

SITUATION REPORT: HUMAN RIGHTS AND TECHNOLOGY IN PARAGUAY



INDEX

EXECUTIVE SUMMARY	3
I. RESTRICTION OF CIVIC SPACE AND FREEDOM OF ASSOCIATION: THE ANTI-NGO LAW	4
Features and threats of the law	4
II. EXPANSION OF STATE SURVEILLANCE AND THE RIGHT TO PRIVACY	5
Acquisition and Use of Surveillance Technologies	5
Surveillance of social protest	5
Misappropriation of public funds	5
III. PERSONAL DATA PROTECTION AND CYBERSECURITY	6
Legal framework for Data protection	6
Cybersecurity and Human Rights Defenders	6
Cybersecurity legislative proposals	7
IV. TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE (TFGBV)	7
Insufficient Legal Framework and Access to Justice	7
TFGBV against female journalists and politicians	8
V. FREEDOM OF EXPRESSION AND THE DIGITAL DIVIDE	8
Censorship through the distorted use of the law	8
Absence of net neutrality	8
VI. INTERNET ACCESS AND DIGITAL EXCLUSION	9
Key Statistics on the Digital Divide	9
Deliberate blackouts and misappropriation of funds for connectivity	9
VII. SUMMARY OF KEY RECOMMENDATIONS	10

EXECUTIVE SUMMARY

This report summarizes the main concerns regarding the intersection of human rights and technology in Paraguay, based on three stakeholder submissions for the 52nd session of the Universal Periodic Review (UPR)¹ by TEDIC², made jointly with the Association for Progressive Communications (APC)³, Artigo19⁴, and Derechos Digitales of Latin America⁵. Key findings reveal a deterioration in the environment for civil society and fundamental freedoms.

First, there has been a **significant restriction of civic space** through the enactment of Law No. 7363/24, known as the “Anti-NGO Law.” This ambiguous and punitive legislation imposes excessive controls that threaten the autonomy and work of civil society organizations, in a context of attacks and disinformation against entities such as TEDIC.

Second, the **expansion of state surveillance capacities** is taking place without an adequate legal framework, transparency, or independent oversight. The acquisition and use of technologies such as facial recognition, IMSI catchers, and drones, partly financed with public funds intended to reduce the digital divide, pose serious risks to the right to privacy. The monitoring of peaceful protests demonstrates the use of these tools for social control.

Third, **technology-facilitated gender-based violence (TFGBV)** is a widespread and structural phenomenon. The existing legal framework, mainly Law No. 5777/16, is insufficient to address the complexity of these attacks and, moreover, has been used in a distorted manner to censor freedom of expression, especially of journalists. Emblematic cases such as that of Belén Whittingslow expose the profound shortcomings of the judicial system in providing justice and redress to victims.

Finally, **deep digital divides** persist, perpetuating inequality, especially between urban and rural areas and for indigenous communities. The lack of robust regulation of net neutrality and the misuse of personal data in the electoral sphere exacerbate citizens’ vulnerability and weaken democratic integrity. The country enacted its first comprehensive personal data protection law in November 2025. It will be important to urgently develop regulations for the implementation of the law. Unfortunately, the law does not provide for an independent supervisory authority and includes a controversial article that limits the exercise of the right of access to public information⁶.

1 TEDIC (2025). TEDIC submits three UPR reports to the UN. Available at: www.tedic.org/tedic-vuelve-a-presentar-tres-informes-ante-la-onu/ in EN: <https://www.tedic.org/en/tedic-submits-three-reports-to-the-un-once-again/>

2 TEDIC: www.tedic.org/ EN: <https://www.tedic.org/en>

3 APC: <https://www.apc.org/es>

4 Artigo19: <https://artigo19.org/>

5 Derechos Digitales: <https://www.derechosdigitales.org/>

6 TEDIC (2025). Law on personal data protection in Paraguay. Available at: <https://www.tedic.org/la-ley-sobre-la-proteccion-de-datos-personales-en-paraguay-un-logro-colectivo-basado-en-evidencia-y-participacion-plural/> y <https://www.tedic.org/en/the-law-on-the-protection-of-personal-data-in-paraguay-a-collective-achievement-based-on-evidence-and-plural-participation/>

I. RESTRICTION OF CIVIC SPACE AND FREEDOM OF ASSOCIATION: THE ANTI-NGO LAW

Law No. 7363/24, “which establishes control, transparency, and accountability for nonprofit organizations”, has raised serious concerns due to its potential to undermine fundamental freedoms and the work of civil society in Paraguay⁷.

Features and threats of the law

- **Ambiguous and Punitive Nature:** Under the pretext of promoting transparency, the law introduces disproportionate controls and registration and reporting requirements that could severely restrict the work of non-governmental organizations (NGOs).
- **Excessive Controls:** It requires all NGOs that receive public or private funds to submit semi-annual financial reports to the Ministry of Economy and Finance and to list the individuals and entities with which they work. The lack of specificity regarding what information must be reported opens the door to arbitrary interpretations.
- **Disproportionate Sanctions:** Penalties for noncompliance are severe and can lead to the forced dissolution of the organization, posing an existential threat to the sector.
- **Privacy and Security Risks:** The obligation to disclose detailed information about beneficiaries raises serious concerns, especially for organizations working in sensitive areas such as human rights.

The enactment of the law has taken place in a climate of hostility towards civil society. Numerous international actors have expressed alarm over this legislation, warning of its incompatibility with international human rights standards. Among them are UN Special Rapporteur Gina Romero, Special Rapporteur on Freedom of Expression (IACHR) Pedro Vaca, Civicus Monitor, Amnesty International, the New York Bar Association, and the Open Government Partnership.

In December 2025, thirty-three (33) Paraguayan civil society organizations filed a constitutional challenge against the law before the country’s Supreme Court⁸.

⁷ TEDIC. (2024): The year 2024 marked by the Anti-NGO law in Paraguay. Available at: <https://www.tedic.org/ley-antiong-en-paraguay/> in EN: <https://www.tedic.org/en/anti-ngo-law-in-paraguay-major-setbacks-and-concerns-for-democracy/>

⁸ CODEHUPY (2025) CODEHUPY and civil society organizations will file a constitutional challenge against the “garrote law”. Available at: <https://www.codehupy.org.py/codehupy-y-organizaciones-sociales-presentaran-accion-de-inconstitucionalidad-contra-la-ley-garrote/>

II. EXPANSION OF STATE SURVEILLANCE AND THE RIGHT TO PRIVACY

The Paraguayan State has increased its surveillance capacities without establishing adequate legal frameworks, transparent oversight mechanisms, or effective remedies, posing a serious threat to privacy and other fundamental rights.

Acquisition and Use of Surveillance Technologies

- **IMSI Catchers (“Stingrays”):** The acquisition and purchase plans for these devices, which enable the interception of mobile communications, have been documented. In 2021, the National Police responded ambiguously to a request for information from TEDIC, stating that it “could neither confirm nor deny” their use, leaving citizens in a state of vulnerability⁹.
- **Facial recognition:** The Ministry of the Interior acquired facial recognition software in 2018, which is used in downtown Asunción and in soccer stadiums. Access to information on its use has been denied citing national security reasons, prompting TEDIC to file a constitutional challenge in 2019. Law No. 7269/2024 formalized the use of this technology in sports venues¹⁰.
- **Drones:** Regulation of drones is fragmented and weak, creating risks of misuse for social control and mass surveillance, especially in the context of protests¹¹.
- **Spyware and cyber-patrolling tools:** The police have publicly stated that they use these tools to “prevent riots and acts of terrorism,” indicating systematic surveillance of legal expression and political activities without clear judicial oversight¹².

Surveillance of social protest

During peaceful demonstrations by young people (“Generation Z”) in September 2025, authorities used open-source intelligence (OSINT) systems and cyber-patrolling tools to monitor participants. The police publicly admitted this “monitoring,” which included infiltration into organizing groups. These actions, combined with the violent repression of the protests, have a chilling effect on freedoms of assembly and expression¹³.

Misappropriation of public funds

Investigations by TEDIC in 2018 and 2024 revealed that Universal Service Funds, administered by CONATEL and intended to reduce the digital divide, were misappropriated to acquire surveillance technologies, such as facial recognition cameras, instead of being invested in improving connectivity in underserved areas¹⁴.

9 TEDIC (2025) IMSI catchers in Paraguay. Available at: <https://www.tedic.org/en/imsi-catchers-in-paraguay-the-invisible-surveillance-threatening-your-right-to-protest/> and ES <https://www.tedic.org/imsi-catchers-en-paraguay-la-vigilancia-invisible-que-amenaza-tu-derecho-a-manifestarte/>

10 TEDIC (2025) Not with my face: Facial recognition in Paraguay. Available at: https://www.tedic.org/reconocimiento_facial_py/ EN <https://www.tedic.org/en/facial-recognition-asuncion/>

11 TEDIC (2025). Drones in Paraguay. Available at: <https://www.tedic.org/lanzamiento-drones-en-paraguay-que-impactos-tienen-a-nuestros-derechos/> EN <https://www.tedic.org/en/release-drones-in-paraguay-what-impact-do-they-have-on-our-rights/>

12 During the social protests in Asunción in September 2025, opposition senators denounced that the authorities monitored the social media and communications of protesters, and even requested telephone companies to provide their call and message records without a court order. These actions represent a potential violation of privacy, personal data protection, and freedom of expression and association. Available at: <https://www.abc.com.py/policiales/2025/09/30/gen-z-abogado-considera-grave-supuesto-monitoreo-policia-de-redes-sociales-y-chats/>

13 18 bis

14 16 bis

III. PERSONAL DATA PROTECTION AND CYBERSECURITY

Paraguay faces serious deficiencies in personal data protection and cybersecurity, characterized by an incomplete legal framework, the vulnerability of citizens, and the lack of institutional preparedness.

Legal framework for Data protection

- **Personal data law is approved:** The country has had comprehensive legislation on personal data protection since November 2025, after several years without this right. It is expected to be regulated within two years¹⁵.
- **Habeas Data and Fraudulent Affiliations:** The use of habeas data reveals the problem of political party affiliations without consent, resulting from the misuse of data. Research on habeas data and fraudulent affiliations shows that the Superior Court of Electoral Justice (TSJE) has acted negligently, shifting the responsibility for oversight to the parties themselves and leaving citizens defenseless¹⁶.
- **Risks of Digital Identity:** Law No. 7177/2023, which implements digital identity cards and driver's licenses, was adopted without human rights impact assessments, raising concerns about privacy and data security¹⁷.
- **Biometrics in the Voting System:** A 2019 bill to implement biometric identification in elections was ultimately rejected by the TSJE in 2023 due to logistical concerns. However, the initial proposal did not include impact assessments on voting privacy and anonymity, and the creation of large-scale biometric databases remains a latent risk¹⁸.

Cybersecurity and Human Rights Defenders

A 2024 TEDIC research¹⁹ on the cybersecurity of human rights defenders revealed an alarming situation:

- **Lack of training:** 76.2% of respondents had never received training in digital security.
- **Absence of Protocols:** 94.6% of their organizations lack protocols or records of security incidents.
- **Gender Gap:** Female defenders face technology-facilitated gender-based violence more frequently.
- **Common Threats:** The most commonly reported threats include hacking, phishing, identity theft, and disinformation.

15 TEDIC (2025). The law on personal data protection in Paraguay: A collective achievement based on evidence and pluralistic participation. Available at: <https://www.tedic.org/la-ley-sobre-la-proteccion-de-datos-personales-en-paraguay-un-lo-gro-colectivo-basado-en-evidencia-y-participacion-plural/> in EN: <https://www.tedic.org/en/the-law-on-the-protection-of-personal-data-in-paraguay-a-collective-achievement-based-on-evidence-and-plural-participation/>

16 TEDIC (2022) Habeas Data and fraudulent affiliations due to misuse of personal data in Paraguay's electoral register. (Exploratory Study) Available at: <https://www.tedic.org/habeas-data-y-afiliaciones-fraudulentas-por-uso-indebido-de-datos-personales-en-el-padron-electoral-de-paraguay-estudio-exploratorio/> EN <https://www.tedic.org/en/towards-a-new-electoral-reform-in-paraguay/> ES <https://www.tedic.org/identidad-digital-en-paraguay/>

17 TEDIC (2024) Digital Identity in Paraguay: risks and recommendations from a Human Rights Perspective. <https://www.tedic.org/en/digital-identity-in-paraguay/>

18 TEDIC (2024). Towards a New Electoral Reform in Paraguay. <https://www.tedic.org/en/towards-a-new-electoral-reform-in-paraguay/> ES <https://www.tedic.org/reforma-electoral-en-paraguay/>

19 TEDIC (2024) Cybersecurity for human rights defenders in Paraguay. See: https://www.tedic.org/ciber_defensores/ EN <https://www.tedic.org/en/research-cybersecurity-among-human-rights-defenders-in-paraguay/>

Cybersecurity cannot fall solely on individual responsibility; it requires a structural and collaborative strategy.

Cybersecurity legislative proposals

There are at least two bills and one draft bill on cybersecurity²⁰, but they lack coordination and have serious shortcomings:

- **Militarized approach:** Some proposals place cybersecurity under the authority of the Ministry of Defense, contrary to international best practices that favor civilian leadership.
- **Conceptual Confusion:** They mix issues such as cybersecurity, data protection, and cybercrime, without harmonization with existing laws.
- **Lack of a Human Rights Approach:** The proposals tend toward a security-focused and reactive approach, overlooking multisectoral participation and the protection of rights.

IV. TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE (TFGBV)

TFGBV in Paraguay is an extension of the structural violence suffered by women in physical spaces, amplified and complicated by the digital environment²¹.

Insufficient Legal Framework and Access to Justice

- **Law No. 5777/16:** Although this law introduces the concept of “cyber violence,” its focus is mainly limited to the non-consensual dissemination of intimate images. It excludes other forms of aggression such as harassment, threats, identity theft, and online sexual exploitation²².
- **Problematic legislative initiatives:** A 2023 bill on “Universal cyberbullying” to punish cyberbullying proposes prior censorship of the Internet as a preventive measure, which poses a serious risk to freedom of expression²³.
- **Barriers to justice:** Victims face revictimization, stigma, and a lack of prompt responses from the judicial system. Criminal proceedings are perceived as slow and ineffective. There are no accurate records or standardized indicators on TFGBV.

20 TEDIC (2025). Cybersecurity in Paraguay: between urgency and legislative improvisation. Available at: <https://www.tedic.org/ciberseguridad-en-paraguay-entre-la-urgencia-y-la-improvisacion-legislativa/> EN <https://www.tedic.org/en/cybersecurity-in-paraguay-between-urgency-and-legislative-improvisation/>

21 TEDIC (2025) Access to justice in the digital age: Contributions to the IACHR. <https://www.tedic.org/acceso-a-la-justicia-cidh/> EN <https://www.tedic.org/en/impunity-and-digital-gender-violence/>

22 TEDIC (2021). Gender-based violence on the Internet – Paraguay. <https://www.tedic.org/wp-content/uploads/2021/08/Violencia-Digital-TEDIC-WRO-2021-ES-v01.pdf> EN <https://www.tedic.org/wp-content/uploads/2021/08/Violencia-Digital-TE-DIC-WRO-2021-EN.pdf>

23 TEDIC (2023). It’s time for a law on digital violence against women in Paraguay. Available at: <https://www.tedic.org/es-momento-de-una-ley-sobre-violencia-digital-contra-las-mujeres-en-paraguay/> EN <https://www.tedic.org/en/its-time-for-a-law-on-digital-violence-against-women-in-paraguay/>

TFGBV against female journalists and politicians

- **Journalists²⁴:** A 2023 research on 150 female journalists identified 253 cases of digital violence, including organized attacks, hate speech, threats, doxing, and hacking. The perpetrators range from anonymous users and trolls to private actors and state authorities.
- **Politicians²⁵:** A study with 20 women politicians documented eight types of digital violence. The impact includes fear, anxiety, and self-censorship, limiting their political participation. The perpetrators range from politicians and parties to organized crime groups, acting with significant impunity.

V. FREEDOM OF EXPRESSION AND THE DIGITAL DIVIDE

Freedom of expression in Paraguay faces threats both from the misuse of legislation and from the lack of an equitable and open digital environment.

Censorship through the distorted use of the law

Researches by TEDIC and CELE have documented how Law No. 5777/16 has been used to censor critical discourse, especially by journalists. Female public officials and politicians' wives have alleged "cyber violence" to request precautionary measures that silence publications²⁶.

Absence of net neutrality²⁷

- **Weak regulation:** Net neutrality is regulated solely by an administrative resolution from CONATEL (No. 190/2009), a low-level provision that lacks enforcement mechanisms.
- **Zero-Rating Practices:** This regulatory gap facilitates practices such as zero-rating²⁸, where certain services do not consume data from the user's plan. This creates a fragmented internet, limits access to information (especially for vulnerable sectors), and promotes misinformation, as users cannot verify sources outside of "free" applications.

24 TEDIC (2023) Gender-based violence against journalists on the Internet in Paraguay. Available at: <https://www.tedic.org/wp-content/uploads/2023/10/Violencia-Genero-Periodistas-TEDIC-2023-web-2.pdf> EN <https://www.tedic.org/wp-content/uploads/2023/10/Violencia-Genero-Periodistas-TEDIC-2023-ENG-web-1.pdf>

25 TEDIC (2024) Technology-facilitated gender-based violence against women politicians in Paraguay. Available at: <https://www.tedic.org/wp-content/uploads/2024/09/Violencia-de-genero-a-mujeres-politicas-WEB-1.pdf> EN <https://www.tedic.org/wp-content/uploads/2024/09/WEB.pdf>

26 CELE (2024) Online gender-based violence and freedom of expression: a study of six cases in Paraguay. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5157887/ EN <https://www.tedic.org/wp-content/uploads/2024/05/Tergiversaciones-Ley-5777-EN-WEB.pdf>

27 TEDIC (2018), Net neutrality. <https://www.tedic.org/zero-rating-es-una-forma-de-precarizar-internet/> and Access to internet in LATAM: <https://www.tedic.org/neutralidadenlaredenamerica/> LAPIN (2021) See PT - <https://lapin.org.br/2021/08/02/zero-rating-e-desinformacao-a-relacao-entre-a-precariedade-do-acesso-a-internet-no-brasil-e-a-disseminacao-de-conteudos-enganosos/>

28 Zero-rating (also called zero rate or zero tariff) is a practice used by mobile phone operators and mobile virtual network operators to not charge their end users for data used by specific applications or for internet services through their networks, in data plans and limited tariffs. In other words, certain data is exempt from being counted against the user's contracted data allowance or from incurring additional charges for excess usage. Available in Wikipedia: <https://es.wikipedia.org/wiki/Zero-rating> EN <https://en.wikipedia.org/wiki/Zero-rating>

VI. INTERNET ACCESS AND DIGITAL EXCLUSION

Although Paraguay has made progress in connectivity, significant structural gaps persist that promote inequality and limit the full enjoyment of human rights.

Key Statistics on the Digital Divide²⁹

Indicator	Relevant information	Source and Year
Internet use	81,6% of the population	INE (2024)
Territorial gap	73,4% of urban households connected vs. 27,9% of rural households.	INE (2023)

Deliberate blackouts and misappropriation of funds for connectivity

- Researches by TEDIC have documented the precarious nature of connectivity and possible **deliberate internet blackouts** in areas of socio-environmental conflict, affecting the ability of human rights defenders to take action³⁰.
- As mentioned above, CONATEL's **Universal Service Funds**, designed to bridge the digital divide, have been diverted to the purchase of surveillance technologies such as facial recognition systems for the country's municipalities³¹.

29 TEDIC (2025) Paraguay officially presented UNESCO's RAM report on artificial intelligence. Available at: <https://www.tedic.org/paraguay-presento-oficialmente-el-informe-ram-sobre-inteligencia-artificial-de-la-unesco/> EN: <https://www.tedic.org/en/paraguay-officially-presented-unescos-ram-report-on-artificial-intelligence/>. UNESCO (2025). RAM- Paraguay: <https://unesdoc.unesco.org/ark:/48223/pf0000396524>

30 TEDIC (2023). Internet blackouts in Paraguay. <https://www.tedic.org/wp-content/uploads/2023/07/InformeApagones-de-internet-2023.pdf> and EN <https://www.tedic.org/en/internet-shutdowns-report-northern-zone-paraguay-2023/>

31 TEDIC (2025) Not with my face: Facial recognition in Paraguay. Available at: https://www.tedic.org/reconocimiento_facial_py/ EN <https://www.tedic.org/en/facial-recognition-asuncion/>

VII. SUMMARY OF KEY RECOMMENDATIONS

In order to address these issues, the Paraguayan State is urged to adopt the following measures:

1. Civic Space and Freedom of Association:

- Amend Law No. 7363/24 (“Anti-NGO Law”) to align it with international human rights standards, ensuring the autonomy of civil society.
- Refrain from using stigmatizing rhetoric or legal mechanisms to intimidate civil society organizations.

2. Privacy, Surveillance, and Personal Data:

- Adopt a legislative framework regulating the use of surveillance technologies, ensuring that all measures comply with the principles of legality, necessity, and proportionality, and require prior judicial authorization.
- Ensure the prompt entry into force of a comprehensive personal data protection law that includes the creation of an **independent supervisory authority**.
- Conduct human rights impact assessments before acquiring or implementing mass surveillance technologies such as facial recognition.

3. Technology-Facilitated Gender-Based Violence:

- Amend Law 5777/16 to include a comprehensive approach to all forms of cyber violence.
- Strengthen the technical capacities of the Judiciary and the Public Prosecutor’s Office in the areas of digital evidence and international cooperation.
- Incorporate a gender and intersectional perspective into all protection policies and mechanisms.

4. Freedom of Expression and Internet Access:

- Create a protection mechanism for journalists and human rights defenders that guarantees their safety both online and offline.
- Adopt a binding legal framework that guarantees **net neutrality** and prohibits discriminatory practices such as zero-rating.
- Refrain from disrupting internet access and ensure that Universal Service Funds are invested in infrastructure to bridge the digital divide.