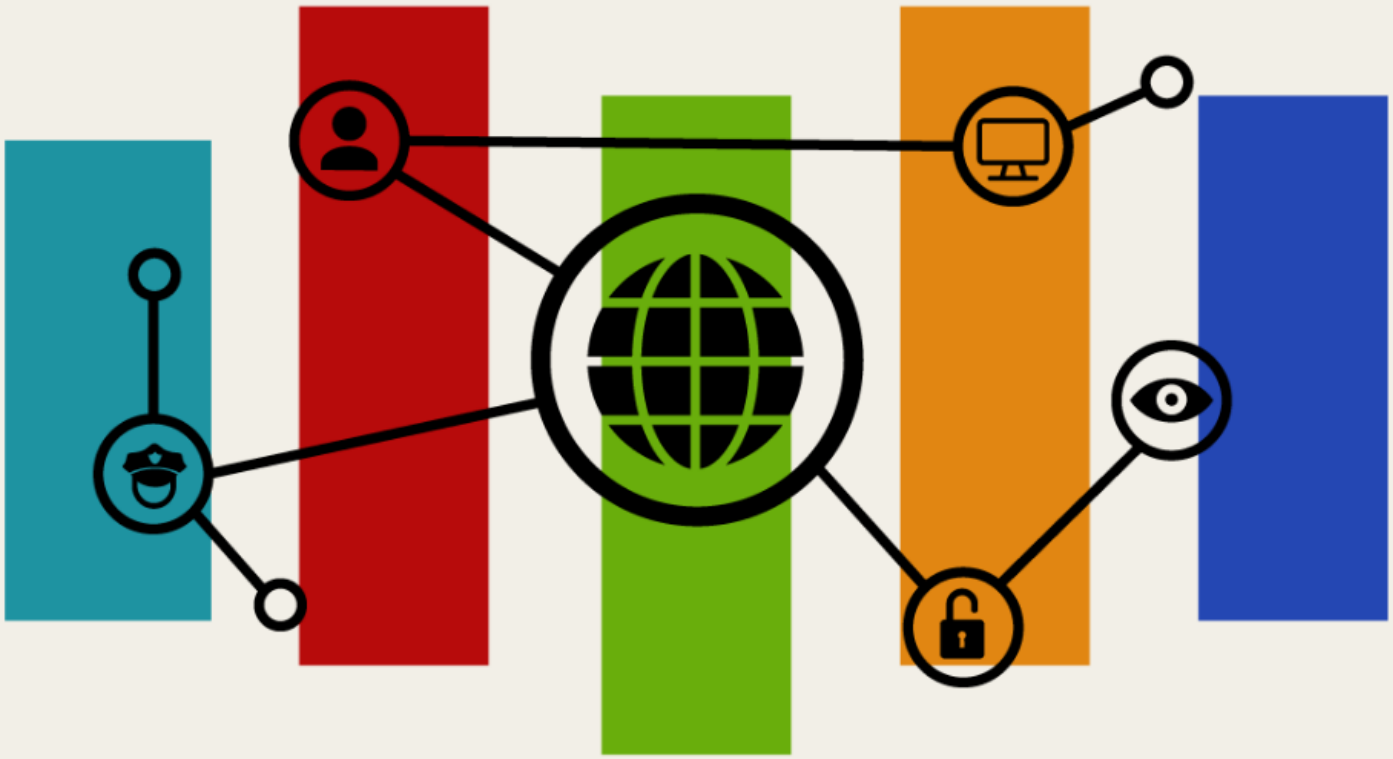


Assessing New Protocol to the Cybercrime Convention in Latin America

Concerns, Human Rights Considerations, and Mitigation Strategies

ELECTRONIC FRONTIER FOUNDATION

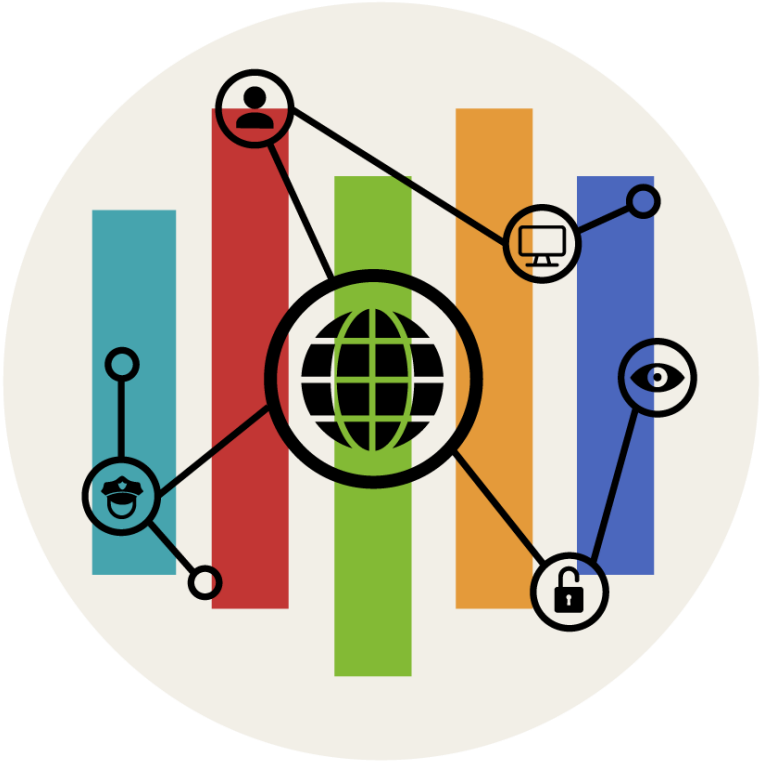
AlSur

Authors: Veridiana Alimonti
Collaborators: Al Sur

EFF's Policy Director for Global Privacy, Katitza Rodriguez, reviewed, and Senior Media Relations Specialist, Karen Gullo, edited this guide. EFF's Translations Manager, Carlos Wertheman, translated the guide into Spanish. EFF's Design Manager, Kim Carlson, along with EFF's Art Director, Hugh D' Andrade, formatted this guide. EFF web developer, Artemis Schatzkin worked on the Necessary & Proportionate website to host this guide.

A publication of the Electronic Frontier Foundation, 2022.

View this report online:
https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam.pdf



Assessing New Protocol to the Cybercrime Convention in Latin America

Concerns, Human Rights Considerations, and Mitigation Strategies

Veridiana Alimonti
Associate Director for Latin American Policy

May 2022

Introduction

The Second Additional Protocol to the Convention on Cybercrime (hereinafter "the Protocol") on enhanced cooperation and disclosure of electronic evidence seeks to establish new international standards that will govern aspects of policing and criminal investigations on a global scale.[1] The Protocol was adopted by the Council of Europe (CoE) in November 2021.[2] Now and in the months to come, various countries all over the world, especially those Parties of the existing CoE Cybercrime Convention, are engaged in or will likely conduct national discussions to assess their accession and potential implementation of the Protocol into their domestic legal framework. Latin American countries that have become part of the 2001 Cybercrime Budapest Convention are eligible to become a Party to the Protocol.[3]

Opened for signature on May 12th, 2022, the Protocol sets several procedures for enhanced international cooperation. Such measures include:

- Emergency mutual assistance.
- Expedited disclosure of stored computer data in an emergency.
- Cooperation among authorities for the disclosure of stored computer data.
- Procedures enhancing direct cooperation with service providers in another Party's territory.

The present guide seeks to assist interested stakeholders in national debates about a possible accession to the Protocol. It highlights the Protocol has considerable weaknesses from a human rights perspective that should lead countries to think carefully about whether to ratify it, and that deserve thorough consideration within national debates about the Protocol. This guide focuses on direct cooperation measures with service providers and the Protocol's human rights and data protection safeguards.

By becoming a Party to the Protocol, eligible Latin American countries will implement these new cross-border data access powers into their domestic framework. State Parties will then rely on such rules when seeking data abroad and will also abide by its conditions and obligations when receiving requests from foreign authorities that are Parties in the agreement.

This guide provides a critical overview of the Protocol, mainly focusing on Articles 7, 13, and 14, and highlights mitigation measures in case of its adoption. The guide is divided into three sections: (**I**) Background on the Protocol; (**II**) Main concerns, including possible negative impacts in Latin American privacy frameworks; (**III**) Assessing accession and mitigating weaknesses. The guide takes into account Latin America's

[1] The full text of the Second Additional Protocol to the Convention on Cybercrime is available at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224
[2] See more at https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe
[3] In this guide, *State Parties*, *Parties*, and *signatories* refer to States having acceded to an international treaty or agreement.

particular challenges in fulfilling human rights safeguards and the rule of law, and considers the legal frameworks on personal data protection and government access to communications data in multiple Latin American countries.[4]

[4] See previous research on government access to data in Latin American countries considered in this guide at https://necessaryandproportionate.org/country-reports/

I. Background on the Protocol

The new international agreement is the Second Protocol to the CoE's Convention on Cybercrime, also known as the Budapest Convention, which was opened for signature in 2001. The Budapest Convention is a comprehensive international agreement on cybercrime providing substantive criminal and procedural law obligations to harmonize criminal legislation and enhance cooperation in investigations that reach across borders. It was the first international treaty aimed at tackling cybercrime and constitutes the most widely ratified cybercrime treaty in effect today, with 66 State Parties and more than 20 observer States and organizations.[5] Although the Convention contains rules for transborder access to data and international cooperation, most of its provisions address legislation and cybercrime investigations at the domestic level. In turn, the Protocol focuses on enhancing international cooperation among authorities and with service providers in another territory. The Protocol includes several legal measures, ranging from emergency mutual assistance, expedited disclosure of stored computer data in an emergency, and cooperation among authorities for the disclosure of stored computer data. It also includes procedures enhancing direct cooperation with service providers in another Party's territory, including measures for competent authorities to access personal data held by a provider in another territory.

The 2001 Budapest Convention has been quite influential in Latin America,[6] acting as a guideline for countries developing comprehensive national legislation against cybercrime, and as a framework for international cooperation between State Parties to this treaty. The Protocol has similar potential and an extra appeal. As many competent authorities may want access to potential electronic evidence across borders, states will likely seek accession to the Protocol because of its novel cooperation rules. Only states in Latin America already a party to the 2001 Budapest Convention can accede to the Second Protocol.[7] To date, they comprise Argentina, Chile, Costa Rica, Colombia, Dominican Republic, Panama, Paraguay, and Peru. Brazil and Mexico were invited to become parties and have acted as observers, with Brazil's accession to the Budapest Convention being approved by Congress in December 2021.

Despite the CoE's background of strong commitment to stakeholder engagement, the Protocol's drafting process by the CoE Cybercrime Committee (T-CY) was strongly influenced by public safety and law enforcement officials.[8] Digital and human rights groups, defense attorneys, and even data protection regulators[9] were largely sidelined

[5] See at https://www.coe.int/en/web/cybercrime/parties-observers
[6] See Bruna Martins dos Santos. Derechos Digitales. *Budapest Convention on Cybercrime in Latin America*: a brief analysis of adherence and implementation in Argentina, Brazil, Chile, Colombia and Mexico, 2022.
[7] Article 16 of the Protocol, and Protocol's Explanatory Report, paragraph 294. Available at https://rm.coe.int/1680a49c9d
[8] Katitza Rodriguez, Tamir Israel. *Global Law Enforcement Convention Weakens Privacy & Human Rights*. June 8, 2021, https://www.eff.org/deeplinks/2021/06/global-law-enforcement-convention-weakens-privacy-human-rights
[9] The European Data Protection Board, in the body's submissions to the TC-Y consultations for the Protocol's draft text, has repeatedly emphasized the importance of involving data protection authorities in the Protocol's drafting process. See EDPB's contribution in November 2019 https://www.eff.org/deeplinks/2021/07/council-europes-actions-belie-its-pledges-involve-civil-society-de

during the drafting process, which was pointed out by civil society organizations.[10] The resulting text is an expression of this uneven process, with mandatory human rights safeguards that are not as robust as the obligations facilitating transborder police access to personal data. Countries assessing whether to accede to the Protocol must consider its shortcomings vis-à-vis their national context and applicable legal framework so as to properly identify gaps in human rights protections and address concerns. The next section highlights main concerns that should be taken into account.

In a nutshell, we group these concerns into four categories: (i) undermining rights and safeguards through direct cooperation orders for service providers in State Parties' territories; (ii) the Protocol's flawed understanding of subscriber information and its negative influence in Latin American legal privacy frameworks; (iii) imbalance between mandatory law enforcement powers and dispensable or optional human rights safeguards; (iv) weaker data protection safeguards compared to other settled international standards.

velopment-cross and EDPB's statement in February 2021 https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_en

[10] See, for example, Joint Letter by Civil Society Organizations to the Chair of the Committee of Ministers of the Council of Europe. May 31, 2021. https://www.eff.org/files/2021/06/07/final_letter_-_council_of_europe-final.pdf. See also Karen Gullo, Katitza Rodriguez. *Council of Europe's Actions Belie its Pledges to Involve Civil Society in Development of Cross Border Police Powers Treaty*. July 22, 2021. https://www.eff.org/deeplinks/2021/07/council-europes-actions-belie-its-pledges-involve-civil-society-development-cross

II. Main Concerns

Mutual Legal Assistance Treaties (MLATs) have traditionally provided the primary framework for government cooperation on cross-border criminal investigations. MLATs are typically bilateral agreements, negotiated between two countries with embedded safeguards. Several States claimed that the MLAT process is slow, leading to delays in criminal investigations.[11] The Protocol's most invasive rules seek to respond to these claims by creating new mechanisms that will let competent authorities access data more quickly and easily.

However, efforts to attain greater efficiency in accessing personal data in criminal investigations across borders must always be grounded on robust human rights protections. The lawfulness and legitimacy of investigations depend on respect for criminal procedural safeguards, data protection regulations, and international human rights law. If cross-border investigations are challenging, securing human rights in such investigations is equally difficult. How to ensure that any interference with the right to privacy is based on publicly-accessible, precise, and non-discriminatory law, and is legitimate, necessary and proportionate? How to make sure that gaining access to and sharing of data is authorized by a competent judicial authority that's impartial and independent? How to secure that due process rights prevail, oversight mechanisms are applied, and immunity and privileges are respected?

Any new regime to expedite cross border access should preserve crucial safeguards needed to uphold human rights. MLATs, for example, typically involve :

- A mechanism for requesting assistance to access data stored in a hosting country;
- A Central Authority that assesses and responds to assistance requests from foreign states or refuses requests that are contrary to human rights;
- A legal basis in national law authorizing the Central Authority to obtain data on behalf of the requesting State;
- The obligation for Central Authorities to rely on national search powers (and be bound by accompanying national privacy protections) when obtaining data in response to a request.
- An assessment by States of the compatibility of the MLAT agreement and the other Party's legal system with their respective domestic legal framework to ensure core values and human rights standards will be respected.

Unfortunately, Article 7 of the Protocol falls short of providing effective human rights safeguards, although Article 8 does keep some of the safeguards embedded in the MLATs system.

While our analysis below focuses predominantly on Article 7 of the Protocol, we note that Article 6 implicates similar privacy and human rights interests and concerns.

[11] See at https://www.eff.org/deeplinks/2015/12/reforms-abound-cross-border-data-requests

Both articles provide for the direct transfer of personal data from service providers located in the territory of one State Party of the Protocol to competent authorities (e.g., police, prosecutors) in another State Party.

(a) The Inherent Flaws in Article 7

Article 7, paragraph 1 of the Protocol obliges signatory states to adopt legislative measures to empower its competent authorities[12] to directly request the disclosure of subscriber information in the possession or control of a service provider located in another Party's territory— driving out key human rights vetting mechanisms.

Under Article 7's default mechanism, authorities in the State Party where the provider is located will not play any "vetting" role and, therefore, won't be able to reject a specific request for assistance if it conflicts with its State's human rights framework. Under this mechanism, law enforcement authorities in one State that are empowered by domestic law to order service providers to disclose subscriber information will be able to submit a direct request for providers located in another State Party, following only the legal standard of the requesting State. This means that orders may be issued without any oversight by a judicial or other independent authority if those are not requirements in the requesting Party's domestic framework.

Article 7, paragraph 2, also compels Parties to adopt legislative measures to authorize service providers to respond to disclose subscriber data requests in response to an order under Article 7, paragraph 1. This means that if a domestic law in the territory where the service provider is located prevents them from voluntarily responding to subscriber data requests without appropriate safeguards—such as a reasonable ground requirement and/or a court order—States are now compelled to remove those legal safeguards for cross-border direct requests.

Requests to service providers under Article 7, paragraph 1, are devised as "orders" that are binding at a national level, although not directly enforceable by foreign requesting authorities given their cross-border application. In principle, service providers still have room to reject foreign direct requests, but the fact they are enforceable through procedures to compel disclosure ("give effect to an order") in Article 8,[13] or another form of mutual assistance, will likely deter providers from refusing such requests. Indeed, under Article 7, service providers are not even given enough information to properly

[12] Article 3, paragraph 2(b) of the Protocol defines "competent authority" as a judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorize or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

[13] Article 8, paragraph 1, requires State Parties to adopt legislative and other measures as may be necessary to empower its competent authorities to issue an order to the State Party where the provider is located so it can compel local service providers to produce stored subscriber and "traffic" data in the possession and control of the provider. Article 8, paragraph 2, requires the requested Party, where the provider is located, to adopt legislative measures and other measures as may be necessary to give effect to the requesting Party's order. As such, if a service provider doesn't comply with a direct cooperation order under Article 7, the requesting Party may seek enforcement pursuant to Article 8's mechanism. Parties may not seek unilateral enforcement. See Protocol's Explanatory Report, paragraph 117.

assess or process a request to identify circumstances that are inconsistent with human rights and fundamental freedoms.

By these means, the Protocol can create unjustifiable asymmetries in national law. For example, under the Protocol's overbroad definition of "competent authority,"[14] any administrative or other law enforcement authority empowered by their domestic law to issue a request for subscriber data is entitled to do so directly to a service provider located in another Party's territory. As a consequence, cross-border direct orders may be issued without any oversight by a judicial or other independent authority in the requesting Party, allowing foreign authorities to apply a more permissive, less privacy-protective legal basis to access subscriber data than what local law enforcement officials would be required to do under the requested Party's local law.

Mexico: In 2016, the Second Chamber of the Mexican Supreme Court held that a judicial order was required to disclose retained data that allow the identification of a communication, including subscriber information, and stated that authorities must specify targets and time periods as well as justify the need for the information sought.[15]

Chile: Chilean internet service providers (ISPs) require prior judicial authorization as a best voluntary practice when processing national subscriber data requests.[16] The country's Criminal Procedure Code allows a more protective standard by requiring a prior judicial order in all proceedings that affect, deprive, or restrict an accused or a third-party's constitutional privacy rights.

Brazil: Brazilian Law n. 12.965/2014 requires a judicial order before users' communications data, such as IP addresses, can be disclosed to law enforcement officials. Yet, local administrative authorities can issue direct requests for subscriber data like name and address, when specifically authorized by law.

In consultations during the drafting process, EFF, together with civil society organizations from Europe and the Americas, including groups from Al Sur, urged the CoE to remove Article 7 from the Protocol's draft text, allowing Article 8 to become the primary legal basis by which subscriber data is accessed in cross-border contexts.[17] The European Internet Services Providers' Association (EuroISPA) made similar

[14] See supra note 12.
[15] See at https://www.internet2.scjn.gob.mx/red2/comunicados/comunicado.asp?id=4301
[16] See at https://www.derechosdigitales.org/wp-content/uploads/QDTD-2021.pdf. See also law enforcement guidelines from Chilean telecommunications companies GTD (https://www.gtd.cl/normativa/privacidad-y-proteccion-de-datos-personales/requerimientos-de-informacion) and Claro (https://www.clarochile.cl/portal/cl/archivos_generales/politica-requerimientos-de-informacion-Marzo-de-2021_20210331.pdf).
[17] EFF, Derechos Digitales, EDRi, Fundación Karisma, CIPPIC, TEDIC. *Privacy & Human Rights in Cross-Border Law Enforcement*. Joint Civil Society Comment to the Parliamentary Assembly of the Council of Europe (PACE) on the Second Additional Protocol to the Cybercrime Convention (CETS 185). August 9, 2021, p. 5. Available at https://www.eff.org/files/2021/08/17/20210816-2ndaddprotocol-pace-ver2-final.pdf

recommendations in their submissions.[18] Article 8 requires the involvement of the requested Party's national authorities. By these means, authorities in the requested Party can apply standards contained in its own national laws when compelling the production of subscriber data to local service providers located in its territory. While Article 8 does not require judicial supervision of police requests, states with strong privacy protections may continue relying on their own courts when compelling a local service provider to identify customers. It's worth noting that Article 8 already provides for an expedited mutual assistance request, while Articles 9 and 10 address international cooperation in emergency situations, without overriding the role of national authorities in the Party where the provider is located.

Paragraph 9(a) of Article 7 allows Parties to reserve the right not to apply Article 7 in its entirety, but only at the time of signature or when depositing its instrument of ratification, acceptance, or approval. A Party that reserves Article 7 is not permitted to issue direct cooperation orders under Article 7, paragraph 1, to service providers in other Parties' territories.[19]

Alternatively, Article 7 stipulates **optional safeguards**, not required by the text but which can be invoked through a State Party's reservations and declarations. They are established in Article 7, paragraph 2(b); Article 7, paragraph 5 (a) and (b); and Article 7, paragraph 9(b). The reservations are only allowed at the time a State is acceding to the Protocol. In some cases, this restriction also applies to declarations. So, to properly present those optional safeguards and their importance, we should consider what subscriber information is and why we should care about the circumstances under which it can be accessed by law enforcement.

What Is Subscriber Information?

The Budapest Convention has always promoted a distinction between "traffic data" (equivalent to "metadata") and "subscriber information," and defines them separately. "Subscriber information" is defined quite broadly in Article 18, paragraph 3, of the Budapest Convention.[20] As noted in the Convention's explanatory report, subscriber information is needed primarily in two specific situations in the course of a criminal investigation: (i) to identify which services and related technical measures the subscriber has used or is using, and (ii) to establish the identity of the person concerned when a technical address is known (eg. an IP address).[21] The Protocol's explanatory report uses the Budapest Convention's definition of subscriber data to consider that it

[18] See, for example, EuroISPA's submissions to the 4th round (https://rm.coe.int/euroispa-s-comments-to-draft-provisions-2nd-add-protocol-final/168098bcab) and 6th round of consultation (https://rm.coe.int/0900001680a25789).
[19] See the Explanatory Report of the Protocol, paragraph 122.
[20] The provision stipulates that: "[...] the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: (a) the type of communication service used, the technical provisions taken thereto and the period of service; (b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement."
[21] See the Explanatory Report of the Budapest Convention, paragraph 178.

includes types of IP address information.[22] The Protocol also establishes a lower level of protection for cross-border access to subscriber information in relation to international cooperation safeguards applied to traffic data or communications content.

Why Does Subscriber Information Matter?

Your IP address can reveal to authorities what websites you visit and who you communicate with. It could disclose otherwise anonymous online identities, your social networking contacts and, even at times, your physical location via GPS. Police can request your name, the subscriber data linking your identity to your online activity, and that can be used to create a nicely detailed police profile of your daily habits, and may also provide relevant hints regarding the content of your communications. Even disclosing an identity associated with a specific phone number may be sensitive, when it could, for instance, reveal the source of a journalist. The consequences of feeble protections when unveiling otherwise anonymous identities can be dire. The lack of proper safeguards, as is the case with Article 7 of the Protocol, poses a threat to the safety of activists, human rights defenders, dissidents, journalists, and everyday people likely to face persecution and reprisals for countering and criticizing entrenched powers.

Chile: In 2013, the Prosecutor's Office formalized an investigation against Rodrigo Ferrari on charges of identity theft as the alleged author of three Twitter accounts parodying the businessman Andrónico Luksic, owner of a major business conglomerate in Chile. Prosecutors obtained the IP address, username, and email from the Twitter account @losluksic. Then, the telecom company VTR disclosed his name, national ID, telephone number, and email without requiring any judicial authorization. The prosecution could not prove Ferrari's connection with the two other Twitter accounts, and the account @losluksic (the only one recognized by Ferrari) was not enough to proceed with an accusation of identity theft. Although the case was finally dropped, Ferrari risked between 61 and 540 days in jail and faced pressure from the prosecution to plead guilty and accept a deal.[23]

More recently, Chile's prosecutor's office sought to obtain all mobile phone numbers that had connected to antennas in Santiago's subway stations, where fires marked the beginning of the country's 2019 social uprising and protests. By obtaining the mobile phone numbers, it would be possible to identify their owners located in the protests' zone. Only one telecom company complied with the prosecutor's voluntary direct request, while others required a judicial order. The broad and disproportionate nature of the request should also receive greater scrutiny.[24]

[22] Protocol's Explanatory Report, paragraph 93.
[23] See interview with Rodrigo Ferrari at https://www.theclinic.cl/2016/09/22/554806/
[24] See at https://www.biobiochile.cl/noticias/ciencia-y-tecnologia/moviles-y-computacion/2020/01/08/afirman-que-wom-entrego-informacion-de-usuarios-durante-estallido-social-compania-se-defendio.shtml

Paraguay: In 2016, one of the main Paraguayan media outlets, *ABC Color*, revealed that military forces' intelligence officials unlawfully accessed data from a telecommunications company to identify one of its journalists reporting about a corruption case within the military, as well as her possible sources.[25]

Brazil: In late 2020, law students who created the Twitter accounts *Sleeping Giants Brasil* and *Sleeping Giants Rio Grande do Sul* decided to publicly reveal their identities after a judge compelled Twitter to disclose IP addresses and other data capable of identifying the accounts' owners. Before revealing their identities to the press, the students took measures to preserve their safety. Both Twitter accounts notify brands about the presence of their ads on websites that spread disinformation and hate speech. The civil suit was filed by *Jornal da Cidade*, a newspaper targeted by *Sleeping Giants* accounts. The media outlet is considered to have spread disinformation in favor of President Bolsonaro's electoral campaign, was included in a congressional investigation on the dissemination of fake news, and had its pieces fact-checked and deemed false on different occasions.[26]

There is a growing international understanding among courts and human rights bodies that accessing some IP addresses and other online identifiers (a type of subscriber data in certain jurisdictions) for the purpose of identifying anonymous online activity[27] can reveal a good deal about individuals' lives—including sensitive details of his or her interests, beliefs, relations, and intimate lifestyle—and thus such access should be subject to solid protections.

As one recent example, the European Court of Human Rights, in the case *Benedik v. Slovenia*, held that there had been a violation of the right to respect for private and family life when Slovenian police failed to obtain a court order before accessing subscriber information associated with a dynamic IP address. According to the Court, the legal provision used by the Slovenian police to access subscriber data associated with the IP address, without first obtaining a court order, had not met the European Convention on Human Rights standard of being "in accordance with the law."[28]

---

[25] See media coverage on the case at https://www.abc.com.py/edicion-impresa/notas/gobierno-uso-su-sistema-de-inteligencia-para-espiar-periodista-1511976.html and at https://www.abc.com.py/edicion-impresa/politica/fiscalia-ya-sabe-que-hubo-espionaje-a-equipo-telefonico-de-periodista-de-abc-1513518.html

[26] See news reports about the case at https://brasil.elpais.com/brasil/2020-08-25/acoes-judiciais-tentam-revelar-identidade-de-administrador-do-sleeping-giants.html, https://www1.folha.uol.com.br/colunas/monicabergamo/2020/12/sleeping-giants-sai-do-anonimato-em-entrevista-a-folha.shtml, and at https://olhardigital.com.br/2020/12/17/noticias/criadores-da-conta-sleeping-giants-brasil-revelam-suas-identidades/

[27] We use "anonymous" here to mean a non directly identified online activity regarding the person or persons involved—although it may involve an identifier, such as an IP address or IMEI number, or be identifiable through other means available or reasonably likely to be used to identify a natural person.

[28] See the ECtHR ruling at https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}.

Other jurisdictions have also recognized the importance of anonymity as a component of the right to privacy. The Supreme Court of Canada, in particular, said in a ruling that the anonymity of individuals online should be protected when it struck down warrantless acquisition of a user identity by the police as unconstitutional, stating:

> "[P]articularly important in the context of Internet usage is the understanding of privacy as anonymity. The identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address and telephone number found in the subscriber information. Subscriber information, by tending to link particular kinds of information to identifiable individuals may implicate privacy interests relating to an individuals' identity as the source, possessor or user of that information. Some degree of anonymity is a feature of much Internet activity and depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure. In this case, the police request to link a given IP address to subscriber information was in effect a request to link a specific person to specific online activities. This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized in other circumstances as engaging significant privacy interests. . . The disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search."[29]

Unfortunately, the Protocol is in contradiction with these trends. It allows cross-border direct requests of subscriber information to service providers without establishing a requirement for prior independent or judicial authorization. Instead, it deems subscriber information, per se, as a less privacy-intrusive category of data.

States can still modify their existing criminal procedural code or similar law, and require prior judicial authorization to access subscriber data. While it will not solve the problem when a foreign State Party requests data to the local service providers under the Protocol's powers, it can help increase the standard of privacy protection. Compelled disclosure of anonymous speakers should only occur once a legally defined offense has been committed. And even in those cases, all the rights of an online speaker should be considered before identifying that individual in response to a request to do so. Judicial authorities, not private companies, are best suited to balance citizens' right to anonymous expression with the need to provide a mechanism to redress wrongs. But judicial systems can only function when a judge or a court has an opportunity to review the circumstances before the identity is revealed. Therefore, to protect a person's freedom of expression and privacy, service providers should only disclose the identity of

[29] R. v. Spencer, 2014 SCC 43, June 13, 2014. Further, the court stated that the "subject matter of the search was not simply a name and address of someone in a contractual relationship with the ISP. Rather, it was the identity of an Internet subscriber which correspond to particular Internet usage." The decision is available at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do?r=AAAAAQAHc3BlbmNlcgE

an anonymous or pseudonymous user of their platform or service upon receipt of a judicial order, granted after a process of prior judicial review.[30]

Article 7's Worrisome Standard Procedure and Optional Safeguards to Consider

The Protocol uses the Budapest Convention's distinction between "traffic data" and "subscriber information" to incorporate a lower level of protection for subscriber data in the context of cross-border requests by allowing the requesting Party to access data under its own domestic legal standards. It makes the troubling assumption that "subscriber information … does not allow precise conclusions concerning the private lives and daily habits of individuals concerned," as noted in the Protocol's explanatory report.[31] The Protocol deems subscriber data as a category of information by nature less intrusive than other types of data. With this, the agreement disregards that unveiling peoples' identities associated with their expressive activities can be highly sensitive. It also overlooks that subscriber information can reveal traffic data and even allow inferences on the content of communications. As the *13 Principles on the Application of Human Rights to Communications Surveillance* states, these formalistic categories of data "content," "subscriber information," or "metadata" are no longer appropriate for measuring how intrusive communications surveillance is for individuals' private lives and associations.[32]

As per Article 7's standard procedure, *any competent* authority in the requesting Party[33] in accordance with this Party's domestic law can issue an order demanding access to subscriber information in the possession or control of a service provider located in another Party's territory. One possible avenue to mitigate asymmetries when standards in the requesting Party differ from those enforced in the requested State is provided for in **Article 7, paragraph 2(b). Under this paragraph, a Party may declare that orders issued to service providers in its territory "must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision.**" However, Parties cannot require prior independent judicial approval of direct foreign requests. As indicated in the explanatory report, a Party making use of this declaration must accept an order by or under the supervision of any of these enumerated authorities, which includes prosecutors.

While States must ensure prosecutors are able to perform their functions without intimidation or improper interference, and while some legal frameworks may grant to prosecutors a supervisory role on the legality of investigations,[34] such supervision does

[30] Rodriguez, Katitza, Anonymity and Encryption Comments submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, February 2015, https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf
[31] Protocol's Explanatory Report, paragraph 92.
[32] See at https://necessaryandproportionate.org/principles/
[33] See supra note 12 for the Protocol's definition of "competent authorities."
[34] UN Guidelines on the Role of Prosecutors. Adopted on September 7, 1990, by the Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders, paragraph 4 and 11. https://www.ohchr.org/en/instruments-mechanisms/instruments/guidelines-role-prosecutors . See also Necessary and Proportionate Coalition on Inter-american standards regarding judicial control for surveillance measures, https://necessaryandproportionate.org/americas-legal-analysis/#vi-competent-judicial-authority

not meet the independence and impartiality standards found in judicial control. Indeed, as underscored by the Inter-American Commission on Human Rights (IACHR), "judges are the lead actors in ensuring judicial protection of human rights in a democratic State." According to the IACHR, judges are the ones that ensure "the acts of other branches of government and public servants in general are consistent with the conventions to which the State is party and with its constitution and laws."[35] Likewise, the European Court of Human Rights has stated "the rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[36] More recently, the EU Court of Justice held that the public prosecutor's office, "whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings," cannot be regarded as an independent administrative authority in order to authorize government access to communications data in criminal investigations.[37] This was already indicated in the *13 Principles on the Application of Human Rights to Communications Surveillance*, which reflect the view that prior judicial authorization for government access to data is not merely desirable but essential.[38]

Moreover, the Protocol's explanatory report considers that types of IP address information are included in the Budapest Convention's definition of subscriber data (Article 18, paragraph 3).[39] Aware that some states already grant a higher level of protection for the disclosure of IP addresses or other types of numbers, **the Protocol allows Parties to reserve the right not to apply this article to certain types of access numbers (Article 7, paragraph 9(b))**. But this is only allowed if disclosure of these access numbers "would be inconsistent with the fundamental principles of its domestic legal system." Again, a Party that makes this reservation is not permitted to issue direct cooperation orders for such numbers to service providers in other Parties' territories.

Paragraph 9(b), however, fails to address some of the most problematic privacy threats posed by Article 7, as law enforcement will continue to be able to demand the name and address of internet subscribers associated with access numbers. Article 7 also does not allow Parties to opt out of its requirements based on other relevant circumstances, like the existence of applicable immunities and privileges ensured in domestic law (i.e. attorney-client privilege) or core principles of international mutual assistance. As

[35] Inter-American Commission on Human Rights. *Guarantees for the independence of justice operators.* Towards Strengthening Access to Justice and the Rule of Law in the Americas. OEA/Ser.L./V/II. 5 December 2013, paragraph 16. https://www.oas.org/es/cidh/defensores/docs/pdf/justice-operators-2013.pdf
[36] See in particular, *Klass and Others v. Germany*, paragraph 55. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57510%22]}. Although the Court in *Klass* agreed that "it is in principle desirable to entrust supervisory control to a judge," it did not go so far as to hold that prior judicial authorisation was required in every case so long as the relevant authorizing body was "sufficiently independent" of "the authorities carrying out the surveillance" to "give an objective ruling" and was also vested "with sufficient powers and competence to exercise an effective and continuous control." In subsequent cases, however, the Court has made clear the desirability of judicial authorization for the use of lawful surveillance. See, *Kopp v. Switzerland*, paragraph 74.
[37] CJUE, Prokuratuur, C-746/18, paragraphs 26 and 59 https://curia.europa.eu/juris/liste.jsf?num=C-746/18
[38] Necessary and Proportionate Coalition, *13 Principles on the application of human rights to communications surveillance.* https://necessaryandproportionate.org/global-legal-analysis/#principle-by-principle-explanation
[39] Protocol's Explanatory Report, paragraph 93.

explained below, Article 7 deters systematic application of these principles by rendering its consultation and notification mechanisms optional. This poses a threat to human rights since rights-protective tenets enshrined in national law or regular mutual assistance requests' safeguards will likely fail to receive appropriate consideration under Article 7's standard procedure.

Peru, Paraguay, Argentina, Chile, Brazil, among many other countries in the region, have constitutional or legal protections regarding professional secrecy like attorney-client or doctor-patient confidentiality and the protection of journalistic sources.[40]

Argentina: The Law 24.767/1997 sets the legal basis for international cooperation in criminal matters in Argentina and describes the procedure for granting assistance where there is no treaty in place with the requesting State. The law stipulates grounds for refusing an international assistance request, such as: when the request relates to a political or military criminal law offense; when the assistance is sought for a prosecution brought to persecute individuals or groups on account of political opinions, nationality, race or religion or when there are grounds to suppose that an individual's right of defense may be undermined for any of those reasons, and when the offense in question is punishable by death in the State requesting the assistance and no assurance is given that this penalty will not be imposed.[41]

Under Article 7's standard procedure, it is up to the service provider to assess whether foreign State Party authorities issuing data requests are legitimate, whether the order is legal and proportionate or otherwise endangers data subjects' human rights, or if any grounds for refusal would apply. Without checking laws enforced where they are located and having a reasonable understanding about the foreign context in which the direct order was issued, service providers risk disclosing data in a way that is not authorized under national law. The authority issuing the data request is not required to provide a summary of the facts related to the investigation or proceeding, which could shed light on circumstances inconsistent with human rights. Authorities in the Party where the service provider is located that are entitled to receive and request additional factual information are, by default, cut off from direct cooperation requests under Article 7.

[40] In their comments to the Protocol's draft text, the Council of Bars and Law Societies of Europe stressed that "professional secrecy/legal professional privilege can cover not only content data, but also other types of data (e.g. traffic data and, in certain circumstances, subscriber information). Furthermore, it is necessary to be sensitive to the circumstances where recovery of subscriber data are sought, that is often the precursor to other investigative activities. Where the data relate to lawyers, recovery of it will bring a substantial risk of subsequent violation of the legal professional privilege attaching to their communications with their clients, and even where the subscriber data relate to non-lawyers, there may be a risk that subsequent investigation will lead to an infringement of privileged communications."
https://rm.coe.int/ccbe-written-comments-draft-2nd-additional-protocol-to-the-convention-/168098bc6e

[41] See Article 67 combined with Article 8 of the Law 24.767/1997.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41442/norma.htm

While Big Tech companies can be better equipped to handle direct foreign orders, they will also face challenges in identifying and refusing cross-border subscriber data requests that are contrary to human rights. Meanwhile, local telecom companies or smaller service providers have significantly less capacity and expertise to handle such orders, which will be even more detrimental for human rights.

Cross-border direct cooperation requests can pose many practical challenges to service providers. In addition to lacking the expertise and/or information needed to check on the legality, proportionality, and local context of such requests, these challenges involve the absence of settled or known contact channels with foreign requesting authorities. Verifying the authenticity of an order and ensuring secure mechanisms for data transmission aren't simple[42] and even major companies can make serious mistakes.[43] Article 7, paragraph 6, establishes only that "appropriate levels of security and authentication may be required" in case data is provided in electronic form. The explanatory report indicates that the use of an official email address could be enough to assert the authenticity of a request, which is still easy to manipulate.[44] Obtaining confirmation of authenticity via a known authority in the requesting Party, another method suggested, may be better but more complex for smaller providers not used to handling foreign authorities' requests.

All this reinforces the importance of having an authority from the Party where the service provider is located involved in processing of such requests. As optional safeguards, **Article 7 of the Protocol allows a Party to require that its authorities receive simultaneous *notification* of an order when a direct cooperation request is issued and/or mandate service providers *consult* the Party's authorities prior to disclosure ((Article 7, paragraph 5 (a) and (b))**. Between the two possibilities, the simultaneous notification is the most appropriate for the protection of human rights. According to Article 7, paragraph 5(c), the authorities notified or consulted may instruct the service provider not to disclose the subscriber information if: (i) disclosure may prejudice criminal investigations or proceedings in that Party; or (ii) conditions or grounds for refusal would apply had the subscriber information been sought through mutual assistance under the Budapest Convention. Authorities notified or consulted may also obtain additional information that would not be shared with the service provider (Article 7, paragraph 5(c)(i)). In any case, the Protocol's explanatory report notes that impediments to cooperation and refusals of requests should be "strictly limited."[45]

Article 7, paragraph 5(e), further stipulates that Parties must designate a single authority to receive notification and/or consultation and perform related actions. This is a key opportunity for State Parties to assign an independent judicial authority to fulfill these roles and review the cross-border direct requests. Within the context of the European Union, the European Data Protection Supervisor (EDPS) recommended

[42] EuroISPA addressed these and other practical challenges in their comments to the draft text of the Protocol. See, for example, EuroISPA's submissions to the 4th and 6th rounds of consultation (supra note 18).
[43] According to media reports, Apple and Meta provided user details, such as a customer's address, phone number, and IP address in response to forged "emergency data requests" made by hackers. See at: https://www.bloomberg.com/news/articles/2022-03-30/apple-meta-gave-user-data-to-hackers-who-forged-legal-requests
[44] Protocol's Explanatory Report, paragraph 116.
[45] Protocol's Explanatory Report, paragraphs 108-110.

instructing Member States to designate a judicial or other independent authority to receive the notification. The EDPS also emphasized the relevance of a systematic involvement of judicial authorities in the requested Parties to preserve the principle of dual criminality.[46]

In summary, under Article's 7 default procedure, *any* competent authority[47] in the requesting Party, subject to its own domestic laws, can issue a direct order to a service provider located in another Party's territory to access subscriber data, based on a broad definition of subscriber information. No national authority is involved in the analysis and processing of this order in the requested Party, much less a judicial or other independent authority. With this, in certain instances, service providers may have to disclose subscriber information to foreign states under a lower standard than they are subject to when responding to domestic authorities' requests.

While it is true that investigations or proceedings for crimes that are entirely domestic in nature[48] may sometimes require law enforcement authorities to seek data abroad, Article 7's application doesn't restrict direct cross-border orders to such domestic cases, where it could seem that the requested Party doesn't have interests involved. Article 7 also applies for cases involving persons located or living in the requested Party. And, even in entirely domestic cases pertaining to the requesting State, the requested Party may consider it critical to deny requests for assistance in support of investigations or prosecutions that are motivated by political or discriminatory reasons, infringe on freedom of expression or the country's constitution, are connected to a political offense, or involve an offense punishable by death. These are safeguards that can be found in certain mutual legal assistance agreements and related norms.[49]

What's more, the asymmetries and assumptions fostered within Article's 7 rationale can serve as a systematic influence to drive down protective standards achieved by State Parties at the domestic level, as we discuss in the next section.

[46] The European Commission adopted two Proposals for the European Council decision on whether to authorize Member States to sign and to ratify the Protocol in the interest of the EU. In its Opinion 1/2022, the EDPS welcomes the proposals of the Commission for the Member States to make the declaration under Article 7(5)(a) of the Protocol, to require simultaneous notification of direct cooperation orders, and further recommends the designated authority to be a judicial or other independent authority. See paragraphs 90-92 at https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-two-proposals-council-decisions_en

[47] See supra note 12 for the Protocol's definition of "competent authorities."

[48] Situations where the crime, the victim and the perpetrator are all in the same country as the investigating authority.

[49] See example of Argentina's Law 24.767/1997 above. For other examples, see: European Convention on Mutual Assistance in Criminal Matters, Article 2, https://rm.coe.int/16800656ce. Brazil MLAT with Italy, Article 3, http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0862.htm. Brazil MLAT with Peru, Article 3, http://www.planalto.gov.br/ccivil_03/decreto/2001/D3988.htm. US MLAT with Kazakhstan (analysis of Article 3), https://www.congress.gov/114/cdoc/tdoc11/CDOC-114tdoc11.pdf. US MLAT with Bermuda states that a "request may also be denied if it relates to a political or a military offense, if it does not conform to the requirements of the Treaty, or if its execution would impair the sovereignty, security, or other essential interests of the requested Party, or would be contrary to important public policy. With respect to this last ground, the government of Bermuda indicated that it intends to interpret the provision to give Bermuda the right to deny assistance in cases involving capital punishment." https://www.congress.gov/111/cdoc/tdoc6/CDOC-111tdoc6.pdf.

All in all, the concerns described in this guide relate not only to human rights threats in the context of cross-border access to data, but will likely affect national privacy frameworks relating to criminal investigations in Latin American countries.

How Can Article 7 Negatively Impact Latin American Privacy Frameworks?

Article 7 can impact Latam legal communications privacy frameworks negatively in a few ways:

- It can play an influential role in establishing a lower level of protection for accessing subscriber data and unveiling a user's identity. The Protocol builds on the Budapest Convention's distinction between subscriber data and other communications data to set a lower level of protection for cross-border access to subscriber information based on the flawed assumption, reflected in the Protocol's explanatory report, that this type of data "does not allow precise conclusions concerning the private lives and daily habits of individuals concerned." Both the distinction and assumption overlook that subscriber data is highly sought after for criminal investigations because, when combined with content or traffic data that is already in the State's possession or can be easily obtained, linked or referenced, it can be used to identify specific people involved in expressive activities, their location, and other sensitive information;
- Over time, TC-Y has issued guidelines seeking to broadly interpret the Budapest Convention's definition of subscriber data to include IP addresses—which can also play an influential role in the region;
- Article 7 also hinders companies' best practice commitments to interpret local laws in a way that provides robust privacy protections for users (e.g., require a judicial order to hand subscriber information to law enforcement authorities), which we see in countries like Chile (see Box 1) ;
- Finally, it fails to set mandatory privacy safeguards for State Parties. Article 7 establishes clear cross-border evidence-gathering powers at the highest level to access subscriber data, but fails to establish a minimum mandatory baseline protection for when authorities can access subscriber data. Under Article 7's standard procedure, safeguards applied to direct cross-border requests to service providers rely on the domestic framework of the Party requesting the data, and not on those ensured in the territory where the requested service provider is located.

A recent analysis of trends in international cooperation for accessing digital evidence by the UN Security Council's Counter-Terrorism Committee Executive Directorate (CTED) notes:

> "[...] if States agree to lower standards for cross-border investigations than they apply at home, there may be pressure to lower the standard at home (since it

> would be odd if it were easier for foreign investigators than for domestic investigators to gain access to digital evidence in a given State)."[50]

Article 7 aligns with Latin America's weaker communication privacy standards.[51] In national disputes concerning privacy safeguards for accessing subscriber data, the CoE's influential standards and underlying conceptions can be used to tip the scale against strong protections. For example, legislative reforms both in Chile[52] and Brazil[53] have proposed allowing police access to subscriber data with no prior judicial authorization, seeking to overturn more protective interpretations of current applicable law.

While national courts around the world, including in Latin America,[54] increasingly recognize that subscriber data can reveal critical information about a persons' life, the Protocol not only furthers the opposite view but largely freezes in place a weaker standard for cross-border disclosure of subscriber information, since reservations to Article 7 are only allowed at the time the State accedes to the Protocol.

If national legal systems, because of new laws or court decisions, eventually recognize additional safeguards for subscriber information after ratifying the Protocol, such as the need for prior judicial authorization, the State will not be allowed to invoke the reservations of Article 7, paragraph 9, to block direct cooperation requests or stop them from being used to disclose certain types of access numbers (ej. log-on IP addresses). Moreover, State Parties are only able to exclude the disclosure of certain kinds of access numbers under Article 7 when doing otherwise "would be inconsistent with the fundamental principles of [the] domestic legal system." While Brazilian law, for example, expressly requires a judicial order before the disclosure of IP addresses, in many Latin American legal systems, judicial control and/or the need for reasonable grounds for accessing communications data are not clearly spelled out in the law. Such safeguards often rely on legislation that does not explicitly distinguish types of

---

[50] United Nations Security Council Counter-Terrorism Committee Executive Directorate. *The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspectives*, 2022, p. 26. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf

[51] See Katitza Rogriguez, Veridiana Alimonti. *When Law Enforcement Wants Your Private Communications, What Legal Safeguards Are in Place in Latin America and Spain?* February 2, 2021. https://www.eff.org/deeplinks/2021/02/when-law-enforcement-wants-your-private-communications-what-legal-safeguards-are. See also *Despite Progress, Metadata Still Under "Second Class" Protection in Latam Legal Safeguards*, February 3, 2021. https://www.eff.org/deeplinks/2021/02/despite-progress-metadata-still-under-second-class-protection-latam-legal

[52] See Michelle Bordachar. *Nueva ley de delitos informáticos*. December 20, 2021. https://www.derechosdigitales.org/17457/nueva-ley-de-delitos-informaticos/

[53] See more on disputes around safeguards applied to law enforcement access to subscriber data in Brazil in Veridiana Alimonti and Karen Gullo. *Without Changes, Council of Europe's Draft Police Surveillance Treaty is a Pernicious Influence on Latam Legal Privacy Frameworks*. September 3, 2021. https://www.eff.org/deeplinks/2021/09/without-changes-council-europes-draft-police-surveillance-treaty-pernicious

[54] In a landmark ruling affirming data protection as a fundamental right in Brazil's constitution, the country's Supreme Court justices pointed out how changes in our technological landscape demand more cautious treatment of subscriber information. They recalled public telephone directories that contained people's names, telephone numbers, and addresses, asserting that "what could be done from the publicization of such personal data [a few decades ago] is not comparable to what can be done at the current technological level, where powerful data processing, cross-referencing and filtering technologies allow the formation of extremely detailed individual profiles." https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false

information or are based on case law that addresses protections in the context of telephone communications.[55]

In the same vein, making a declaration to require prosecutorial and judicial supervision of foreign direct cooperation orders is only allowed to Parties when signing or ratifying the Protocol (under Article 7(2)(b)). The mandatory inclusion of "prosecutors" in the permitted declaration prevents signatories from requiring the requesting Party to subject its direct orders to judicial oversight only. The requested State, however, can ensure judicial review of direct cross-borders requests received in its territory by requiring that local judicial authorities be simultaneously notified of direct orders (Article 7, paragraph 5 (a) and (e)). The Protocol does not stipulate a final term for this to be invoked by Parties.

(b) Imbalance between safeguards and law enforcement powers in the Protocol

The law enforcement powers the Protocol recognizes are mostly mandatory for all signatories, whereas many of its human rights safeguards are nonessential or applicable depending on broad standards derived from national legal frameworks and states' international human rights law obligations.

Article 7 reflects this imbalance. As seen in the previous section, most of its safeguards are optional and rely on reservations and declarations of State Parties. Other provisions also contain optional statements that can be invoked by Parties and deserve attention within national debates on the accession to the Protocol. For example, another relevant declaration lies in Article 8, paragraph 4, by which Parties may declare that additional supporting information is required to give effect to expedited orders for production of subscriber information and traffic data. The pertinent information may vary in each case, so states may declare that the additional supporting information required will depend on the circumstances of the order and the related investigation or proceeding. **A summarized list can be found in Article 19, which pinpoints all reservations and declarations present in Protocol's provisions.**

This section focuses on Chapter III of the Protocol. It sets human rights and privacy safeguards that apply when states rely on powers outlined by the Protocol.

Article 13's Conditions and Safeguards

Article 13 recognizes a general obligation to ensure adequate protections are in place for human rights and fundamental freedoms. It builds on the Budapest Convention's general safeguards to establish that setting and applying powers and procedures in the Protocol are subject to conditions and safeguards in states' domestic law. This is

[55] See, for example, Argentina's Supreme Court's decision in the Halabi case. http://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-halabi-ernesto-pen-ley-25783-dto-1563-04-amparo-ley-16986-fa09000006-2009-02-24/123456789-600-0009-0ots-eupmocsollaf

particularly important regarding the obligation to incorporate the principle of proportionality in determining the scope of human rights safeguards. Yet, Parties are largely left to determine what protections are "adequate" and "proportionate" on the basis of national law. Various countries in the region rely on the principle of proportionality when balancing and restricting fundamental rights in case law[56] and criminal procedural norms.[57] But the interpretation and application of the principle broadly varies across national frameworks, and, in practice, Article 13 places few direct obligations for State Parties to impose specific safeguards in specific investigative contexts.

We should note, however, that applicable safeguards include rights arising from obligations taken by States under international human rights agreements. The United Nations International Covenant on Civil and Political Rights Article 17 and the American Convention on Human Rights Article 11 are the universal and regional benchmarks among Latin American states for applicable rights and safeguards under Article 13 of the Protocol.[58]

Article 14's Data Protection Safeguards

Article 14 stipulates a series of detailed data protection obligations applicable to any personal information obtained through the Protocol's law enforcement powers. This has particular importance in Latin America since many data protection laws in the region exempt criminal investigations and procedures from their scope and other specific data protection regulations for law enforcement activities—as occurs in the EU with the Law Enforcement Directive—don't exist.

Nonetheless, Article 14 has worrying shortcomings vis-à-vis other international standards, notably the CoE's own Convention 108/108+ (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its amending protocol). In Latin America, Argentina, México, and Uruguay are Parties of the 1981 Convention 108. So far, Argentina has signed, and Uruguay have ratified the Convention 108 amending protocol (Convention 108+).[59] In addition, Article 14's safeguards can be circumvented by the Protocol's signatories. We outline those concerns below.

[56] For example, there is rich a case law regarding the principle of proportionality in Argentina (such as decisions 248:800; 243:449; 334:516; 335:452; 313:1638; 330:855; and 334:516) and in Chile (https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002012000100003). In Peru, the first and most referenced precedent is under the case n. 045-2004-PI/TC, available at https://www.tc.gob.pe/jurisprudencia/2006/00045-2004-AI.pdf

[57] We can mention as examples Article VI of the Preliminary Title and Article 203 of Peru's Criminal Procedure Code, Article 276 of Chile's Criminal Procedure Code, and, among others, Article 12 of Panama's Criminal Procedure Code.

[58] It's relevant to note that the Protocol's evidence-gathering powers aren't limited to domain name registration information (Art. 6), subscriber information (Art. 7 and Art. 8), and traffic data (Art. 8). These powers also involve disclosing communications content, for example, through Article 9, which addresses the expedited disclosure of stored computer data in an emergency.

[59] See Convention 108+ signatures and ratifications at https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223. The Amending Protocol will enter in force once all Parties to the 1981 Convention 108 have ratified the agreement or on 11 October 2023 if there are 38 Parties to the Convention 108+ at this date.

1. Weakening powers related to the assessment of an adequate level of protection in international personal data transfers

A range of data protection laws empower national oversight authorities to assess whether third party countries provide an equivalent level of protection.[60] By these means, they seek to ensure that people's rights can flow along with their data in international data transfers. Some of these laws also empower authorities to suspend personal data transfers when such level of protection is not met. Similarly, the CoE's amending protocol to Convention 108 stipulates that international transfers to recipients under the jurisdiction of States that are not Parties of the Convention 108/108+ may only take place where an appropriate level of protection based on its provisions is secured. It also sets that signatories shall empower their data protection authorities to take steps to safeguard data subjects' rights in international data transfers. These steps include requiring entities to demonstrate that existing safeguards are effective, prohibit or suspend transfers, or subject transfers to conditions that will protect the rights and freedoms of the data subject.[61] However, as we explain below, the Protocol limits such data protection enforcement powers in states Parties' where they would apply:

1.a. Assessing an equivalent level of protection for personal data transfers to third countries: According to Article 14, paragraph 1(d), each Party shall consider that the processing of personal data under Article 14, paragraphs 2 to 15, of the Protocol, or under previous international data transfer agreements between Parties, meets the requirements of Parties' data protection legal frameworks for international personal data transfers. With that, and because relevant protections set in paragraphs 2 to 15 depend on how they are articulated in States' national laws,[62] the Protocol asks Parties to assume a level of protection that may be significantly weak in other Parties' domestic frameworks.[63] Unfortunately, the Protocol has failed to ensure Parties' ability to assess the level of protection of the requesting Party before allowing transfers.[64]

1.b. Suspension of international data transfers: Although the Protocol allows Parties to suspend data transfers if Article 14's safeguards are breached, this is possible only with "substantial evidence" of a "systematic or material breach" or that a "material breach is imminent," and after engaging in consultation with the suspended State (Article 14, paragraph 15).[65] This sets a high bar compared to other instruments, such as the GDPR

[60] In the context of EU Member States, the authority in charge of this assessment is the European Commission.
[61] See Article 14(6) of the Convention 108+.
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000016807c65bf
[62] See, for example, Article 14, paragraph 2(a), paragraph 5, paragraph 11 (b), and paragraph 12(a).
[63] The digital rights organization Access Now raised this concern in their submission to the 6th round of consultations to the Protocol's draft text. https://rm.coe.int/0900001680a25783
[64] In the abovementioned submission, Access Now recommended the Protocol's drafters to replace Article 14, paragraph 1(d), by "a requirement that each Party assess, with the relevant oversight authority for data protection, the level of protection of the requesting Party before allowing transfers." The T-CY Committee did not follow the recommendation.
[65] Exceptionally, a Party may suspend transfers before starting the consultation. According to Article 14, paragraph 15, a Party may provisionally suspend transfers in the event of a systematic or material breach that poses a significant and imminent risk to the life or safety of, or substantial reputational or monetary harm to, a natural person, in which case it shall notify and commence consultations with the other Party immediately thereafter.

and the CoE's Convention 108/108+.[66] In addition, the Protocol doesn't provide for a cooperation mechanism between data protection authorities through which such consultation could take place. In the context of an international agreement, this consultation will then occur at the government level. Data protection authorities empowered by law to suspend transfers will have to involve and obtain the agreement of their national government. This undermines the independence of data protection oversight authorities in Parties where such independence is ensured.[67]

2. Confidentiality of data transfers vs data subject's rights to information and access

The Protocol does not require signatories to provide personal notices to individuals affected by cross-border data transfers based on the Protocol's powers. According to Article 14, paragraph 11(a), states may only provide general notices to the public instead (for instance on a governmental website).[68] It is not clear how the persons affected would be able to understand that a disclosed data request relates to their personal information, and in some way it assumes that people regularly consult websites or repositories displaying such general notices. By this assumption, the Protocol ultimately accepts an ineffective notification as a sufficient measure. Without individual notification (either from the service provider or authorities in either the requesting or requested State) people will have no actual or effective way of knowing that their personal data has been transferred to law enforcement in another country. This disregards international standards that recognize the importance of individual notice for ensuring rights to remedy and a fair processing of personal data for the individuals concerned.[69] Further, even where notification is mandatory in the requested Party, the Protocol allows the Party requesting data to restrict, under conditions set in its own domestic law, any personal notice requirement that may exist under the national law of the requested Party, provided restrictions are needed to protect the rights and freedoms of others or important objectives of general public interest, and give due regard to the legitimate interests of the individual concerned. "Important objectives of general public interest" is a broad clause that can cover far more than protecting ongoing investigations from being compromised. Moreover, Article 14 doesn't require independent oversight for secret data transfers and establishes no deadline for ending confidentiality restrictions. Countries with notification obligations established as a safeguard in national law will likely be hampered in enforcing those laws in cross-border contexts.

---

[66] See GDPR, Articles 46 and 58(2), and Convention 108+, Article 14 (2) to (6).
[67] As EDRi (the European Digital Rights) highlights in its paper *Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention*, 2022, p. 7. https://edri.org/wp-content/uploads/2022/04/EDRi-Position-Ratification-EU-Member-States-Cybercrime-Second-Additional-Protocol.pdf
[68] See Protocol's Explanatory Report, paragraph 267.
[69] The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has emphasized that "[i]ndividuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath." UN Doc A/HRC/23/40. 17 April 2013, paragraph. 82. Available at https://undocs.org/A/HRC/23/40. See also the EU Court of Justice's Opinion 1/15 on the EU-Canada PNR Agreement, ECLI:EU:C:2017:592, paragraph. 220. https://curia.europa.eu/juris/document/document.jsf?docid=193216&doclang=EN

The same limitations apply to a data subject's right to access personal data (Article 14, paragraph 12(a)(i)), which is to be ensured by signatories according to their domestic legal framework. As pointed out by the European Data Protection Supervisor, although the Protocol positively sets standards to gauge restrictions to the right to access, it fails to guarantee that data subjects can, de facto, exercise this right.[70]

3. Biometric data

The Protocol's approach to biometric data undermines a growing international understanding that this type of data is sensitive and requires additional protection given its ability to persistently identify individuals through automated means. Biometric data involves mathematical representations of people's personal features such as their finger, voice or iris prints, and fuels a range of intrusive technologies such as facial recognition. Article 14, paragraph 4, deems biometric data sensitive only "in view of the risks involved."[71] The Protocol provides little guidance on what might constitute this added risk, narrowing the scope of biometric data protection compared to competing laws such as the GDPR, the EU Law Enforcement Directive, the Council of Europe's Convention 108+, and data protection regulations in Latin American countries. All of them recognize the sensitivity of biometric data when used to uniquely identify individuals regardless of the risks involved.[72]

Colombia, Brazil, and Panamá are examples of Latin American countries with data protection laws that include, without further conditions, biometric data in the definition of sensitive personal data.

---

4. Avenues to Circumvent the Protocol's Data Protection Safeguards

Under Article 14, paragraph 1, signatories are explicitly permitted to bypass data protection safeguards detailed on paragraphs 2 to 15 through other international agreements. In contrast to the law enforcement powers established in the Protocol, Parties are allowed to mutually determine that personal data transfers under their power can occur according to terms worked out in superseding agreements or arrangements that will apply "in lieu of paragraphs 2 to 15" (Article 14, paragraph 1(c)). There is no obligation to ensure that superseding agreements adequately protect data or

[70] European Data Protection Supervisor. Opinion 1/2022 (see supra note 46), paragraphs 99 and 107. "[the EDPS] regrets, however, that the Protocol does not require the domestic legal framework of the Parties to make sure that the possibility for data subjects to have access to their own data, de facto, exists, even if limited or exercised through an authority."

[71] Protocol's Explanatory Report, paragraph 237. "Because the level of sensitivity of biometric data may vary, paragraph 4 provides flexibility to Parties to regulate this area by indicating that sensitive data include "biometric data considered sensitive in view of the risks involved." This language recognises that biometrics is an evolving field and what data are considered "sensitive" under this paragraph will need to be evaluated over time in conjunction with technological, investigatory and other developments and the risks to the individual involved."

[72] See Article 4(14 and 9(1) of the GDPR, Article 3(13) and Article 10 of the EU Law Enforcement Directive, and Article 6 (1) of the Convention 108+.

employ safeguards comparable to those set in Article 14. There is no requirement for such agreements or arrangements to be publicly disclosed either.[73]

Of particular concern is how the combination of Articles 12 and 14 may affect data protection in certain jurisdictions. While the latter allows Parties to circumvent its data protection safeguards by mutual agreement, Article 12 empowers frontline law enforcement authorities to enter into informal agreements to govern specific joint investigations on an ad hoc basis on behalf of Protocol's signatories. Supervision of cross-border investigative conduct under these joint teams is left largely to local policing forces. The combined impact of these two provisions seems to be that frontline officials can bypass the Protocol's data protection safeguards, without any approval or input from other Parties' government authorities and no transparency on what has been agreed. In addition, Article 12, paragraph 5, authorizes law enforcement agencies to bypass formalized mutual assistance arrangements already in place for specific investigative tasks. Despite civil society organizations' recommendation to amend the Protocol draft text to prevent joint investigative teams' arrangements from superseding its central data protection safeguards,[74] the text adopted does not clearly preclude this possibility.

At least part of these issues can be mitigated by the declaration allowed in **Article 12, paragraph 3, by which Parties may require its central authority to be a signatory to or otherwise concur in the agreement establishing the team.** Countries acceding to the Protocol should strongly consider invoking such a clause. Once again, this is only allowed at the time of signature or when depositing its instrument of ratification, acceptance or approval.

[73] See Protocol's Explanatory Report, paragraph 223. "In order to provide for legal certainty and transparency for individuals and for the providers and entities involved in data transfers pursuant to measures in Chapter 2, section 2, of this Protocol, *the Parties are encouraged to clearly communicate to the public their mutual determination that such an agreement or arrangement governs the data protection aspects of personal data transfers between them*." [emphasis added]

[74] See EFF, Derechos Digitales, EDRi, Fundación Karisma, CIPPIC, and TEDIC. *Privacy & Human Rights in Cross-Border Law Enforcement*, (supra note 17), p. 13. See further concerns regarding the regulation of Joint Investigative Teams under the Protocol in section 2 of this document.

III. Assessing Accession and Mitigating Weaknesses

As national discussions on the accession to the Protocol gain steam, it is crucial that the content and shortcomings of its text are properly assessed through an open and participative debate. This last section highlights relevant steps and opportunities states and relevant stakeholders should consider and promote as part of this participative process.

Human Rights/Legal Impact Assessment and Constitutional Review

In addition to the a priori review by competent legislative and/or administrative entities of the Protocol's adherence to the country's constitution, national debates on whether to accede to the Protocol should involve a proper legal and human rights impact assessment carried out by the state institutions entitled to approve and ratify international agreements. These assessments should include broad and effective participation of all interested stakeholders, including human and digital rights civil society organizations. It's pivotal that such assessments take into account not only domestic legislation and safeguards that would be impacted, but also states' obligations under international human rights law. Likewise, constitutional review should give particular attention to principles applied to international relations and cooperation, as well as to constitutional privacy and data protection safeguards (including institutional powers of oversight authorities). With this, governments will be better equipped to assess whether to ratify the Protocol and, in this case, reservations and declarations they should invoke. They will also be better equipped to consider legislative reforms resulting from accession so as not to undermine human rights and constitutional protections.

In Case of Adoption, Important Reservations and Declarations to the Protocol's Text

Article 19 indicates the entire set of reservations and declarations mentioned in the Protocol's text and when to invoke them. We list below those specifically recommended by this guide, which serve to mitigate Protocol's shortcomings:

> *Article 7, paragraph 9(a)* - allows Parties to reserve the right not to apply Article 7 for cross-border requests, thereby turning Article 8 into the primary basis by which subscriber data is accessed in cross-border contexts. A Party that reserves to this article is not permitted to issue direct cooperation orders as per Article 7, paragraph 1, of the Protocol to service providers in other signatories' territories.

Alternatively,

Article 7, paragraph 2(b) - a Party may declare that orders issued to service providers in its territory "must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision."

Article 7, paragraph 5 (a) and (b) - allows a Party to require simultaneous *notification* of orders to its national authorities when a direct cooperation request is issued and/or to mandate service providers *consult* the Party's authorities prior to disclosure. Between the two possibilities, the simultaneous notification is the most appropriate for the protection of human rights.

Article 7, paragraph 5(e) - stipulates that Parties must designate a single authority to receive such communications and perform related actions. To ensure a higher level of protection, Parties should designate an independent judicial authority to fulfill this role.

Article 7, paragraph 9(b) - allows Parties to reserve the right not to apply Article 7 to certain types of access numbers (ej. IP addresses). A Party that makes this reservation is not permitted to issue direct cooperation orders for such numbers to service providers in other Parties' territories.

Other articles:

Article 8, paragraph 4 - Parties may require additional supporting information to process expedited requests for production of subscriber information and traffic data.

Article 12, paragraph 3 - Parties may require its Central Authority to be a signatory to or otherwise concur in the agreement establishing joint investigative teams.

This is not intended to be a complete list of all relevant opportunities for reservations and declarations in the Protocol's text. Others are available, and countries should examine these opportunities when deciding whether to accede and when assessing its impacts on existing domestic legislation and the State's human rights obligations.

Additional Safeguards

1. On Data Protection. Accession to the Convention 108/108+

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), with its 2018 amending protocol (Convention 108+),[75] is an influential and pivotal international reference on the protection of personal data, with robust safeguards needed to strike a due balance between law enforcement powers and human rights safeguards. The Protocol's explanatory report states its safeguards complement Convention 108's, but few Latin American countries are Parties to this Convention. National debates on the adoption of the Protocol are a key moment to assess

[75] Protocol's Explanatory Report, paragraph 23.

the opportunity for States to be invited to accede or request accession to the CoE's Convention 108/108+.[76]

2. On Privacy. Ensure Strong Safeguards in National Law

States should also establish, or make sure to preserve, strong privacy safeguards in their domestic legal frameworks. While this does not necessarily address Article 7's main problems, it helps to increase the standard of privacy protection and counter the Protocol's negative influence to drive down privacy standards, especially when it comes to subscriber information.

We list a set of safeguards that States, and decision-makers, should consider:

- Require prior judicial authorization for access to noncontent data including metadata and subscriber data;
- Require clear evidentiary basis for data request;
- Base independent prior judicial authorization on a strong evidentiary showing that the investigative step being contemplated will yield evidence of a serious crime;
- Establish effective independent regulatory oversight of the general operation of the cross-border regime including through audits, spot checks, and annual reporting;
- Provide notification to users about government access to their personal data, effective redress mechanisms, and enough information to assess any impact on their human rights and freedoms;
- Require annual transparency reporting by the State on the volume, nature, and scope of data access demands sent within and across borders, as well as on the data demands received from other States.
- Adopt legal measures to ensure that gag requests—confidentiality and secrecy requests—are not inappropriately invoked when law enforcement make data access demands;
- Explicitly guarantee that domestic legal frameworks recognize biometric data as categorically personal sensitive in all instances, that should be treated with the highest levels of protection.

[76] See more about the accession to the Convention 108 by States which are not member States of the Council of Europe, https://rm.coe.int/16809028a4.