New Protocol to the Cybercrime Convention in LatAm: Challenges and Mitigation Strategies

EFF (*in collaboration with AI Sur*) One-Pager
Revised May 2022

Learn more:
necessaryandproportionate.org/council-of-europe/

Support our work:
eff.org/donate

Now and in the months to come, countries eligible to accede to the Second Additional Protocol to the Council of Europe's Cybercrime Convention will likely conduct national discussions towards its adoption. Opened for signatures on May 12th, 2022, the Protocol sets procedures that seek to enhance international cooperation for law enforcement access to data across borders and poses substantial challenges to human rights and fundamental freedoms. Civil society organizations, activists, and experts working at the intersection of technology and human rights can play a critical role in making sure proper attention is paid to these challenges, promoting mitigation measures in case of adoption, and encouraging effective participation of all interested stakeholders.

Here we provide an advocacy roadmap to help civil society actors on that front. More detailed information about the Protocol can be found in our guide *Assessing New Protocol to the Cybercrime Convention in Latin America*.

Main Concerns:

- The Protocol's direct orders require State Parties to adapt their legislation to authorize competent authorities (e.g. police, prosecutors) to request subscriber information, such as a persons' name and address, from a service provider located in another territory. The standard procedures under Articles 6 and 7 bypass the assessment of a central authority or judicial authority in the territory where the provider is located.

EFF

AlSur

- There is no mechanism to ensure direct cooperation orders are issued by a judicial or other authority independent from those carrying out the investigation in the requesting State Party.

- Relying mainly on service providers to assess foreign direct orders' implications for human rights and fundamental freedoms can undermine rights and safeguards enshrined in the national law of where the service provider is located (e.g. judicial control, privileges/immunities).

- The Protocol's direct cooperation procedures between authorities and service providers in another Party's territory stem from the flawed assumption that subscriber information is inherently less sensitive and private than other types of communications data and "does not allow precise conclusions concerning the private lives and daily habits of individuals concerned". On the contrary, subscriber data is key to identifying users and linking them to their online activities.

- The Protocol's troubling understanding of subscriber information can influence Latin American legal privacy frameworks to drive down protections for the disclosure of this type of data.

- The Protocol has an overall imbalance between law enforcement powers that State Parties are *obliged* to implement *versus* human rights safeguards that are *optional* or *dispensable*.

- The Protocol contains weaker data protection safeguards compared to other settled international standards.

Points to Emphasize:

- Subscriber information is critical to identify users and can reveal people's activities, expressions, relations, and movements. It can be the tip of the iceberg, revealing a detailed profile about someone. Our Guide highlights how the lack of proper safeguards when disclosing subscriber information puts activists, human rights defenders, dissidents, journalists, and everyday people at risk.

- Which protections can be undermined by direct cooperation orders compared to domestic legal safeguards and core principles of international mutual assistance? (e.g. judicial authorization, privileges/immunities, conditions or grounds for refusal that would apply had the subscriber information been sought through mutual assistance).

- How the Protocol's data protection safeguards fall short of more protective international benchmarks (and higher national standards, when applicable), and can be circumvented through other provisions in the Protocol.

Calls for Action to Consider:

- In addition to the analysis of the Protocol's adherence to the country's constitution, seek legal and human rights impact assessments of the Protocol with broad and effective participation of all interested stakeholders.

- Advocate for important reservations and declarations in case of accession to the Protocol (see our Guide).

- Couple debates on whether becoming a Party to the Protocol with assessing the opportunity for the State to be invited to accede or request accession to the Council of Europe's Convention 108/108+, which provides stronger data protection safeguards.

- Ensure robust safeguards in domestic law in case of legal reforms resulting from Protocol's national implementation.

Stakeholders to Engage:

- *Government/State actors*: government agencies responsible for or assigned to safeguard human and fundamental rights, and consumer rights; data protection authorities; judges associations.

- *Civil society*: data protection experts, consumer organizations working with data protection, human rights organizations working on criminal justice, criminal defense lawyers.

- *Companies*: domain name registration services, telecommunications companies, and internet service providers.