Joint contribution by
Derechos Digitales, R3D, IPANDETEC and Hiperderecho
for the Ad Hoc Committee on the Elaboration of a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes - Sixth session

Introduction

The organizations **Derechos Digitales, Red en Defensa de los Derechos Digitales (R3D), Instituto Panamericano de Derecho y Tecnologías (IPANDETEC)** and **Hiperderecho**, part of **AlSur**[1], a consortium of 11 civil society and academic organizations from Latin America seeking to strengthen human rights in the digital sphere in the region, welcome the opportunity to submit their proposals for the Sixth meeting of the Ad Hoc Committee on the Elaboration of a Comprehensive International Convention on Countering the the Use of Information and Communications Technologies for Criminal Purposes.

With reference to the draft text of the convention, as per A/AC.291/22, the undersigned organizations wish to make the following substantive recommendations for Member States' consideration:

A) The need to mainstream gender across the convention as a whole and throughout each article in efforts to prevent and combat cybercrime.

   Add "gender mainstream" to **Articles 24 and 36**.

   Article 5 should include a specific provision emphasizing that women's and girls' rights are human rights and they are at greater risk of technology-facilitated violence, especially adolescent girls and women and girls who face different and intersecting forms of discrimination.

   IInclude provisions specifying that States have the possibility to refuse a request for legal assistance if there are serious doubts that the request may be based on discrimination on grounds of gender or sexual orientation in **Article 40.**

   Reincorporate the need of methods for mainstreaming gender into policy development, legislation and programming in **Article 54.**

B) In **Chapter II on Criminalization**, we recommend **modifications to Articles 6, 8 and 9** regarding the term "dishonest intent" and replacing it with "malicious intent" to narrow the scope; **evaluate the need to maintain Articles 10 to 16** since they duplicate offenses already covered by other articles and because they include common criminal conduct; **establish an exception** for cases of dissemination of intimate images in **Article 15**, as these open the door to revictimization and criminalize the victims themselves; **eliminate Article 17**, as well as **paragraphs b and c of Article 23**, as these are contrary to the guarantee of the exercise of freedom of expression.

C) **In Chapter IV on Procedural Measures and Law Enforcement we recommend: Article 23**: it is necessary to eliminate subparagraphs b and c in order to ensure that procedural measures are only applied to offenses covered by the Convention. **Article 24: it is necessary to add in the first paragraph that the conditions and safeguards in accordance with international law and the gender perspective**

[1] https://www.alsur.lat/

should be included in local legislation. We also recommend reincorporating references to the principles of legality, proportionality and necessity. In the second paragraph, clarify that the conditions and safeguards expressed in this article apply to all procedures or powers provided for in the Convention and are necessary for due justification of the use of procedural measures. **Article 29**: add that the article shall apply to the offenses contained in articles 6 to 16. **Article 30**: replace "in relation to serious offences that it shall determine under its domestic law" with "in relation to Articles 6 and 16 of this Convention".

D) In relation to **International Cooperation**, we recommend eliminating the reference to Article 17 **in Article 35** and adding the requirement of double criminality in order to be able to carry out international cooperation. We also recommend including in **Article 36** the express mention of international human rights law from a gender perspective. Likewise, the principle of protection of personal data is international and should be expressly recognized in the text.

1. ***Gender mainstream***

Recommendations:

- The need to mainstream gender across the convention as a whole and throughout each article in efforts to prevent and combat cybercrime.

  Add "gender mainstream" to **Articles 24 and 36**.

  Article 5 should include a specific provision emphasizing that women's and girls' rights are human rights and they are at greater risk of technology-facilitated violence, especially adolescent girls and women and girls who face different and intersecting forms of discrimination.

  IInclude provisions specifying that States have the possibility to refuse a request for legal assistance if there are serious doubts that the request may be based on discrimination on grounds of gender or sexual orientation in **Article 40.**

  Reincorporate the need of methods for mainstreaming gender into policy development, legislation and programming in **Article 54.**

Rationale:

While we welcome the inclusion of the importance of mainstreaming a gender perspective in the preamble of the zero draft, this reference alone is insufficient to ensure that the Convention is not used to the detriment of people's human rights on the basis of gender.

It is essential to mainstream a gender perspective[2] throughout the convention as a whole and throughout each article. This will enable the Convention to address the specific needs and priorities of women and LGBTQIA+ people as well as the gender-differentiated impacts

[2] Gender mainstreaming is understood as a strategy to make women's and men's concerns and experiences an integral dimension of the design, implementation, monitoring and evaluation of policies and programs in all political, economic and social spheres, so that inequality is not perpetuated. See: https://www.un.org/womenwatch/daw/csw/GMS.PDF

of cybercrime in conjunction with other intersectionalities. This will lead to more effective implementation of the Convention, as well as provide special guarantees of protection for groups in vulnerable situations.

Both digital spaces and penal systems are inserted within societies that account for pre-existing structural inequalities. Neither digital technologies nor the laws and norms that govern them are neutral: they have the potential to promote the exercise of human rights, but they can also perpetuate and aggravate structural inequalities. With this in mind, **Derechos Digitales and APC** have previously[3] emphasized that a **central element of this future convention should be the mainstreaming of a gender perspective, which aims to advance gender equality.**

Gender mainstreaming will enable the Convention to address the specific realities, needs and priorities of women and LGBTQIA+ people, as well as gender-differentiated impacts in conjunction with other intersectionalities. In this sense, the Convention should seek to provide a legal basis that binds signatory states to adopt a gender perspective in their processes of reporting, investigation, sanction and enforcement of sentences. This will lead to a more effective application of the Convention, as well as provide special guarantees of protection to groups in vulnerable situations.

To this end, we propose that the reference to the need to mainstream a gender perspective be added to articles that we consider need special protection guarantees due to their capacity to deepen gender inequalities. This, in order to prevent other human rights from being violated in the application of the Convention.

2. **Criminalization.**

Recommendations:

- **Articles 6, 8 and 9**: remove the expression "dishonest intent" and replace it with "malicious intent".
- **Article 10**: evaluate whether its permanence in the Convention is necessary given that the offenses it seeks to combat are already enshrined in Articles 6 to 9 of the Convention and its permanence criminalizes the technology.
- **Article 15:** remove the reference to the intention to cause harm and establish an exception for cases of dissemination of material through complaints made by victims or journalists.
- **Articles 11 to 16**: it is necessary for States to evaluate the permanence of these articles in the Convention, because they contain common criminal conduct that can be committed through technologies.
- **Article 17:** it is necessary to delete the article in its entirety.

Rationale:

In the chapter on **Criminalization (Art 6-21)** we welcome the reduction of the catalog of offenses in the new version of the presidency from 30 to 11 offenses.

[3] Joint contribution of Derechos Digitales and the Association for Progressive Communications (APC). Fifth session of the AHC on Cybercrime. Available at: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main

The new text focuses on offenses committed through and against computer systems (cybercrimes)[4]. We celebrate that the current text avoids including content-related offenses that criminalize activities related to the legitimate exercise of citizens' rights.

However, in some of the offenses included in the first draft there are still ambiguities in the wording that could criminalize the work of journalists and digital security researchers, as well as human rights defenders, activists and journalists. With the consequent generation of gender-differentiated impacts and revictimization.

Latin America has been consolidating as a dangerous region for activists, journalists, defenders and researchers to defend their rights. This is due to the fact that governments have implemented various mechanisms of repression and obstruction against the exercise of citizens' civil rights. Criminalization and surveillance are mechanisms to hinder the work carried out by these actors in defense of democracy and the rule of law.

Currently, there is a pressing need for criminal instruments based on a gender and human rights perspective. The current legislative trend allows the increase in the arbitrary use of surveillance technologies by States instead of preventing the prosecution of actors with positions and opinions critical of the States.

Organizations throughout the Latin American region[5] have repeatedly reported to the IACHR serious cases of these arbitrary uses: judicial persecution of journalists, the use of content laws against women and LGBTQIA+ activists to criminalize legitimate expressions at regional and global level[6], the persecution of whistleblowers[7], the use of Osint software for investigations[8] [9], the use of spyware[10] or the prosecution of investigators[11].

The criminalization generated by the abuse of these laws has already been identified by human rights mechanisms as a "growing trend around the world", which has opened the door to surveil and punish activists, causing a significant chilling effect on advocacy and mobilization, hindering the work of human rights defenders and endangering their safety in a manner contrary to international law[12].

---

[4] Human Rights Watch. Letter to the UN Ad Hoc Committee on Cybercrime. Available at:: https://www.hrw.org/news/2022/01/13/letter-un-ad-hoc-committee-cybercrime

[5] They denounced before the IACHR the advance of "judicial harassment" against journalists in Latin America. Clarín. Available at: https://www.clarin.com/politica/denunciaron-cidh-avance-acoso-judicial-periodistas-america-latina_0_en4HJXFUSv.html. Article 19. Judicial harassment of journalists and human rights defenders, the victim is freedom of expression. Available at: https://articulo19.org/acoso-judicial-a-periodistas-y-defensoresas-de-derechos-humanos-la-victima-es-la-libertad-de-expresion/

[6] Derechos Digitales. Normativas contra los ciberdelitos como herramientas para silenciar mujeres y personas LGBTQIA+ alrededor del mundo, July 5, 2023. Available at: https://www.derechosdigitales.org/21876/cuando-la-proteccion-se-transforma-en-amenaza-normativas-contra-los-ciberdelitos-como-herramientas-para-silenciar-mujeres-y-personas-lgbtqia-alrededor-del-mundo/

[7] CIDH. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/180.asp

[8] https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/

[9] https://datysoc.org/informe-ciberpatrullaje/

[10] https://www.nytimes.com/es/2023/04/18/espanol/pegasus-mexico-gobierno-ejercito.html

[11] https://www.youtube.com/watch?v=mVNzL0l5U3k

[12] UN - General Assembly. Implementation of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms by Providing a Safe and Enabling Environment for Human Rights

Recent research[13] by Derechos Digitales and APC highlights the need to consider the gendered impacts of this criminalization, on the basis that freedom of expression is essential for gender equality. The report provides concrete evidence, through 11 cases mapped globally, of the trend of the use of these regulations as a legal tool to silence critical voices, which has a differential impact on the activism of groups historically excluded from public debate such as women and LGBTQIA+ people. The cases demonstrate that we are not talking about potential risks, but about concrete harms, which raises the alarm about the dangers in advancing on international norms on the matter without taking into account national contexts or including safeguards for the protection of human rights, particularly of historically marginalized groups.

The guarantee of the exercise of freedom of expression necessarily requires a safe and enabling environment in order to be effective. Therefore, legislation that criminalizes the ability to express social demands related to structural inequalities -either because of the content of the expression or because of the gender of the person expressing their opinion- excludes women, since illegitimate restrictions directly threaten their visibility and full participation in public life[14]. Following the Inter-American Court of Human Rights, one of the main consequences of silencing is that it "leads to an increase in the gender gap (...) and undermines pluralism as an essential element of freedom of expression and democracy"[15].

The zero draft includes a new article on **Offenses relating to other international treaties (Art. 17)** which opens a loophole to apply the Convention to other conducts not contemplated in the treaty, leading to risks of criminalization.

Article 17 establishes the obligation of States to take the necessary measures to penalize and prosecute actions defined as offenses in "international treaties and protocols" when committed through the use of technologies. This wording is ambiguous and poses a serious risk to the sovereignty of countries and human rights.

The broadness of the provision enables the inclusion of content related offences that were listed in previous versions, in addition to any other offence that is recognized in another treaty, even if the States Parties to the Convention have not agreed to it.

For example, taking into account that there are conventions relating to matters such as terrorism or trafficking in persons, among many others, some of the conducts excluded directly from the text of the cybercrime convention could end up being reinstated at the

---

Defenders and Ensuring their Protection. A/RES/74/146. Available at: https://digitallibrary.un.org/record/3847133

[13] Derechos Digitales. Normativas contra los ciberdelitos como herramientas para silenciar mujeres y personas LGBTQIA+ alrededor del mundo, July 5, 2023. Available at: https://www.derechosdigitales.org/21876/cuando-la-proteccion-se-transforma-en-amenaza-normativas-contra-los-ciberdelitos-como-herramientas-para-silenciar-mujeres-y-personas-lgbtqia-alrededor-del-mundo/

[14] IACHR. Office of the Special Rapporteur for Freedom of Expression. Office of the Special Rapporteur for Freedom of Expression expresses concern about the criminal investigation initiated in Chile against members of Las Tesis. Press Release R152/20. Available in Spanish at: https://www.oas.org/es/cidh/expresion/showarticle.asp?lID=2&artID=1178

[15] Inter-American Court of Human Rights. Case of Bedoya Lima et al. v. Colombia. Judgment of August 26, 2021, par. 113. Available at: https://www.corteidh.or.cr/docs/casos/articulos/seriec_431_ing.pdf

national level[16]. At the same time, the article does not contain a time limitation allowing that future treaties, created for example bilaterally, could be included.

Therefore, it is important to ensure that the Convention is in line with the defense of human rights and does not legitimize the increase of mechanisms of criminalization of the exercise of rights. To achieve this, it is not only essential to include a human rights and gender perspective in an intersectional manner, but it is also urgent to take into account the historical and political context of the Latin American countries.

Consequently, we present below our recommendations for Chapter II Criminalization. The drafting proposals for this chapter can be found in **ANNEX I** at the end of this document.

Articles 6, 8 y 9

The **crimes of Illegal access (Art. 6), Interference with data or information (Art. 8), Interference with a system or device (Art. 9)** are formulated as <<Intentionally and without right>> and with <<dishonest intent>>, leaving the door open to arbitrary interpretations that hinder the work of investigation[17].

Considering that defenders, researchers, activists and journalists can be criminalized through these offenses, it is necessary that "dishonest intent" be replaced by "malicious intention". In addition, the wording should include specific provisions that explicitly protect legitimate investigative activities by citizens.

Similarly, it should incorporate the element of material harm to avoid criminalization of the activities of security investigators.

Article 10. Misuse of devices offense

This article contains ambiguous and broad wording that could criminalize the acquisition and use of technologies that allow the exercise or protection of human rights. Mainly, it puts at risk essential actors for a free and safe internet such as security researchers, journalists or academic staff.

It is necessary not to criminalize the tool and to understand the reach that these technological developments can have for a democratic society. The use of words such as <<possession>>, <<obtaining>>, <<production>>, <<sale>>, <<acquisition>>. criminalize the tool and not its use with malicious intentions that result in material damage.

Article 15. Non-consensual dissemination of intimate images

We acknowledge that the crime of non-consensual dissemination of intimate images **(Art. 15)** is extremely serious for the region. Therefore, the text must be improved to ensure that

[16] An example of the possible misuse of terrorism-related legislation associated with the internet is the case of prosecutions during protests in Colombia in 2021. In this regard, UN experts have publicly expressed their concern regarding the use of anti-terrorism provisions to prosecute protesters. Available at: https://www.ohchr.org/es/press-releases/2023/03/colombia-misuse-counter-terrorism-measures-prosecute-protesters-threatens

[17] For more information on the legal risks for cybersecurity researchers, we recommend consulting the following source: https://github.com/disclose/research-threats.

the text does not result in revictimization or criminalizing legitimate activities of the victims and their companions.

First, the term nudity tends to have an ambiguous interpretation. This concept may exclude sexual content of people who were not fully nude or include non-sexual, non-intimate content of parts such as arms, legs, shoulders that are not covered by clothing. While it is vital to maintain the element of the victim's consent, the conduct to be prosecuted must also be specified.

Likewise, the offense does not establish legitimate exceptions to cases of dissemination that may result in the criminalization of the victims themselves, their companions or journalists. For example, sharing evidence to their legal advisors where there is content of other people besides the victim.

Finally, it is vital that the text eliminates the intention to cause harm as a necessary requirement for this crime and replaces it with "with knowledge of the lack of consent of the victim". The harm to the victim of this crime occurs from the moment the content is shared without his or her consent. Many of these cases happen secretly behind the victim's back for purposes other than causing direct harm to the victim. Therefore, adding an intentionality requirement imposes an unjustified burden of proof on the victims.

Article 17. Offenses related to other international treaties

We strongly recommend deleting this article. This provision opens the door to the inclusion of crimes that are not cyber-dependent, can be applied arbitrarily and infringe on the sovereignty and human rights of the States Parties.

3. Chapter IV. Procedural Measures and Law Enforcement

Recommendations:

- **Article 23:** it is necessary to remove paragraphs b and c in order to ensure that procedural measures are only applied to offenses covered by the Convention.
- **Article 24:** it is necessary to add in the first paragraph that the conditions and safeguards in accordance with international law and the gender perspective should be included in local legislation. We also recommend reincorporating references to the principles of legality, proportionality and necessity. In the second paragraph, clarify that the conditions and safeguards expressed in this article apply to all procedures or powers provided for in the Convention and are necessary for due justification of the use of procedural measures.
- **Article 29:** add that the article applies to the offenses contained in articles 6 to 16.
- **Article 30:** replace "in relation to serious offenses that it shall determine under its domestic law" with "in relation to Articles 6 and 16 of this Convention".

Rationale:

Article 23. Scope of procedural measures

The wording o**f Article 23** second paragraph, clearly allows the Convention to be applied to other criminal offenses not covered by the criminalization chapter.

This broad wording poses a risk that law enforcement agencies may apply measures that seriously interfere with the right to freedom of expression of individuals in order to, for example, prosecute misdemeanors or criminal content-related offenses, which are inherently incompatible with States' human rights obligations. It is also incompatible with international standards of proportionality and necessity considering it enables criminal authorities to apply intrusive measures that could seriously harm the right to privacy of individuals.

In this regard, we recommend the removal of **subparagraphs b and c, paragraph 2, Article 23**, in order to ensure that procedural measures are only applied to offenses directly included in the Convention.

Article 24. Conditions and safeguards

The chapter on criminal procedural measures contains three main problems: (i) it introduces highly invasive surveillance powers in its **articles 27 to 30**[18]; while **article 24**: (ii) offers limited democratic controls and essential safeguards against their abuse; and (iii) applies only to this chapter.

The relevance of effective safeguards against the abuse of undercover electronic surveillance measures has been highlighted by the United Nations General Assembly[19], the UN Special Rapporteur on the Right to Freedom of Expression and Opinion[20], the UN High Commissioner for Human Rights[21], the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights[22], as well as by civil society organizations and

[18] For example, Article 28 provides for the search and seizure of stored computer data, including personal devices, which contain a large amount of personal information about the individual. Similarly, Article 29 provides for the real-time collection of traffic data, which represents sensitive personal data that may reveal patterns of movement, communication, relationships, activities and browsing habits. For its part, Article 30 establishes the power for "competent authorities" to obtain or record content-related data in real time "in relation to various serious offenses to be determined in its domestic law", without being subject to cybercrimes and leaving a dangerous margin of action for certain States to include valid expressions in the exercise of freedom of expression. It also requires the confidential cooperation of service providers to assist in the collection or recording of data.
[19] General Assembly of the United Nations. Resolution A/RES/68/167 on the right to privacy in the digital age. December 18, 2013.
[20] UN. Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression Frank La Rue. April 17, 2013. A/HRC/23/40, para. 81: "Legislation should stipulate that State surveillance of communications should occur only under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards should be articulated in law regarding the nature, scope and duration of possible measures, the grounds necessary to order them, the authorities competent to authorize, carry out and supervise them, and the type of remedies provided for in law to obtain redress."
[21] OHCHR, The Right to Privacy in the Digital Age, 30 June 2014, A/HRC/27/37, para. 37. Article 17(2) of the International Covenant on Civil and Political Rights provides that everyone has the right to the protection of the law against unlawful or arbitrary interference or attacks. The "protection of the law" must be granted through effective procedural safeguards, including effective and adequately funded institutional arrangements. It is clear, however, that the lack of effective oversight has contributed to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards, without independent external monitoring, have proven particularly ineffective against illegal or arbitrary surveillance methods. While these safeguards can take a variety of forms, the involvement of all levels of government in the oversight of surveillance programs, along with independent civilian agency oversight, is essential to ensure effective protection of the law.
[22] IACHR. Office of the Special Rapporteur for Freedom of Expression. Freedom of Expression and the Internet. December 31, 2013. OEA/Ser.L/V/II.

experts who have collected best practices derived from comparative jurisprudence and doctrine, as well as by civil society organizations and experts who have compiled best practices based on comparative jurisprudence and doctrine and have elaborated the International Principles on the Application of Human Rights to Communication Surveillance (the "Necessary and Proportionate Principles) [23].

Article 24. Paragraph 1

In many Latin American experiences, authorities —often without the legal powers to carry out surveillance measures— motivate the use of such measures based solely on vague considerations of national security or the fight against terrorism[24].

The **Inter-American Court of Human Rights (IACHR)** has pointed out that in the context of covert surveillance measures, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the conditions, circumstances and procedures under which the authorities will be authorized to resort to such measures[25].

In order for restrictions to rights such as privacy, protection of personal data and freedom of expression to comply with national and international human rights standards, they must meet the requirements of **legality, necessity and proportionality, which implies the establishment of adequate safeguards to prevent, avoid and remedy their abusive exercise.**

In this regard, we recommend that the first paragraph of the article be modified to ensure that the principles referred to above, safeguards such as judicial control, right to notification and transparency measures, as well as the gender perspective, be included both in the Convention and in local legislation. In this line, we note with concern that references to the obligation to adequately protect human rights and freedoms, as provided for in the Budapest Convention, were excluded.

Article 24. Paragraph 2.

The current wording of **Article 24, paragraph 2**, establishes that the conditions and safeguards established shall include judicial or other independent review. This wording encourages the discretion of States and is conducive to the abuse of surveillance measures. The existence of a standard of necessity or justification of the measures is indispensable to inhibit the risks of abuse of surveillance measures.

Laws authorizing the application of restrictions to our rights must use precise criteria and not confer uncontrolled discretion to those in charge of their application. Therefore, we

[23] International Principles on the Application of Human Rights to Communications Surveillance, available at: https://es.necessaryandproportionate.org/text.
[24] For example, in Mexico, the acquisition of Pegasus spyware by authorities that did not have the authority to intercept private communications, such as the Ministry of Defense, has been reported. The evidence gathered leaves as an incontrovertible fact that Mexican government agencies hired and used Pegasus to spy on journalists, activists, human rights defenders, among others. Likewise, the acquisition of licenses for the use of surveillance malware marketed by the Italian company Hacking Team by multiple authorities without powers, such as the Ministry of Government of the State of Jalisco, the Ministry of Planning and Finance of the Government of Baja California or even Petróleos Mexicanos, has been documented.
[25] IACHR Court. Case of Escher et al. v. Brazil. Preliminary Objections, Merits, Reparations and Costs. Judgment of July 6, 2009. Series C No. 200.

recommend deleting this expression to clarify that the conditions and safeguards expressed in this article apply to all procedures or powers provided for in the Convention and are necessary for a proper justification of the use of procedural measures.

Safeguards

We recommend, first of all, the need to include the principles of legality, proportionality and necessity. States must demonstrate that any restrictions applied are necessary and proportionate to the objective.

For example, with respect to restrictions on freedom of expression, UN mechanisms have held that "the principle of necessity and proportionality presumes that restrictions cannot be justified when the harm to freedom of expression outweighs the benefits"[26]. Likewise, the IACHR Court has recognized, when assessing the necessity of a limitation to the right to freedom, that necessary means that the means chosen "are absolutely indispensable to achieve the end pursued, and that among all the possible measures, there is none less severe in relation to the right involved, which is so adequate to achieve the proposed objective".

Secondly, we consider the establishment of adequate safeguards to prevent, avoid and remedy the abusive exercise of the procedural measures provided for in the chapter crucial.

On the one hand, we propose specific guidelines regarding the judicial **control procedure** as an essential element to prevent the abuse of power by States, especially considering the regional context where evidence persists of the use of surveillance measures without judicial control[27] and legal uncertainty regarding the imperative need for prior or immediate judicial control to carry out such surveillance measures[28]. Such independent judicial control cannot be replaced by other types of independent review. Along these lines, the text should clarify which procedural measures must be unavoidably authorized by a judicial authority prior to their implementation and which can only be subject to subsequent, but timely, review.

On the other hand, the fact that most of these measures are carried out in secrecy makes the **right of notification** to the affected user particularly important as a fundamental

[26] Idem
[27] For example, in Mexico, between 2016 and 2019, around 60 percent of requests for access to retained data were made without judicial oversight. This percentage includes both requests made without judicial authorization and those made through emergency mechanisms. About 75 percent of the requests without prior judicial authorization were made through emergency mechanisms, and about 50 percent of these requests were not or only partially ratified.
Regarding the above, there is no evidence that in these cases the authorities whose surveillance measures are systematically not ratified face any disciplinary process or that the affected persons are notified that their privacy was unjustifiably invaded.
[28] The fundamental relevance of prior or immediate judicial control of covert surveillance measures that invade the privacy of individuals has been highlighted by the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, which has pointed out that: "Decisions to carry out surveillance tasks that invade the privacy of individuals must be authorized by independent judicial authorities, which must account for the reasons why the measure is suitable to achieve the purposes it pursues in the case of the individual:
Decisions to carry out surveillance tasks that invade the privacy of individuals must be authorized by independent judicial authorities, who must account for the reasons why the measure is suitable to achieve the ends pursued in the specific case; whether it is sufficiently restricted so as not to affect the right involved more than necessary; and whether it is proportional with respect to the interest it seeks to promote. IACHR. Office of the Special Rapporteur for Freedom of Expression. Freedom of Expression and the Internet. December 31, 2013. OEA/Ser.L/V/II, para. 165.

safeguard to protect the right to privacy, guarantee due process and access to an effective remedy. This right establishes the obligation on the part of the authority to notify a person that his or her privacy or personal data were interfered with through a covert surveillance measure[29].

Finally, it is necessary to establish **transparency mechanisms** so that covert surveillance measures are recorded in a detailed and immutable manner. In cases of abuse of surveillance measures, many obstacles to clarification of cases, accountability and reparations for victims persist. Reliable records regarding the acquisition and use of surveillance tools are an effective tool to avoid these obstacles.

Articles 29 y 30:

Under the same arguments concerning the need to limit the scope of the Convention to prevent it from being used in an abusive or arbitrary manner, we propose to include the reference that these articles shall apply only to the offenses included in articles 6 to 16 of the Convention.

This is especially important considering the highly intrusive nature of the powers granted in the articles in question. From a gender perspective, it is also important to keep in mind that there is a significant risk of overuse or misuse of law enforcement powers under this chapter of the consolidated negotiating document to collect data on a wide range of vulnerable or high-risk individuals or communities. Women and other marginalized groups are affected by this more severely because of their position in society, exposing sensitive information relating to personal health, sexuality and gender identities and expressions. These provisions could be used, for example, to monitor location data and/or the use of fertility tracking apps by individuals who may become pregnant, in order to determine proximity to sexual and reproductive health services.

4. Chapter V. International Cooperation

Recommendations:

Article 35: remove the reference to **article 17** and add the requirement of double criminality in order to be able to carry out international cooperation.

Article 36:

- The safeguards established in the procedural measures should also be applicable to international cooperation measures, especially in the transfer of personal data.
- Include express mention of international human rights law and the gender perspective. In addition, it is suggested to add human rights-based minimum standards of data protection, such as the principles of lawful and fair processing, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.
- Take into consideration gender-related risks in personal data protection.

Rationale:

[29] Although such notification may not be carried out in advance or immediately, as it could frustrate the success of an investigation, it must be made when an investigation is not at risk, there is no risk of flight, destruction of evidence or knowledge may generate an imminent risk of danger to the life or personal integrity of any person.

The main concern of the international cooperation section is the lack of safeguards in the mutual legal and technical assistance powers given to States.

The international cooperation section should point out that **Article 24** of this Convention also applies to the international cooperation chapter, so as to standardize the application of such safeguards as a minimum and essential criterion, regardless of the jurisdiction in which such surveillance measures are being carried out.

Artícle 35. General principles of international cooperation

As mentioned in previous sections, it is essential that the scope of the Convention be limited to the offenses recognized in articles 6 to 16. By removing the reference to Article 17, a clear legal framework for international cooperation is provided, ensuring that the Convention is not used to the detriment of the rights of freedom of expression and association, among others.

As for the principle of dual criminality as a requirement for international cooperation, it needs to be included as an obligation to ensure that cooperation is not requested for political, gender-based discrimination and/or arbitrary reasons. From a gender perspective, it is important to consider that in many countries gender identity, sexual orientation and/or abortion are issues that are criminalized, generating serious risks of surveillance and criminalization for women and persons belonging to the LGTBIQ collective.

Article 36. Personal data protection

The article only mentions the applicable domestic law on personal data protection as an exception to the obligation to transmit personal data.

This provision is insufficient because the protection of personal data is a right, along with the right to privacy, that is recognized by international human rights law and regional legal frameworks such as the Inter-American System. This is especially important when considering that not all countries have personal data legislation.

We recommend including an express mention of international human rights law from a gender perspective and making reference to specific international standards in the first paragraph of Article 36 States Parties shall not be obliged to transmit personal data in compliance with this Convention if, in accordance with their applicable personal data protection laws and human rights-based minimum standards of data protection, such as the principles of lawful and fair processing, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

The text states that only effective domestic law safeguards are applicable to the transfer of personal data between States. Similarly, the text ambiguously establishes the obligation of States to apply these safeguards. This is because the verb "shall ensure" can be interpreted as a discretionary option or power, instead of the express obligation of States to protect the right to privacy and protection of personal data.

We recommend that the text state that the safeguards of **Article 24** are applicable to all international cooperation measures, including those related to the transfer of personal data.

The international cooperation chapter should apply a gender perspective. This perspective is implemented by analyzing the gender-differentiated impacts of data collection for vulnerable or high-risk communities. Differential protection safeguards must be included to ensure the protection of the rights of these communities.

Data collection never takes place in a gender-neutral environment. It is crucial that data collection, storage and transfer be subject to an intersectional gender analysis to identify the risks to individual security that such procedures entail. For example, broad powers to exchange data between States can be problematic for individuals with diverse sexual identities, expressions and orientations, both in general and in jurisdictions where LGBTQIA+ identity expression is not currently legally permitted and/or for women/pregnant women in jurisdictions where access to abortion is prohibited, creating high risks of criminalization and surveillance.

In this sense, as we have already pointed out in previous sections, it is imperative to add that the gender perspective must be applied within the framework of human rights, understanding that gender issues -including sexuality, gender identity and gender expression- are private personal data that require special protection.

The recommendations made are in line with UN resolutions on privacy. For example, the latter[30] emphasizes that States should respect international human rights obligations relating to the right to privacy when collecting personal data, when sharing or otherwise facilitating access to data collection through, inter alia, information and intelligence, and when requiring disclosure of personal data to third parties, including companies.

Submitted by NGOS registered under operative 8 or 9:

Derechos Digitales
Red en Defensa de los Derechos Digitales (R3D)
Instituto Panamericano de Derecho y Tecnologías (IPANDETEC)
Hiperderecho

The full list of signatory supporters from Al Sur Consortium:

Asociación TEDIC
CELE - Centro de Estudios en Libertad de Expresión y Acceso a la Información
Idec - Instituto Brasileiro de Defesa do Consumidor
Fundación Karisma

[30] General Assembly. A/RES/77/211. Resolution adopted by the General Assembly on 15 December 2022. The right to privacy in the digital age (p. 5). https://www.undocs.org/A/RES/77/211

Annex 1 - Text changes proposal

Mainstream gender across the convention as a whole and throughout each article in efforts to prevent and combat cybercrime.

Chapter I General Provisions

Article 5. Respect for human rights

States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law, the principle of equality and non-discrimination and gender equality.

Chapter II Criminalization

Article 6. Illegal access

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of [a computer system] [an information and communications technology device] ~~without right.~~ with malicious intent.
2. A State Party may require that the offence be committed by infringing security measures, with the malicious intent of obtaining [computer data] [digital information] or other ~~dishonest~~ malicious intent or in relation to [a computer system] [an information and communications technology device] that is connected to another [computer system] [information and communications technology device]
3.States Parties should require as a condition that the acts described in paragraphs 1 and 2 result in serious harm.

Article 8. Interference with [computer data] [digital information].

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed with malicious intent ~~without right~~, the damaging, deletion, deterioration, alteration or suppression of [computer data] [digital information].
2. States Parties should require as a requirement that the acts described in paragraph 1 result in serious harm.

Article 9. Interference with a [computer system] [information and communication technology device].

1. Each State Party shall adopt such legislative and other measures as may be

necessary to establish as criminal offences under its domestic law, when committed ~~without right~~ with malicious intent, the serious hindering of the functioning of [a computer system] [an information and communications technology device] by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing [computer data] [digital information].

2. States Parties should require as a condition that the acts described in paragraph 1 involve serious harm.

Chapter IV. **Procedural Measures and Law Enforcement**

Article 24. Conditions and safeguards

1. Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall be consistent with its obligations under international human rights law and commitment to gender mainstreaming, and which shall incorporate the principles of proportionality necessity, legality, and the protection of privacy and personal data, to include data relating to gender and sexuality and privileged communications.

2. Such conditions and safeguards should include: ~~as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent review, grounds justifying application, and limitation of the scope and the duration of such power or procedure.~~

A) Procedures for prior independent judicial authorization for measures referred to in Articles 27 to 31, and expedited judicial review of measures referred to in Articles 25 and 26.

B) The obligation to keep detailed records of the measures implemented. The records must be accessible to the authorities in charge of investigating the potential illegal or abusive use of such procedural measures.

C) The obligation of the authorities authorized to exercise any of the powers and procedures provided for in this chapter, and of any service provider assisting in any way in the implementation of the procedural measures, to produce an annual transparency report disclosing, at a minimum, disaggregated statistical information regarding the number of measures implemented, authorized or rejected; as well as the number of persons, accounts or devices affected by such measures.

D) Notification of any person whose personal data is subject to the procedural measures provided for in this chapter. Notification may be delayed without prior independent judicial authorization for a maximum period of one year after the procedural measure began to be implemented.

E) The establishment of an independent supervisory body authorized to randomly audit the implementation of the procedural measures.

3. ~~To the extent that it is consistent with the public interest, in particular the proper administration of justice, each State Party shall consider the impact of the powers and procedures in this article upon the rights, responsibilities and legitimate interests of third parties.~~
The powers and procedures in this chapter should not be designed to require any person or service provider to compromise the security or integrity of its services or to create significant risks to third parties.

Article 29. Real-time collection of traffic data

1. With respect to the criminal offences established in accordance with Articles 6 to 16 of this Convention, each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
(...)

Article 30. Interception of content data

Each State Party shall adopt such legislative and other measures as may be necessary, with respect to the criminal offenses established in accordance with articles 6 to 16 of this Convention, to empower its competent authorities to:

(...)

Chapter V. International Cooperation

Article 35. General principles of international cooperation

1. States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of investigations, prosecutions and judicial proceedings concerning offences established in accordance with articles 6 to 16 of this Convention, or for the collection, obtaining, preservation and sharing of evidence in electronic form of offences established in accordance with articles 6 to 16 of this Convention, ~~as well as of a serious crime including those offences covered by article 17 of this Convention when applicable.~~ This cooperation is subject, in all cases, to compliance with the principle of dual criminality.

Article 36. Protection of personal data

1. A State Party transferring personal data pursuant to this Convention shall do so subject to the conditions of that State Party's domestic law and applicable international human rights

law applying a gender perspective. States Parties shall not be required to transfer personal data in accordance with this Convention if it cannot be provided in compliance with their applicable laws concerning the protection of personal data and with minimum human rights based data protection standards, such as the principles of lawful and fair processing, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. They may also seek to impose conditions, in accordance with such applicable laws, to achieve compliance in order to respond to a request for personal data. States Parties are encouraged to establish bilateral or multilateral arrangements to facilitate the transfer of personal data.

2. For personal data transferred in accordance with this Convention, States Parties shall ensure that the personal data received are subject to effective and appropriate safeguards established in this Convention, in international human rights law and in their respective legal frameworks".

Article 40. General principles and procedures relating to mutual legal assistance

(...)

21. Mutual legal assistance may be refused:

(a) If the request is not made in accordance with the provisions of this article;
(b) If the requested State Party considers that that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests;
c) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;
d) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted;
e) If the execution of the request would prejudice, inter alia, the protection of human rights or fundamental freedoms and gender equality.

Chapter VII Technical Assistance and Information Exchange

Article 54. Technical assistance and capacity-building

3. Activities referred to in paragraphs 1 and 2 of this article may include, to the extent permitted by domestic law, the following:
(a) Methods and techniques used in the prevention, detection, investigation and prosecution of the offences covered by this Convention;
(b) Methods for integrating a gender perspective into policy development, legislation and planning;
(c) Building capacity in the collection, preservation and sharing of evidence, in particular in electronic form, including the maintenance of the chain of custody and forensic analysis
(d) Modern law enforcement equipment and the use thereof;

(e) Training of competent authorities in the preparation of requests for mutual legal assistance and other means of cooperation that meet the requirements of this Convention, especially for the collection, preservation and sharing of evidence in electronic form;
(f) Prevention, detection and monitoring of the movements of proceeds deriving from the commission of the offences covered by this Convention, property, equipment or other instrumentalities and methods used for the transfer, concealment or disguise of such proceeds, property, equipment or other instrumentalities;
(g) Appropriate and efficient legal and administrative mechanisms and methods for facilitating the seizure and return of proceeds of offences covered by this Convention;
(h) Methods used in the protection of victims and witnesses who cooperate with judicial authorities;
(i) Training in relevant substantive and procedural law, and law enforcement investigation powers, as well as in national and international regulations and in languages.
(...)