishing the Brazilian Law of Freedom, Responsibility and Transparency on the Internet [73]	— Determines that Internet application providers operating in Brazil must be headquartered and appoint legal representatives in the country.[74] — Creates a new criminal offense on the promotion or financing of the use of automated accounts and other means to disseminate content that is not truthful (disinformation) or subject to criminal sanction.
Bill 8045/10, about the Code of Criminal Procedure [75]_[76]	— Creates alternatives to the topic of precautionary measures such as the use of mechanisms such as electronic monitoring and electronic address blocking.[77] — Seeks to increase the possibilities for the use of telephone interception. — Modifies the part relating to electronic evidence, allowing the monitoring of persons under investigation, interception of data at rest and others. — Addresses the possibilities of international legal cooperation for the instruction or production of evidence.

In addition to the draft laws highlighted above, the country has also been analyzing the possibility of drafting and approving a General Law on Personal Data Protection applicable to the field of public security[78]. A draft bill has been prepared by a commission of jurists set up by the president of the Chamber of Deputies[79] and focuses a considerable part of its provisions on the dichotomy between the setting up of safeguards and guarantees to protect the rights of individuals versus the conduct of research in the digital environment. However, this preliminary draft has not yet been presented as a bill.

---

73 Chamber of Deputies. Bill. 2630/2020, Establishing the Brazilian Law of Freedom, Responsibility and Transparency on the Internet. April, 2020. Available at: https://www.camara.leg.br/propostas-legislativas/2256735

74 Report of the Working Group aimed at preparing the opinion on the 2630/2020 bill. Available at: 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 Chamber of Deputies. Bill 8045/10, concerning the Code of Criminal Procedure, Available at: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

76 Chamber of Deputies. Opinion of the draftsman of the Special Committee to analyze the bill of the Criminal Procedure Code, João Campos. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1998270&filename=Parecer-PL804510-26-04-2021

77 Chamber of Deputies. See the main points of the reform of the Code of Criminal Procedure. Available at: https://www.camara.leg.br/noticias/210377-veja-os-principais-pontos-da-reforma-do-codigo-de-processo-penal/

78 Supreme Court of Justice. Commission delivers draft bill to the House of Representatives on processing of personal data in the criminal area. November 2021. Available at: 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 The Preliminary Draft Law, in the version presented by the Commission of Jurists, is available here: 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

Table 5 - Summary Chart - Brazil

Is the country part or observer? Currently, the country has observer status in the Convention. However, the invitation for accession came in 2019.[80]

Date of accession and ratification? The accession process was formalized by the Brazilian Congress in December 2021 with the issuance of Legislative Decree No. 37 of 2021[81]. The ratification date is not yet confirmed, as the process depends on a final phase of executive action and confirmation of ratification.

Submitted Reservations? No.

Does the country have its own law on cybercrime and international cooperation? Since what year? Yes, since 1999, the creation of a law dedicated exclusively to the fight against cybercrime has been debated in the country. Although Bill 84/99 (PL Azeredo) was the first to be debated more categorically, the country currently has a set of laws on the subject of the fight against cybercrime:

- Law 14.197/2021 - Law for the Defense of the Democratic Rule of Law[82]
- Law 12.737/2012 - Provides for the criminal characterization of computer crimes[83]

Important current discussions on cybercrime, international cooperation and data flow for purposes of conducting investigations.

- Bill 8045/10, which modifies the Code of Criminal Procedure[84]
- Discussions around a Bill for a General Law on Data Protection for Public Security, which has not yet been presented but which has had a working group of jurists in congress.[85]

80 Council of Europe. Chart of signatures and ratifications of Treaty 185. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

81 Official Gazette. Legislative Decree n. 37 de 2021. December, 2021. Available at: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/12/2021&jornal=515&pagina=7&totalArquivos=188

82 Presidency of the Republic of Brazil. Law nº 14.197, on september 1st, 2021, that Extends Title XII in the Special Part of Decree-Law nº 2.848, of December 7, 1940 (Penal Code), regarding crimes against the Democratic State of Law; and revokes Law No. 7.170 of December 14, 1983 (National Security Law) and provisions of Decree Law No. 3688 of October 3, 1941 (Law of Criminal Misdemeanors)). September 2021. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14197.htm#:~:text=359%2DR.,a%208%20(oito)%20anos

83 Presidency of the Republic of Brazil. Law No. 12,737, of November 30, 2012, which Provides for the criminal typification of computer crimes; amends Decree-Law No. 2,848, of December 7, 1940 - Criminal Code; and makes other provisions. November 2012. Available at: http://planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

84 Chamber of Deputies. Bill 8045/2010, on the Code of Criminal Procedure. Available at: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

85 Supreme Court of Justice. Commission submits to the Chamber a draft bill on the treatment of personal data in the criminal area. November, 2021. Available at: 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

Chile's accession to the Budapest Convention was formalized before the Council of Europe in April 2017, days before the enactment of Decree No. 83/2017, which "promulgates the convention on cybercrime."[86] The need to reinforce the commitment made at the national level to ensure cybersecurity in the country (through the National Cybersecurity Policy) and to be part of a rapid and effective system of international cooperation, as well as to establish channels for the exchange of knowledge on the fight against cybercrime are some of the main reasons given by the Chilean government for joining the treaty.[87]

Regarding the reservations submitted, it is worth mentioning that in the Chilean case the accession document to the Budapest Convention deposited at the Council of Europe left out, provisions mostly related to measures concerning the possibility of application of national law, child pornography and jurisdictional issues (the following provisions: 6.1[88], 9.2.b[89], 9.2.c[90], 9.4[91], 22.1.b[92] and 29.4[93]). Just like Argentina, the country also reserves the right to reject requests for international assistance in cases where the behavior is not criminalized under Chilean law.

---

86 BCN Chile. Decree 83, promulgates the convention on cybercrime. Available at: https://www.bcn.cl/leychile/navegar?idNorma=1106936

87 Ministry of Foreign Affairs of Chile. Chile deposits instrument of accession to the Budapest Convention on Cybercrime. April, 2017. Available at: 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.

It is important to mention that, recently, a bill was discussed and approved in the country dedicated to modernize Law 19223/92, which "typifies criminal behaviors related to informatics, creating new crimes". The text of the bill in question is also dedicated to update other legal texts in force in the country in order to promote a better level of compliance with the Budapest Convention.[94]

In line with the above, Bill No. 12.192-25[95] establishes rules on computer crimes, revokes Law 19,223 and amends other legal corps in order to adapt them to the Budapest Convention. The text received considerable pressure from the Government for its rapid approval.[96] Among the points that were excluded from the text in its final stage was the possibility of modifying the Penal Code to allow the Public Prosecutor's Office to request data from citizens at any time, without a court order or a specific transparency and accountability mechanism, to which representatives of civil society, academia and business associations were strongly opposed.[97]

94 Senate of the Republic of Chile. Bill that modernizes rules on computer crimes will be analyzed by a Joint Commission. October 2021. Available at: https://www.senado.cl/proyecto-que-moderniza-normas-sobre-delitos-informaticos-sera-analizado

95 Bulletin 12192-25, which establishes rules on computer crimes, repeals Law No. 19.223 and modifies other legal bodies to adapt them to the Budapest Convention. Available at: 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. January, 2022. Available at: 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. January, 2022. Available at: https://www.derechosdigitales.org/17623/en-rechazo-a-la-modificacion-del-codigo-procesal-penal-que-habilita-la-vigilancia-sin-controles-ni-contrapesos-legales/

Table 7 – Bills in Chile	
Bills	**Relevant Points**
Bill 12192-25, which seeks to amend the current regulation (Law n.19.223) that typifies behaviors related to computer systems.	— Aims to promote a higher level of alignment between Chilean legislation dedicated to the fight against cybercrime and the Budapest Convention; — Attempted changes that were ultimately rejected, including: * A relative reduction in the control of state investigative activities while seeking to introduce mechanisms for requesting data from citizens without sufficient safeguards; * A flexibilization of invasive investigative measures in force in the Chilean criminal justice system, including a modification of Article 219 of the Code of Criminal Procedure that talks about the interception of private communications; * Alternatives to introduce into the Chilean criminal procedure system the possibility of collecting data from individuals without a specific court order authorizing the act.

The modifications proposed and rejected for the Chilean legislation in the case of Bill 12.192-25 followed a worrying tendency to instrumentalize the process of adaptation to the Budapest Convention as an excuse to reduce the control and transparency of the State's research activities, tending to the violation of the privacy of citizens.

Table 8 - Summary Chart - Chile

Is the country part or observer? Chile is part of the Budapest Convention.[98]

Date of accession and ratification? Treaty ratified on April 20, 2017 and with entry into force of the convention as of August 1 of the same year.

Submitted Reservations? Yes, the Chilean accession document to the Budapest Convention left out provisions mostly related to domestic law enforcement measures, child pornography and jurisdictional issues (articles 6.1[99], 9.2.b[100], 9.2.c[101], 9.4[102], 22.1.b[103] and 29.4[104]). Just like Argentina, the country also reserves the right to reject requests for international assistance in cases where the behavior is not criminalized under Chilean law.[105]

Does the country have its own law on cybercrime and international cooperation? Since what year? Law 19223/92, which typifies criminal offenses related to computer crimes.[106]

Important current discussions on cybercrime, international cooperation and data flow for purposes of conducting investigations. Bill 12.192-25, which establishes rules on computer crimes, repeals Law No. 19,223 and amends other legal entities to adapt them to the Budapest Convention.[107]-[108], approved in Congress in March 2022.

---

98 Council of Europe. Chart of signatures and ratifications of Treaty 185. Available at: 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 Council of Europe. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185) - Chile. Available at: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=Chi

106 Library of the National Congress of Chile. Law 19223 Typifies criminal offenses related to Informatics. May, 1993. Available at: https://www.bcn.cl/leychile/navegar?idNorma=30590

107 Chamber of Deputies of Chile. Bill Amends Law No. 19.223 which typifies criminal offenses related to information technology, incorporating a new crime. Available at: https://www.camara.cl/verDoc.aspx?prmID=14367&prmTIPO=INICIATIVA

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

d. Colombia

In the Colombian case, the discussion and elaboration of public policies on issues related to cybercrime have favored perspectives related to cyber defense and security and aim to facilitate the use of information in judicial processes and to prevent or anticipate the consummation of cybercrimes, as pointed out by *Fundación Karisma*[109]. In 2018, the organization pointed out that the country needed a more comprehensive public policy on criminal matters and that it needed to resolve the precariousness present in Law n. 1.273/2009[110] - which institutes in the country the notion of preservation of data and information systems, as well as communications- before moving forward in the negotiations for accession to the Budapest Convention.

However, the country enacted Law No. 1928 of July 24, 2018, approving the text of the Budapest Convention on Cybercrime.[111]Already the instrument of accession to the Budapest Convention was deposited with the Council of Europe in March 2020.[112]In the Colombian case, the reservations presented refer to the possibility of the country to apply the measures mentioned in articles 20 (collection of real-time transit data) and 21 (interception of content data) of the Convention in accordance with its internal regulations on personal data and protection of the right to privacy.

Among the motivations given by the government for membership were the increasing incidence of cybercrime in the early months of the Covid-19 pandemic and the need for more tools to deal with cybercrime through international cooperation between countries.[113] The facilitation of transnational cybercrime investigations through the formalization of information exchange channels between the countries that have signed the Convention, in addition to the possibility of accessing projects and

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

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

111 Vlex. Law 1928 from July 24th 2018 Senate. July, 2018. Available at: https://vlex.com.co/vid/ley-1928-24-julio-737603069

112 Government of Colombia, Ministry of Foreign Affairs of Colombia. Colombia accedes to the Budapest Convention against cybercrime. March, 2020. Available at: 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. April 07 2020. Available at: 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

programs of access and transfer of knowledge on the topics of the Convention, were some of the other benefits claimed by the Colombian government.[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. April 07 2020. Available at: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126496:Adhesion-al-Convenio-de-Budapest-contra-la-ciberdelincuencia-clave-para-Colombia-en-tiempos-de-Coronavirus

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

Table 8 - Summary Chart - Colombia

Is the country part or observer? Colombia is part of the Convention, invitation made in 2019. [116]

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

Submitted Reservations? Yes, the reservations submitted are intended to allow the country to apply the measures mentioned in Articles 20 (collection of real time transit data) and 21 (interception of content data) of the Convention in accordance with its domestic legislation on personal data and protection of the right to privacy.[117]

Does the country have its own law on cybercrime and international cooperation? Since what year?

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

Important current discussions on cybercrime, international cooperation and data flow for purposes of conducting investigations. In March 2021, the Ministry of Information Technologies and Communications published Resolution n. 500/2021, which establishes the guidelines and standards for the digital security strategy and adopts the security and privacy model as an enabler of the Digital Government policy.[120]

116 Council of Europe. Chart of signatures and ratifications of Treaty 185. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty treaty no=185

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

118 Official Journal, Colombia. Law 1273, 2009, which amends the Penal Code. Available at: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

119 Vlex. Law 1928 July 24th, 2018 Senate. July, 2018. Available at: https://vlex.com.co/vid/ley-1928-24-julio-737603069

120 Republic of Colombia, MINTIC. Resolution number 00500 of March 10, 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". March, 2021. Available at: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

e. Mexico

Mexico represents a particular case, since it is only listed as an observer to the Convention and has not yet formalized its accession, despite having applied for membership in 2006. The lack of formalization, however, has not prevented the Convention from also having a certain level of influence in the local debate on the fight against cybercrime. As in other countries in the region, repeated attempts have been made in Mexico to transpose specific provisions to the national legal system, and this has been the driving force behind the draft laws aimed at updating Mexican legislation on cybercrime.

The country has its own legal framework applicable to certain cases of cyber crimes, which is constituted by the Penal Code.[121], National Security Law[122] and some other scattered rules.[123]

For the specialists interviewed during the preparation of this report, there would exist a dangerous tendency of legitimization of the texts of the convention and use of the justification of the need for the implementation of its text for the production of harsher laws, dedicated to implement more control and surveillance measures in the criminal process, in addition to deliberately vague, imprecise and broad criminal offenses. In this sense, with respect to Mexico's accession, some risk factors could be an eventual strengthening of the capacities and competencies of an authoritarian State, and even more so legislative initiatives that end up legitimizing the already existing abuses of the Mexican criminal procedural system.[124]In the event that the country continues with the process of accession to the Budapest Convention, it would be necessary an even greater attention from all sectors involved in the issue, especially to help resolve possible ambiguities between the text of the Treaty and the Mexican system and the Inter-American Human Rights System. Some of the issues of attention would be: protection of whistleblowers, guarantee of the right to freedom of expression, use of copyrighted materials.

---

121 Justia México. Federal Penal Code. Available at: https://mexico.justia.com/federales/codigos/codigo-penal-federal/

122 Official Gazette of the Mexican Federation. National Security Law. Available at: 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. September, 2020. Legal Forum. Available at: https://forojuridico.mx/el-estatus-de-mexico-y-el-convenio-sobre-la-ciberdelincuencia-de-budapest/

124 Interview performed with Grecia Macias and Luis Fernando Garcia, Lawyer and Executive Director of the Network in Defense of Digital Rights. - R3D.

An investigation conducted by Mexican organization R3D with the support of Derechos Digitales in June 2018 pointed out some persistent inconsistencies between Mexican legislation and the Convention, especially as a function of the legal uncertainty generated by the broad and generic typifications of cybercrimes established in the Treaty.[125] The organization also points out that after the country's eventual accession to the Convention, a thorough analysis would be necessary on issues such as jurisdictional competencies, the level and instance of implementation, and even the possible drafting of a new special law or the modification of laws in force in the country's federal entities in order to promote greater harmonization and guarantee the exact application of the Criminal Law.[126]

Currently, the country has discussed - at least - 13 bills dedicated to the field of cybersecurity and dedicated to institute in the country a Cyber Security Law with criminalization of behaviors such as cybercrimes, cyber threats, the creation of a national cybersecurity agency and other discussions.[127] Additionally, it is worth noting that in 2017 a National Cyber Security Strategy (ENCS, for its acronym in Spanish)[128] was edited for the country, as a guiding document of the Mexican State and that brings as main objectives the a. promotion of collaboration between different sectors, b. the need for analysis and mapping of risks and threats in cyberspace, c. the promotion of the responsible use of information and communication technologies, among others.

Yet regarding the ENCS, it is worth noting that civil society organizations -such as R3D- have reinforced the importance of adopting a human rights-based approach, and have claimed that the Strategy should be openly discussed with society precisely because it proposes modifications to the legal and juridical frameworks with which cybercrimes are typified, which could represent a threat to the exercise of freedoms and rights on the Internet.[129] More recently, the country initiated the discussion of a

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

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

128 Mexican Government. National Cybersecurity Strategy. 2017. Available at: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

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

constitutional reform on cybersecurity with the aim of allowing the Mexican Congress to have the competence to draft laws on national security, including cybersecurity and protection of human rights in cyberspace, establishing the requirements and limits to the corresponding investigations.[130] On this issue, civil society organizations also warned, in a letter sent to the Mexican Congress in 2021, that the text also presented risks in that the ambiguity and breadth of what is considered as conduct that threatens national security would impede to have clarity and certainty on the scope, content and limits of the exercise of power and restriction of the State towards the rights and freedoms of society.[131]

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

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

Table 9 - Summary Chart - Mexico

Is the country part or observer? Mexico is Observer [132]

Date of accession and ratification? Country is not a signatory.

Submitted Reservations? Country is not a signatory.

Does the country have its own law on cybercrime and international cooperation?
Since what year? Yes, in 1999 Congress initiated a first wave of reforms to its Penal Code in charge of inserting the topic of cybercrime into the text of the law. In addition, the country currently has provisions on the subject in its Criminal Code, the National Security Law and a National Cybersecurity Strategy, announced by the President of Mexico in 2017.

Important current discussions on cybercrime, international cooperation and data flow for purposes of conducting investigations.
There is an ongoing debate on a reform of the laws governing the National Public Security System within the framework of the constitutional reform initiative on cybersecurity. [133] [134]

132 Council of Europe. Chart of signatures and ratifications of Treaty 185. Available at: 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? September, 2020. Available at: https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/

134 In September 2019, the Public Security Commission of the Chamber of Deputies approved two resolutions to reform the General Laws of the National Public Security System on cybersecurity and of National Security on intelligence matters.

IV. The debate on Cybercrime beyond the Budapest Convention

Despite being one of the main texts on the subject, the Budapest Convention on Cybercrime is not the only recent initiative being discussed worldwide. In recent years, more and more forums and spaces such as the United Nations (UN) or the Organization for Economic Cooperation and Development (OECD) have been discussing the fight against cybercrime and ways to foster more channels of cooperation between authorities. These discussions include reflection on how to allow and request access to the data of individuals under investigation within guidelines and safeguards that are in line with international human rights standards.

In December 2019, the UN General Assembly approved in a resolution[135] the creation of an ad hoc committee to draft a new international treaty to combat cybercrime, despite objections from countries such as the United States and blocs such as the European Union.[136] The Resolution[137] determines that the Committee will be composed of specialists from all regions of the world and will seek to develop a new Convention on combating the use of technology for criminal purposes, taking into consideration international instruments and existing efforts at the national, regional and international levels.

Civil society organizations with international participation expressed concern about the speed of the process and the lack of evidence of the need for it. In a letter to the ad hoc Committee in 2019, the same organizations warned about the lack of a clear and well-defined objective for the Treaty text considered, noting that the use of generic terms and definitions opens up the possibility of criminalizing online conduct that are currently protected by international human rights standards and norms.[138]

135 United Nations. General Assembly Resolution. Countering the use of information and communications technologies for criminal purposes. December 2019. Available at: https://undocs.org/A/Res/74/247

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

137 United Nations. General Assembly Resolution. Countering the use of information and communications technologies for criminal purposes. December 2019. Available at: 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. Available at: https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human

The treaty discussed by the UN is a long-standing proposal expressed by countries such as Russia[139] as a new global instrument capable of replacing the Budapest Convention. In addition to concerns about the origin of the initiative, which in its early versions was also supported by authoritarian regimes such as China, Cambodia and other countries,[140] another point of concern raised by third sector entities is the lack of transparency and common spaces for social participation in the discussions held at the United Nations, which continues to have many limitations for the participation of entities that do not have ECOSOC status.[141]

In addition to the discussions conducted by the UN, it is also worth mentioning the recent discussions conducted by the OECD on government access to personal data. The discussion, conducted exclusively within the scope of the Committee on Digital Economy Policy - CDEP and in the context of the recent review of the implementation of the OECD 1980 Privacy Guidelines, identified *"unconstrained and disproportionate government access to personal data held by the private sector as a crucial issue for data governance and the protection of individual rights and as a potential barrier to enabling the free flow of data with trust"*.[142]

However, in December 2021 the initiative aimed at developing high-level principles or guidance for OECD member countries regarding reliable government access to personal data stored by the private sector was discontinued until further notice by the OECD due to disagreements and lack of consensus among CDEP member countries[143]–[144]

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

Within the framework of the Organization of American States (OAS), a Working Group on Cybercrime was created in 1999 by the Meeting of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA), a political and technical forum on justice and international legal cooperation. The objective of this Working Group is to strengthen international cooperation in the prevention, investigation and prosecution of cybercrime, facilitate the exchange of information and experiences among members, and recommend actions necessary to strengthen cooperation among member states in this area. Among other things, this Group also promotes the recommendation for States to accede to the Budapest Convention and encourages States to develop national cybercrime strategies.[145] In addition to providing training programs,[146] the group consolidates the development of the topic in each State, publishes an Inter-American Cooperation Portal on Cybercrime,[147]and also facilitates the exchange of consolidated information on the authorities.[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. Conclusion and Recommendations

The implementation and discussion scenario of the accession processes in countries such as Chile, Brazil, Argentina, Colombia, and Mexico tends to be quite similar in aspects such as (a) lack of participation of the interested sectors in a relevant way, (b) the speed in discussing laws and enacting decrees without transparency and in haste, (c) the utilization of the need to comply with the Budapest Convention to promote comprehensive reforms of the current penal and criminal procedure legislation that pose risks to citizens' rights such as the right to privacy, the right to data protection, and due legal process.

Despite the Budapest Convention being a text of great relevance for matters of international cooperation in criminal matters, the fact that the text was developed in a legal and political system different from that in force in Latin American countries makes the adaptation process relatively more costly for the countries of the region and requires even greater attention to compliance with the standards developed in the Inter-American system for the protection of human rights.

In this sense, as a final part of this document, we present recommendations for the different sectors on the respective processes of accession and implementation of the Budapest Convention in the region, as well as participation in future discussions on issues such as international cooperation, government access to data of investigated subjects and the fight against cybercrime.

To States and national governments

1. Conducting multisectoral discussions on the accession process of the countries to the group of signatories of the Convention in order to facilitate a mapping of the risks and inconsistencies of the text with the local legal system, as well as a frank and proactive discussion on the presentation of possible reservations and the process of implementation of the International Treaty;

2. Conduct an analysis of adequacy of the Budapest Convention and its protocols, in accordance with the human and fundamental rights recognized by the State, avoiding its use only as a common basis for the discussion of possible paths in the fight against cybercrime.

3. Avoid merely copying the criminal offenses addressed in the text of the Convention, as this raises doubts about their application;

4. Guarantee full respect for the fundamental rights of its citizens recognized in the respective Constitutions and laws in force, for the performance of criminal prosecution activities in the digital environment by establishing clear and specific guarantees;

5. Include all stakeholders in future discussions on new criminalizations for cybercrime, international legal cooperation mechanisms, research and others. The multi-stakeholder model should also be taken into account in the discussion of issues related to the Budapest Convention, as well as in most Internet policy-making processes.

6. Latin American countries have an obligation to ensure that their commitments are reflected in their adherence to and implementation of the Budapest Convention, so they cannot, in this discussion, ignore the human rights obligations that underpin the Inter-American human rights system.

7. Avoid the punitive and worrying trend of criminal law as the only way forward. The tradition of South American countries in terms of police abuses and human rights violations by authoritarian regimes should be the main reason to consider and discuss guarantees of human rights protection in the digital sphere for the continent.

To non-governmental sectors

8. Raise awareness in society about possible and eventual governmental abuses in the implementation of the Budapest Convention on Cybercrime, as well as in the execution of criminal prosecution activities in the digital sphere by the State;

9. Conduct training activities for citizens, third sector organizations and the academic world on the main international cooperation instruments in force, as well as aspects of their implementation.

10. To monitor and act on the legislative impact of the worrying instrumentalization of the process of adaptation to the Budapest Convention as a pretext to reduce the control and transparency of the state's investigative activities, with violations of fundamental guarantees and the privacy of citizens.

11. Document the processes of participation in discussions on new cybercrime typifications, international legal cooperation mechanisms, research and others.

12. Explore new lines of research and complementary studies in Latin America on the regional importance and evolution of the forms of institutionalization of the fight against cybercrime, including the implementation of bilateral agreements on mutual legal assistance in criminal matters (MLAT) and international legal cooperation.

Annex I - Table of Country Situation Analysis

	Is the country part or observer?	Date of accession and ratification	Submitted Reservations?	Does the country have its own law on cybercrime and international cooperation? Since what year?
Argentina	Part [149]	Treaty ratified on June 05, 2018, and with date of entry into force of the convention as of October 01 of the same year.	Yes, the Argentine law internalizing the provisions of the treaty leaves out the provisions mostly related to measures concerning child pornography and jurisdictional issues (the following provisions: 6.1.b, 9.1.d, 9.2.b, 9.2.c, 9.1.e, 22.1.d and 29.4) [150] [151]	— Law 25.326 [152], Personal Data Protection Law — Law 26.388 [153], Amendments to the Criminal Code — Law 27.411 [154], Approves the text of the Budapest Convention — Law 11.723 [155], Intellectual Property Law

149 Council of Europe. Chart of signatures and ratifications of Treaty 185. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

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

151 Council of Europe. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185). Available at: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=ARG

152 Presidency of the Nation. Argentina. Law 25.326, Protection of Personal Data. Infoleg. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

153 Presidencia de la Nación. Argentina. Law 26.388, Penal Code. Infoleg. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

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

155 Presidency of the Nation. Argentina. LAW 11.723 - Intellectual Property Legal Regime. Available at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

	Is the country part or observer?	Date of accession and ratification	¿Presentó Reservas?	Does the country have its own law on cybercrime and international cooperation? Since what year?	Important current discussions on cybercrime, international cooperation and data flow for purposes of conducting investigations.
Brasil	Currently, the country has observer status in the Convention. However, the invitation for accession came in 2019. [156]	The accession process was formalized by the Brazilian Congress in December 2021 with the issuance of Legislative Decree No. 37 of 2021. [157] The ratification date is not yet confirmed, as the process depends on a final phase of executive action and confirmation of ratification.	No	Yes, since 1999, the creation of a law dedicated exclusively to the fight against cybercrime has been debated in the country. Although Bill 84/99 (PL Azeredo) was the first to be debated more categorically, the country currently has a set of laws on the subject of the fight against cybercrime: — L14197 - Law for the Defense of the Democratic Rule of Law [158] — 12.737/2012 - Provides for the criminal characterization of computer crimes. [159]	— Criminal Procedure Code Amendment [160] — Discussions around a Bill for a General Law on Data Protection for Public Security, which has not yet been presented but which has had a working group of jurists in congress. [161] — Draft Fake News Bill. [162]

156 Council of Europe. Chart of signatures and ratifications of Treaty 185. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

157 Official Gazette. Legislative Decree n. 37 of 2021. December, 2021. Available at: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/12/2021&jornal=515&pagina=7&totalArquivos=188

158 Presidency of the Republic of Brazil. Law No. 14,197, of September 1, 2021, Expanding Title XII of the Special Part of Decree-Law No. 2,848, of December 7, 1940 (Penal Code), concerning crimes against the Democratic State of Law; and revoking Law No. 7,170, of December 14, 1983 (National Security Law), and the provisions of Decree-Law No. 3,688, of October 3, 1941 (Law on Criminal Misdemeanors). September, 2021. Available at: 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 Chamber of Deputies. Bill n. 8045/2010, on the Criminal Procedure Code. Available at: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

161 Supreme Court of Justice. Commission submits to the House a draft bill on the treatment of personal data in the criminal area. November, 2021. Available at: 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 Chamber of Deputies. Bill n. 2630/2020, Instituting the Brazilian Law of Freedom, Responsibility and Transparency on the Internet. April, 2020. Available at: https://www.camara.leg.br/propostas-legislativas/2256735

	Is the country part or observer?	Date of accession and ratification	¿Presentó Reservas?	Does the country have its own law on cybercrime and international cooperation? Since what year?	Important current discussions on cybercrime, international cooperation and data flow for purposes of conducting investigations.
Chile	Part [163]	Treaty ratified on April 20, 2017 and with entry into force of the convention as of August 1 of the same year.	Yes, the Chilean accession document to the Budapest Convention left out provisions mostly related to domestic law enforcement measures, child pornography and jurisdictional issues (articles 6.1, 9.2.b, 9.2.c, 9.4, 22.1.b e 29.4). Just like Argentina, the country also reserves the right to reject requests for international assistance in cases where the behavior is not criminalized under Chilean law. [164]	Law 19223/92, which typifies criminal offenses related to computer crimes [165] Bill No. 12192-25, establishes rules about cybercrime, repeals Law No. 19223, and modifies other legal bodies to adequate them to the Budapest Convention. [166]	Law bulletin n. 12.192-25, which establishes rules on computer crimes, repeals Law No. 19,223 and amends other legal entities to adapt them to the Budapest Convention. [167] [168]

163 Council of Europe. Chart of signatures and ratifications of Treaty 185. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

164 Council of Europe. Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185) - Chile Colombia. Available at: 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 Library of the National Congress of Chile. Law 19223 Typifies criminal figures related to Informatics. May, 1993. Available at: https://www.bcn.cl/leychile/navegar?idNorma=30590

166 Senate of Chile, 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. Available at: https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=12192-25

167 Chamber of Deputies of Chile. Bill Amends Law No. 19,223 which typifies criminal offenses related to information technology, incorporating a new crime. Available at: https://www.camara.cl/verDoc.aspx?prmID=14367&prmTIPO=INICIATIVA

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

	Is the country part or observer?	Date of accession and ratification	¿Presentó Reservas?	Does the country have its own law on cybercrime and international cooperation? Since what year?	Important current discussions on cybercrime, international cooperation and data flow for purposes of conducting investigations.
Colombia	Part, invitation made in 2019. [169]	03/16/2020, with entry into force of the convention on July 1, 2020.	Yes, the reservations submitted are intended to allow the country to apply the measures mentioned in Articles 20 (collection of real time transit data) and 21 (interception of content data) of the Convention in accordance with its domestic legislation on personal data and protection of the right to privacy.[170]	— Law n. 1273/2009 [171] — Law n. 1928/2019[172]	In March 2021, the Ministry of Information Technologies and Communications published Resolution n. 500/2021, which establishes the guidelines and standards for the digital security strategy and adopts the security and privacy model as an enabler of the Digital Government policy. [173]

169 Council of Europe. Chart of signatures and ratifications of Treaty 185. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty treaty no=185

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

171 Official Gazette, Colombia. Law 1273 of 2009, which modifies the Penal Code. Available at: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

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

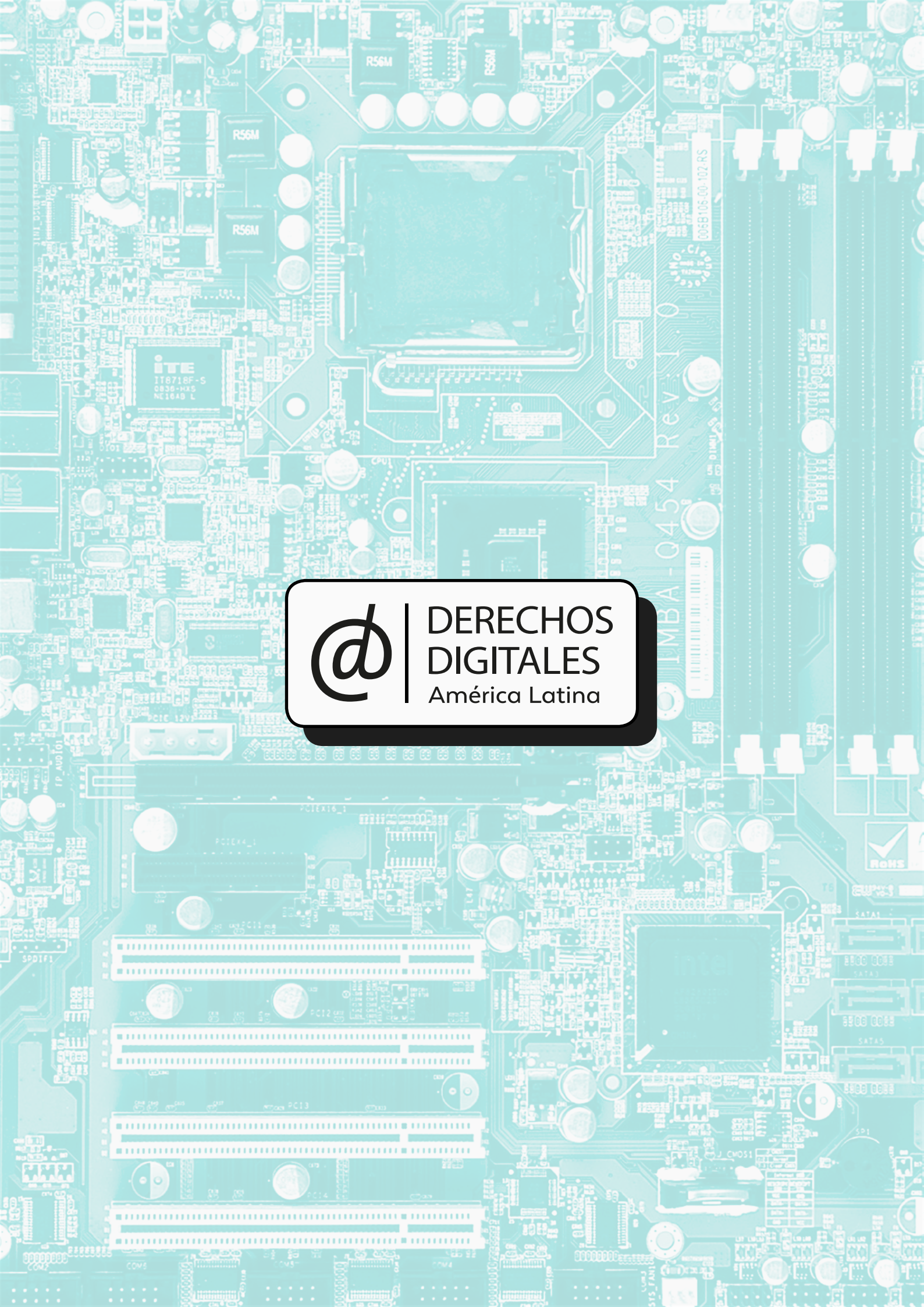
173 Republic of Colombia, MINTIC. RESOLUTION NUMBER 00500 OF MARCH 10, 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital". March, 2021. Available at: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

	Is the country part or observer?	Date of accession and ratification	¿Presentó Reservas?	Does the country have its own law on cybercrime and international cooperation? Since what year?	Important current discussions on cybercrime, international cooperation and data flow for purposes of conducting investigations.
Mexico	Convention Observer[174]	Not applicable	Not applicable	Yes, in 1999 Congress initiated a first wave of reforms to its Penal Code in charge of inserting the topic of cybercrime into the text of the law. In addition, the country currently has provisions on the subject in its Criminal Code, the National Security Law and a National Cybersecurity Strategy, announced by the President of Mexico in 2017.	There is an ongoing debate on a reform of the laws governing the National Public Security System within the framework of the constitutional reform initiative on cybersecurity[175]-[176]

174 Council of Europe. Chart of signatures and ratifications of Treaty 185. Available at: 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? September, 2020. Available at: https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/

176 In September 2019, the Public Security Commission of the Chamber of Deputies approved two resolutions to reform the General Laws of the National Public Security System on cybersecurity and National Security on intelligence.


DERECHOS
DIGITALES
América Latina