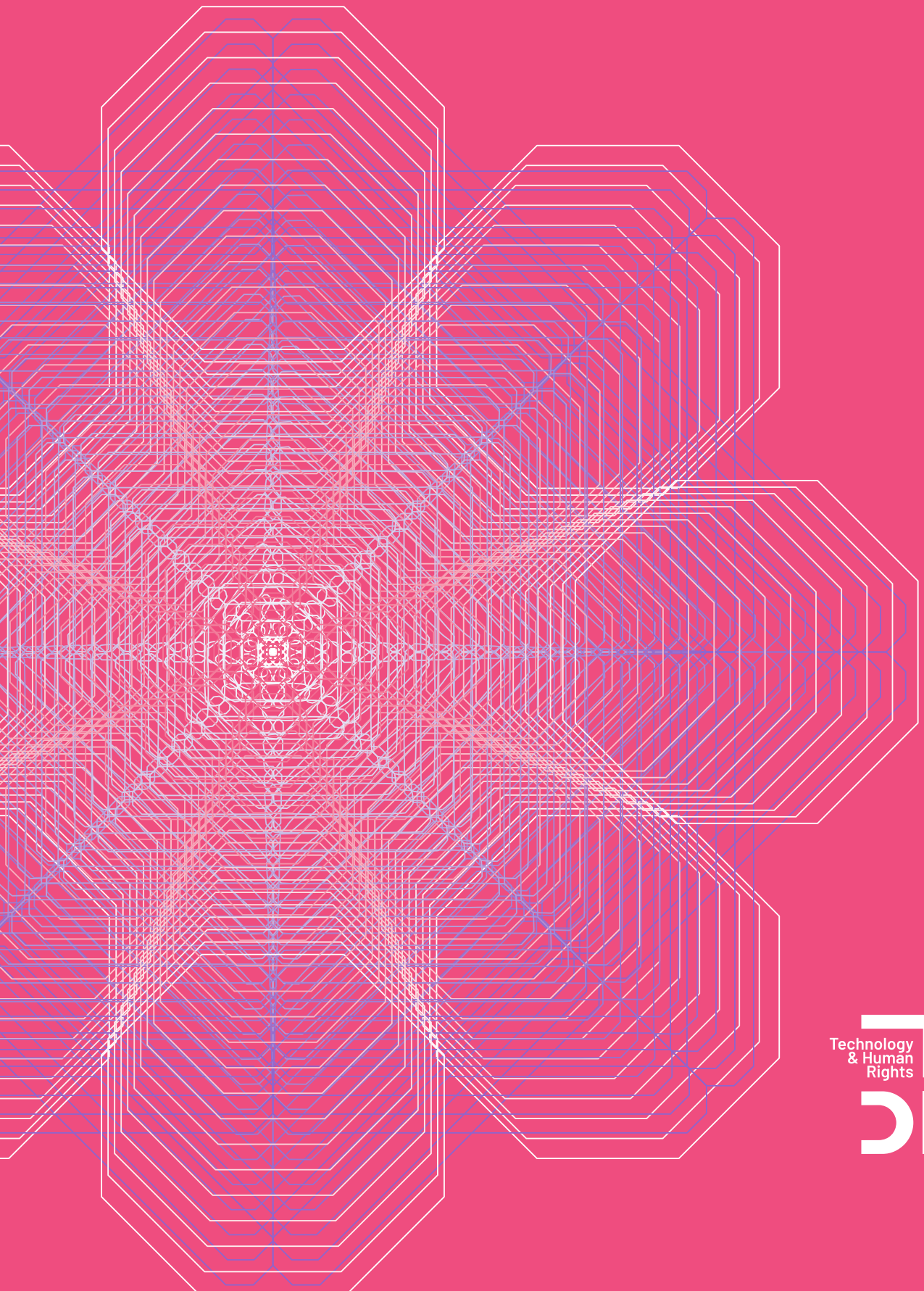
WHO HAS YOUR BACK?

Paraguay 2026



Technology & Human Rights

TEDIC

WHO HAS YOUR BACK?

Paraguay 2026

Technology & Human Rights

"Who has your back?" aims to promote transparency and best practices in the areas of privacy and data protection by companies providing Internet access in Paraguay. It is conducted annually and each new assessment is preceded by a review of the methodology, so that the results can more accurately reflect the existing legal framework, consider emerging issues and cover good practices in the areas of privacy and personal data protection.

TEDIC is a non-profit organization that defends and promotes human rights in digital environments as technology advances with a focus on gender inequalities and their intersections.

WHO HAS YOUR BACK?

Paraguay 2026

JUNE 2026

COORDINATION & CO-EDITING
Maricarmen Sequera

CO-EDITING & REVIEW
Veridiana Alimonti

AUTHOR
Marlene Samaniego

PROJECT ASSISTANT
Maricel Achucarro

COMMUNICATION
Camila Rolón

DESIGN AND LAYOUT
Horacio Oteiza

ENGLISH TRANSLATION
Alejandra González

View this research at:
https://qdtd.tedic.org

ISBN 978-99989-999-5-4

Technology & Human Rights TEDIC

TABLE OF CONTENTS

INTRODUCTION

The Who Has Your Back? project draws inspiration from the Who Has Your Back? initiative developed by the Electronic Frontier Foundation (EFF). However, the methodology applied in this study differs, as Paraguay's legal and regulatory framework presents specific characteristics that require a different approach.

The primary objective of this study is to promote transparency and encourage the adoption of best practices in privacy and personal data protection by Internet service providers (ISPs) in Paraguay. This study seeks to answer, among others, the following questions: How and to what extent do ISPs protect users' privacy? Do ISPs take measures to protect users' personal data? Do ISPs have protocols in place to govern how they respond to government requests? Do ISPs actively defend digital rights in the public sphere?

The United Nations has declared, in various reports and resolutions, that access to the Internet is fundamental to the exercise of human rights, including freedom of expression, access to information and participation in democratic life (Human Rights Council, 2016) (General Assembly, 2016). Similarly, the UN Guiding Principles on Business and Human Rights establish that companies must respect human rights and avoid adverse impacts arising from their activities (United Nations, 2011).

The main development in this edition, compared to previous ones (TEDIC, 2017, 2020, 2022, 2024), is the enactment of Law No. 7593/2025 on the Protection of Personal Data in the Republic of Paraguay (Presidency of the Republic of Paraguay, 2025a), which establishes, for the first time, a comprehensive legal framework for the protection of personal data in the country. This law constitutes "a collective achievement based on evidence and broad participation" (TEDIC, 2025), resulting from a multisectoral process led by the Personal Data Coalition, with the active participation of civil society organizations, academia and experts in digital rights.

Law No. 7593/2025 aims to provide comprehensive protection for the personal data of natural persons, in order to guarantee the full exercise of their rights and the free flow of information in accordance with the Constitution and the international treaties ratified by Paraguay. Its scope of application covers the wholly or partly automated processing of personal data, as well as non-automated processing when the data form part of a file, carried out by natural or legal persons, whether public or private.

The law also establishes criteria for its extraterritorial application in cases involving the offering of goods or services to individuals in Paraguay or the monitoring of the behaviour of individuals within the national territory. This provision is particularly relevant to service providers whose infrastructure or data processing activities involve international data flows.

The enactment of this law substantially changes the context for this research. Given the absence of a framework law, many of the criteria in previous versions focused on what were considered international best practices. In this edition, the analysis is structured around the legal provisions introduced by the law across the key pillars of personal data regulation: processing principles, legal bases, data subjects' rights, security, breach notification, the regulation's international dimension and the establishment of a competent authority.

Therefore, in this context, the assessment of business performance is no longer limited to examining voluntary commitments, but also assesses the degree of alignment with a binding regulatory framework that sets higher standards for privacy and personal data protection. Furthermore, it is necessary to carry out regular reviews of ISPs' performance and then systematize the findings, thereby safeguarding personal data protection in Paraguay's digital environment.

COMPARATIVE OVERVIEW

Comparative Overview									
ISP	Criteria								Percentage of compliance*
	Privacy and personal data protection policy	Judicial authorization	User notification	Policies for the promotion and protection of human rights	Transparency	Guidelines for requesting personal information	Accessibility	Data disclosure protocol for criminal investigations	
STARLINK	★	☆	☆	☆	☆	☆	★	☆	24%
Claro	☆	☆	☆	★	★	★	☆	★	45%
tigo	☆	☆	☆	★	★	★	★	★	48%
personal	☆	☆	☆	☆	☆	☆	☆	☆	14%

* Percentages were calculated based on the total number of criteria met by each ISP in relation to the total number of existing criteria (22 in total). Values were rounded up to the nearest whole number.

METHODOLOGY

This study focused on evaluating the main Internet service providers (ISPs) in Paraguay, which have a significant presence in the country. For this edition, the companies were selected based on their coverage and operational presence, using the market indicators published by the National Telecommunications Commission (CONATEL, 2025) as the primary reference.

Unlike previous editions, this study excludes Vox and Copaco from the companies assessed and includes Starlink as a new key player. The inclusion of Starlink (Sequera, 2024) is justified by its operational presence in the country, as well as the importance of evaluating its privacy performance in light of the technical and regulatory framework governing the provision of satellite services.

Internet service providers collect information about their users both for commercial use and to comply with legal obligations. In this regard, this study focused on a qualitative analysis of privacy policies, standard-form contracts, sustainability reports, public protocols and other documents publicly available on each company's website as of the fieldwork cutoff date specified for this study.

The analysis was conducted within the framework of the criteria established for this study, which take into account both the current regulatory framework in Paraguay, including the recently enacted Law No. 7593/2025 on the Protection of Personal Data, and international best practices for privacy protection and the processing of personal data.

NATIONAL CONTEXT

1. ACCESS AND CONNECTIVITY

Internet access in Paraguay has experienced sustained growth in recent years. Access to information and communication technologies is not only a right but also enables different forms of participation in society, the economy and politics. However, gaps in Internet access and use persist, particularly in rural areas and among vulnerable population groups.

According to the National Institute of Statistics (INE), in 2024, 81.6% of the population used the Internet. Among them, Internet use stood at 81.0% for men and 82.1% for women. Meanwhile, by area of residence, 86.2% (2,690,170) of the urban population used the Internet, compared to 73.7% (1,327,659) of the rural population (INE, 2024).

Regarding advances in connectivity indicators, it is worth noting that, according to the Paraguay National Telecommunications Plan 2021–2025 (PNT 21–25), developed by the National Telecommunications Commission (CONATEL) in October 2021, significant progress has been made in recent years. In 2023, fixed broadband Internet penetration reached 14% per 100 inhabitants, representing a 4% increase compared to 2022. Mobile broadband Internet penetration stood at 84.4% in 2023, significantly higher than the 64.5% recorded in 2022. Although no updated data is available for 2024, these figures remain highly relevant to the national context, as they reflect the evolution of connectivity in the country.

The PNT 21–25 (CONATEL, 2021) also notes that the predominant fixed broadband access technologies are currently HFC, followed by FTTX and ADSL. This analysis provides a more comprehensive understanding of network capacity and efficiency in the country and could contribute to the development of strategies and policies to improve connectivity and ensure equitable and efficient access to telecommunications services nationwide.

The expansion of connectivity also entails an increase in the volume and sensitivity of the personal data processed by service providers. The more deeply users engage with these services, the greater the demands placed on ISPs to adopt more robust data protection policies and to comply with the principles of transparency and due process.

The inclusion of satellite services such as Starlink introduces new regulatory challenges, particularly regarding international data transfers, jurisdiction and oversight by national authorities.

In the first phase, a preliminary assessment was conducted to determine an initial score for each company. It also helped identify strengths, weaknesses and areas for improvement for each of the criteria analyzed.

TEDIC then contacted the companies assessed via email to present some preliminary results, request clarifications and provide them with an opportunity to supplement information that was not publicly available. This methodological step is essential not only to ensure the rigor of the study but also to foster dialogue and ensure that the information published accurately reflects the information available at the time of publication.

Finally, the comments received were analyzed and, where warranted, taken into account in the final results and the assignment of scores.

2. REGULATORY FRAMEWORK

This study requires a brief but substantive analysis of the privacy and personal data protection laws governing Internet service users, as well as specific telecommunications regulations and other laws and regulations that directly impact the management and processing of personal data. These laws and regulations establish the obligations of service providers and the rights of users, providing the framework within which this research is situated.

2.1. International legal framework

Under the current international legal framework adopted and ratified by Paraguay, instruments such as the Universal Declaration of Human Rights (United Nations, 1948) and the American Convention on Human Rights (Presidency of the Republic of Paraguay, 1989) protect the right to privacy and the inviolability of communications. The case law of the Inter-American Court of Human Rights (IACHR) has reinforced these protections, establishing relevant precedents for States Parties, including Paraguay, regarding the protection of privacy and state surveillance, including those outlined below:

Escher v. Brazil (2009)

In this case, the Inter-American Court of Human Rights (IACHR, 2009) examined human rights violations committed during telephone interceptions conducted on members of the organizations Coana and Adecon in Paraná between May and June 1999. Although the recordings were judicially authorized, they lacked adequate legal grounds, extended beyond the permitted time limit and were leaked to the media.

The Court found Brazil responsible for violating the rights to privacy, freedom of association and judicial guarantees, ordering compensation, investigations and the publication of the ruling. The State paid US$22,000 to each victim and partially complied with the provisions, but did not hold anyone responsible due to the statute of limitations on the case. Finally, the Court closed the case, the only one in Brazil considered fully complied with.

This judgment highlights for the first time that the American Convention protects not only the content of communications but also any related information, such as the origin, duration and time of the communication. The Court made it clear in this judgment that both the content and related metadata are protected by inter-American human rights laws:

> 114. As this Court has indicated previously, even though telephone conversations are not expressly mentioned in Article 11 of the Convention, they are a form of communication included within the sphere of the protection of privacy.117 Article 11 protects conversations using telephone lines installed in private homes or in offices, whether their content is related to the private affairs of the speakers, or to their business or professional activity. Hence, Article 11 applies to telephone conversations irrespective of their content and can even include both the technical operations designed to record this content by taping it and listening to it, or any other element of the communication process; for example, the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls, aspects that can be verified without the need to record the content of the call by taping the conversation. In brief, the protection of privacy is manifested in the right that individuals other than those conversing may not illegally obtain information on the content of the telephone conversations or other aspects inherent in the communication process, such as those mentioned.

Restrepo (CAJAR) v. Colombia (2023)

The Court issued a landmark ruling against Colombia, finding the State responsible for a campaign of surveillance, harassment and persecution of members of the "José Alvear Restrepo" Lawyers' Collective (CAJAR) that lasted more than two decades (IACHR, 2023a, 2023b). These actions, which included threats and harassment, violated fundamental rights such as the right to life, personal integrity, privacy, freedom of expression and association, particularly affecting women human rights defenders and those who were forced into exile.

The decision sets a precedent as the first to hold a State responsible for violating the right to defend human rights. Furthermore, it highlighted the need for independent oversight of intelligence services, clear limits on their powers and strict standards for the handling and protection of personal data.

The Court emphasized that Colombia's legal framework did not prevent abusive surveillance practices against CAJAR and other human rights defenders, even after legal reforms. The ruling advances the protection of privacy, freedom of expression and informational self-determination under the American Convention on Human Rights, establishing key standards for intelligence activities in the region.

The Court also underscored that practices such as covert surveillance, the interception of communications and the collection of personal data constitute a serious interference with human rights. These actions require clear regulations and effective controls to prevent abuses. Citing European case law, it stressed that even the existence of laws permitting secret surveillance poses a threat to freedom of communication.

The Court reaffirmed that surveillance must be subject to prior judicial authorization, including strict limits on scope, time and method. This applies both to the collection of personal information from private companies and to the use of techniques to access non-public databases, track users online or locate electronic devices. It also covers access to sensitive metadata, such as emails, GPS locations, IP addresses and app data.

However, the Court did not clearly distinguish between targeted and mass surveillance, missing an opportunity to explicitly condemn the latter, which leaves room for ambiguous interpretations of these practices.

The Court recognized informational self-determination as an autonomous human right, guaranteed by the American Convention. This right allows individuals to decide when and how to disclose aspects of their private lives, including control over their personal data.

The Court noted that informational self-determination includes several key components: the right to know what data is collected, its source, use, retention period and possible transfer; the right to correct, update or delete inaccurate data; the right to object to its processing; and the right to data portability. Furthermore, any restriction on this right must be justified, limited in time and comply with the principles of necessity and proportionality, excluding generic justifications such as national security.

The Court concluded that Colombia violated this right by arbitrarily restricting CAJAR members' access to and control over their personal data in intelligence files. It rejected the notion that the mere fact that documents belong to intelligence agencies is sufficient to classify them as confidential, requiring that restrictions be based on their specific content (EFF, 2024).

Both rulings underscore the importance of protecting human rights, ensuring privacy protection and limiting state surveillance to prevent abuses. Paraguay[1], like many jurisdictions in Latin America, provides less protection for metadata than for content. However, in light of these cases and in accordance with the principle of conventionality, the Paraguayan State must implement measures to prevent mass and disproportionate surveillance, guarantee the protection of personal data and provide judicial safeguards so that individuals, especially human rights defenders, can carry out their work without fear of reprisals or arbitrary interference.

2.2. National legal framework

The National Constitution recognizes the right to privacy (Article 33), the right to inviolability of documentary heritage and personal information (Article 36) and the protection of habeas data (Article 135), which grants individuals the right to access, modify or delete information concerning them that is recorded in public or private databases.

The enactment of Law No. 7593/2025 marks a new phase in Paraguay's legal system by establishing a comprehensive framework for the protection of personal data. The law defines fundamental concepts such as personal data, sensitive data, processing, data controller and data processor, consent and anonymization.

The law structures the processing of personal data around a set of general principles that must guide all operations, including the recording, organization, access, retention, disclosure, transfer or deletion of data. Among these principles are: accuracy, requiring that data be truthful and up-to-date; confidentiality, mandating discretion to prevent improper disclosure; purpose limitation, which restricts processing to specific, explicit and legitimate purposes; data minimization or proportionality, which requires processing only relevant and non-excessive data; limitation of retention periods, establishing that data must not be retained longer than necessary; fairness and transparency, which require that data be processed lawfully and that clear information be provided to the data subject; security, which mandates the adoption of technical and organizational measures to ensure integrity and confidentiality; and demonstrable accountability, which requires the data controller to adopt and be able to demonstrate compliance measures. These principles are particularly relevant when evaluating ISPs' privacy policies, as they translate into obligations regarding information provision, limitations on use, technical protection and internal governance.

The law also establishes legal grounds for processing, including the data subject's free, informed and unambiguous consent; compliance with legal obligations; the performance of contracts, and the exercise of public authority.

The law further consolidates a set of data subject rights that must be implemented by data controllers and processors to assess the practical effectiveness of corporate policies. Among these rights, the law regulates: the right to information regarding processing, the right of access, the right to rectification, the right to object, the right to erasure, the right to data portability and safeguards related to automated individual decision-making, including the right to request a review. The law sets forth minimum information requirements at the time of data collection, such as data categories, the identity and contact

1 In Paraguay, the principle of conventionality has significant implications because the country has been a party to the ACHR since 1989 and has accepted the jurisdiction of the Inter-American Court of Human Rights. The country has been found responsible by the Inter-American Court in several cases, such as that of the Yakye Axa Indigenous Community, as well as others concerning violations of the rights of Indigenous communities and labour rights. These judgments have led to legal reforms and public policies aimed at aligning Paraguay's legal framework with international standards. Full version of the judgment: https://www.corteidh.or.cr/docs/casos/articulos/seriec_125_ing.pdf

information of the data controller, the purposes, legal basis, transfers, channels for exercising rights and retention criteria. It also establishes procedural rules on how requests must be handled, including obligations to respond and maintain records of requests and denials. This legal framework requires ISPs to have clear and effective channels, as well as reasonable and verifiable timeframes and responses, and serves as a direct foundation for the practical component of this study, which includes requests to exercise data subject rights.

With regard to security, the law establishes the adoption of appropriate measures and the reporting of security incidents to the supervisory authority and, where applicable, to data subjects. It also provides for the appointment of a data protection officer and the conduct of impact assessments in cases where data processing poses certain significant risks.

Regarding the international transfer of personal data, it provides the relevant regulation to ensure adequate levels of protection and compliance with certain conditions. Finally, it mandates the creation of the National Agency for the Protection of Personal Data as the supervisory authority and assigns it functions of oversight, regulatory functions and control over the exercise of sanctioning powers.

The existence of this comprehensive regulatory framework redefines the minimum standard requirements for Internet service providers in Paraguay and serves as the foundation for this edition's evaluation.

Law No. 6534/2020 on the Protection of Personal Credit Data (Presidency of the Republic of Paraguay, 2020). This law, which repeals the previous Law No. 1682/2001 and its amendments[2], establishes a new framework for the protection of personal data and information in Paraguay, placing greater emphasis on matters relating to the credit information of all individuals, regardless of their nationality, residence or domicile, held by banks, financial institutions and credit bureaus. Although this law is sector-specific, it provides relevant definitions in this area, such as those for personal data and sensitive personal data, and complements other laws and provisions within the national regulatory framework.

Within the aforementioned regulatory context, it is important to highlight Resolution No. 3/2023 of the Central Bank of Paraguay (Central Bank of Paraguay, 2023) and Resolution No. 1502/2022 of the Consumer Protection Secretariat, which regulate and supplement the Law on the Protection of Personal Credit Data in their capacity as enforcement authorities. These regulations not only define the procedures applicable to the entities regulated by the law but also the mechanisms for guaranteeing the rights of data subjects. Their importance lies in the fact that ISPs, by including creditworthiness verification in their Internet service contracts, must comply with the standards established by current legislation on data processing, taking into account the nature of these contracts.

Furthermore, in accordance with the aforementioned constitutional provisions, it is worth noting Law 642/95 on Telecommunications (Presidency of the Republic of Paraguay, 1995), which also guarantees the inviolability of the secrecy of correspondence and documentary heritage, except by court order (Article 89). This provision applies to both telecommunications personnel and to any person or user aware of the existence or content of such communications. Furthermore, the law specifies that inviolability entails a prohibition against opening, removing, interfering with, altering the text, diverting the course of, publishing, using, attempting to ascertain or enabling a third party to become aware of the existence or content of communications entrusted to service providers, as well as facilitating actions that may lead to the commission of such acts (Article 90).

2 This law repealed Law No. 1682/2001 and its amendments (Law No. 1969/2002 and Law No. 5543/2015), which provided partial regulation on private information, although with limitations. As a result, the repeal left a gap in the current regulatory framework.

Similarly, we must consider Law No. 4868/2013 on Electronic Commerce (Presidency of the Republic of Paraguay, 2013); and its complementary provisions, as well as Law No. 6822/2021 on Trust Services for Electronic Transactions, Electronic Documents and Electronically Transmittable Documents (Presidency of the Republic of Paraguay, 2021b) and its complementary provisions. According to Law No. 6738/2021, which regulates telework in employment relationships (Presidency of the Republic of Paraguay, 2021a), these regulations have a limited scope and do not comprehensively address data protection in the country.

Article 9 of the Electronic Commerce Law establishes that ISPs must comply with certain additional obligations, in addition to the existing regulations on Internet Access Services and Data Transmission established by the Competent Authority. These obligations include providing their customers with ongoing, easy, direct and free information about various technical tools that enhance information security, such as protection against computer viruses and spyware, and the blocking of unsolicited emails. They must also provide information about the tools available to filter and restrict access to unwanted online content and services or those harmful to children and adolescents. ISPs may fulfill this disclosure obligation by including the required information on their main website.

Additionally, in Article 10, the same law establishes a duty of traffic data retention on the part of Intermediation Service Providers (internet access) and Data Hosting Service Providers, who must store the connection and traffic data generated during the provision of their services for a minimum period of six months. This obligation has the sole purpose of allowing the location of the terminal equipment used by the user to transmit information, while hosting providers only need to retain the data essential to identify the origin of the hosted content and the moment the service began. The law expressly prohibits using this data for purposes other than those legally permitted, and requires the adoption of appropriate security measures to prevent its loss, alteration, or unauthorized access. Failure to comply is considered a very serious infraction (Art. 36), punishable by fines of up to 1,000 minimum daily wages and, in cases of repeat offenses, by blocking the infringing party's access to its services for up to two years.

Similarly, Regulatory Decree No. 1165/14 of the Electronic Commerce Law, in Article 11, establishes the Duty to Inform and Data Protection, stating that remote providers of goods and services by electronic means are required to inform consumers or users about the purpose and processing of their personal data, in accordance with applicable legislation. In addition, they must disclose who will receive the data provided and who will be responsible for the safekeeping or storage of the information supplied. Furthermore, they are required to use secure systems to prevent the loss, alteration and unauthorized access by third parties to the data provided by the consumer or user.

Additionally, there are fragmented regulations on the proactive protection of personal data; for example, there is MITIC Resolution No. 733/2019 established an information security governance model to strengthen cybersecurity and risk management in the public sector.

In addition, regulations such as Decree No. 8709/2018, which governs the Information Exchange System (SII), include key principles such as purpose limitation, data minimization and ARCO rights (access, restriction, cancellation and objection). This system handles both public and private data, distinguishing itself from open data, which covers only public government information.

On the other hand, Decree No. 4845/2021, which implements Law No. 6562/2020 on reducing paper use in public administration, establishes provisions to ensure the traceability and protection of personal data, allowing access to it only for specific procedures and under the supervision of responsible officials. Although these regulations provide useful guidelines, they do not constitute a comprehensive framework for data protection in the country.

With regard to the criminal procedural framework, Article 200 of the Code of Criminal Procedure establishes that the interception of communications requires a well-founded order from a judge, regardless of the technical means used to obtain them. The results of the interception must be delivered solely to the judge who ordered it, who may request a written transcript of the recording and order the destruction of the entire recording or those parts unrelated to the proceedings, after the Public Prosecutor's Office, the defendant and the defendant's counsel have had access to them. The same body of law, in Article 228, grants the judge and the Public Prosecutor's Office the authority to request reports from public or private individuals or entities. These reports may be requested verbally or in writing, specifying the proceedings, the name of the defendant, the location for delivery of the report, the deadline for submission and the consequences of noncompliance.

These provisions underscore the exceptional nature of the interception of communications and the protection afforded to communications against disclosure of their content, in line with international and constitutional provisions that guarantee a rights-based approach in criminal law. Although not binding, recent case law also highlights the importance of a court order as a requirement for the lawful interception of communications, thereby safeguarding the constitutional guarantee of the inviolability of private communications[3].

It is also worth noting that contracts for the purchase of Internet services fall under the category of consumer contracts and are therefore protected by Law No. 1334/1998 on the Protection of Consumers and Users, as amended. This legislation protects consumers from clauses unilaterally established by the provider, which the consumer cannot modify. In this context, this legislation is relevant when evaluating how ISPs protect users' rights and considering aspects such as transparency in commercial practices, the resolution of complaints or disputes and the right of access to information.

Regarding the retention of traffic data, Law No. 7,549/2025, titled "Establishing the mandatory retention of traffic data to combat pornography involving children and adolescents and other punishable offenses," was enacted in 2025. The law establishes the obligation to retain internet service traffic data and identify users, as a tool for judicial investigations of punishable offenses related to child and adolescent pornography and other related crimes. The core of the law is found in Article 6, which requires internet service providers to retain users' traffic and connection data for a period of twelve months, including the IP address, the identity of the service holder, the date and time of connection and disconnection, and the location tag, expressly clarifying that these records do not include the content of communications but only the technical data necessary to identify users. Article 10 further reinforces that the law does not, under any circumstances, authorize mass surveillance or access to the content of users' messages.

Additionally, there is CONATEL Resolution No. 2583/2024 (CONATEL, 2024), which mandates that all licensees of Internet access and data transmission services retain connection logs. This resolution aims to record data traffic, such as IP addresses (date and time of assignment and release of the address) and, in the case of NAT (Network Address Translation), the corresponding mapping between private and public addresses, as well as mandating their storage for a minimum period of 6 months. Severe sanctions

3 Supreme Court of Justice, Criminal Chamber, Judgment No. 777, November 30, 2022, opinion of Justice Manuel Ramírez Candia.

will be imposed if the ISP fails to comply. However, the resolution does not specify which authorities are empowered to request and process this data, nor does it outline the necessary legal procedures, such as obtaining a court order to ensure respect for the principle of due process. This regulatory gap raises concerns about potential violations of privacy rights and the protection of personal data.

Understanding this context is essential for an adequate assessment of the performance of telecommunications companies in Paraguay and for designing strategies to strengthen the protection of users' rights, taking into account the interplay between legislation, social participation and the specific regulations governing these companies' handling of privacy and data protection.

EVALUATION CRITERIA

In this study, the evaluation consists of eight criteria, each with corresponding parameters that allow for an analysis of the extent to which companies comply with or fail to comply with each criterion. The criteria include: privacy and personal data protection policy, judicial authorization, user notification, policies for the promotion and defense of human rights, transparency, guidelines for requesting personal information, accessibility and data disclosure protocol for criminal investigations.

For this evaluation, service agreements, sustainability reports and other documents available on the companies' websites as of March 30, 2026, were reviewed. We also searched for news stories published in the press and specialized media and reviewed previous editions of the "Who has your back" reports (TEDIC, 2017, 2020, 2022, 2024) to verify updates and qualitative progress and conduct a final comparison.

In the first stage, a preliminary assessment was conducted to determine an initial score for each of the companies analyzed in this study and to identify the aspects of each criterion where improvements could be made to achieve a higher score. This process lasted three months and concluded on April 30, 2026.

Following the preliminary evaluation, TEDIC contacted the companies to request a meeting to explain the study's scope and present the preliminary results from the 2025 analysis, along with a comparison over time with previous editions. The goal of this meeting was for the companies to provide accurate information about their efforts to protect user privacy, as well as to supplement publicly available information or even clarify any ambiguities that might arise from it.

All companies were contacted via email. This first step is considered essential for understanding the company's perspective and providing an opportunity to clarify any questions regarding its privacy policies.

Below, we outline each of the eight criteria used to evaluate the companies.

1. PRIVACY AND PERSONAL DATA PROTECTION POLICY

The ISP has a privacy and personal data protection policy written in clear language free of technical jargon. It informs users about the collection, use, storage and processing of their personal data. In particular, this policy should be viewed as an opportunity to clearly inform users about their rights rather than as a mere legal formality. The ISP also has policies regarding requests from government authorities. These policies describe the legal procedure for disclosing user data in the context of a criminal investigation pursuant to an order issued by a competent judge.

In this regard, both Article 33 of the Constitution of the Republic—on the privacy of individuals—and international treaties protect the right to privacy as one of the pillars of modern democracies. Likewise, international human rights organizations have noted that companies must establish and implement terms of service that are transparent, clear and accessible, as well as adhere to international human rights standards and principles; including the conditions under which interference with users' right to privacy may occur (IACHR, 2013). It is essential for ISPs to have policies in place that comply with these protocols when providing information and personal data to the authorities.

Furthermore, metadata forms part of communications and is considered inviolable, as established in Article 36 of the National Constitution.

> It may not be examined, reproduced, intercepted or seized except by court order for cases specifically provided for by law.

Companies must store users' metadata for a minimum of 6 months, in accordance with Article 10 of the Electronic Commerce Law No. 4868/2013 and CONATEL Resolution No. 2583/2024. In this context, it is essential that ISPs describe and disclose what personal information is being retained, as well as the measures taken to safeguard such data against potential attacks or risks that could affect it.

In a contentious case (IACHR, 2009) in which Brazil was found liable for the illegal use of wiretaps in a criminal proceeding, the Inter-American Court noted that the right to privacy protects both the content of electronic communications and other data inherent to the technical process of communication, such as metadata or traffic data.

In the CAJAR v. Colombia case (IACHR, 2023b), the judgment concluded that Colombia had violated the fundamental rights of the lawyers' collective, such as privacy, freedom of expression and the right to defend human rights. It also recognized informational self-determination as an autonomous human right, emphasizing that individuals have control over who accesses and uses their personal data. It also stressed that invasive surveillance and access to sensitive metadata, such as location, IP addresses and private communications, require strict judicial authorization to prevent abuses and ensure the proportionality of these measures. The Court condemned the expansive surveillance techniques used by Colombia, which include the indiscriminate collection of personal information and access to non-public databases. Furthermore, it highlighted the importance of clear standards for the collection and processing of metadata, establishing that such data contains sensitive information that can reveal individuals' habits, relationships and movements. Like the Escher case, this national precedent places such data under the protection of the constitution and human rights.

The institution responsible for ensuring compliance with the Electronic Commerce Law is the Ministry of Industry and Commerce, which is tasked with coordinating inspections and oversight of the various ISPs. It is also required to impose sanctions for violations not specifically provided for in the Consumer Protection Law but established in the Electronic Commerce Law.

In addition to analyzing how information is presented in contracts or other documents, this research also seeks to evaluate the publication of specific protocols governing the disclosure of personal data to state authorities. These protocols must clearly define the terms and conditions for accessing personal data in the context of investigations or similar proceedings. The existence of clear and publicly available protocols, such as those adopted by various technology companies, is a key indicator of a company's commitment to the privacy and protection of its users' data. This aspect will be specifically addressed in criterion 6 of this investigation.

In this first criterion, therefore, given that it concerns an area of legal controversy, the issue is examined through several subcriteria that seek to distinguish between different levels of protection, clarity and commitment regarding access to data for investigations. This criterion aims to reflect the company's commitment to transparency with respect to competent authorities, current regulatory disputes and the limitations established by law (particularly regarding which types of investigations may be exempt from the requirement of a court order to access registration data), as well as the commitments expressed in its policies on location data, connection logs and the publication of protocols for the disclosure of data in judicial investigations.

Finally, in this edition, within the framework of this criterion, we also consider whether companies comply with the established provisions regarding the reporting of risks or personal data breaches (La Política Online, 2024). We will assess whether they have mitigation measures in place and protocols for notifying authorities in the event of security breaches that compromise the personal information of service users.

2. JUDICIAL AUTHORIZATION

Surveillance without the consent of the affected individual carries the risk of abuse by the authorities; therefore, authorization from a competent judge is essential. To request personal information, authorization from a competent judge is required, as stipulated by criminal law and the Constitution of the Republic of Paraguay. The interception of individuals' private communications is considered an exceptional measure and is subject to a nullity sanction in court proceedings. This criterion involves verifying whether the ISP has policies in place that comply with the protocols for providing information to judicial authorities. Specifically, this includes details of the criminal case file, the case number, the individual's personal information, the criminal offense with which the person under investigation is charged, the legal justification and the signature of the judge presiding over the case.

The judiciary, in both individual and class-action lawsuits, is an important space for the defense and consolidation of users' rights against abuses and illegal actions. With this in mind, we have sought to assess the stance of companies in lawsuits concerning privacy and data protection.

Article 36 of the National Constitution, regarding the inviolability of communications, requires state authorities to request information from ISPs only through a duly justified court order.

Surveillance without consent carries the risk of abuse by authorities; therefore, authorization from a competent judge is essential. To request personal information, authorization from a competent judge is required, as stipulated by criminal law and the Constitution of the Republic of Paraguay. The following table explains the procedure for accessing information in compliance with due process standards, as well as the relevant provisions of the Paraguayan Code of Criminal Procedure:

3. USER NOTIFICATION

The ISP must have a policy for notifying users affected by government surveillance measures as soon as permitted by law. It must demonstrate that it has challenged legal or regulatory obstacles to carrying out such notification and publicly state, in an accessible manner, that it has advocated for user notification mechanisms before Congress or other regulatory bodies. When users are notified that their personal data or Internet connection records have been requested by administrative or judicial authorities, they are provided with robust safeguards against abuses and irregularities.

In light of the constitutional principle of due process, many laws establish the duty to notify those affected of measures that impact their rights. In this line, Article 303 of the Code of Criminal Procedure provides, in accordance with Articles 75 and 151 of the same legal body, the obligation to notify individuals when the Public Prosecutor's Office has charged them with an alleged criminal offense.

In the context of data requests, ISPs play a crucial role in protecting the procedural safeguards of affected users. This is because, by notifying them of such requests, the companies enable users to challenge illegal requests in the first instance. These include both unfounded court orders and requests from administrative authorities that lack jurisdiction or sufficient grounds.

Without notification, users are dependent on the companies themselves to challenge requests they consider abusive. If notified by the companies, users have the opportunity to defend themselves against potential violations of their privacy. This right to notification for individuals affected by surveillance measures has been recognized by digital rights experts and was enshrined in the Necessary and Proportionate Principles, which state the following:

> It is impossible for a person to effectively challenge a government's interference with his or her privacy without knowing whether he or she has been a victim in the first place. More generally, the absence of transparency concerning the operation of laws governing covert surveillance can prevent meaningful democratic scrutiny of those laws ("Necessary and Proportionate". International Principles on the application of Human Rights to communications surveillance. 2014)

Furthermore, the United Nations Special Rapporteur on Human Rights expressed the following opinion on the matter:

> Individuals 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. (United Nations, 2013).

According to the Special Rapporteurship for Freedom of Expression of the IACHR (IACHR, 2025), when there are no notification systems in place for surveillance operations, the right to an effective remedy becomes illusory. This is because individuals cannot challenge actions of which they are unaware. In light of this, it maintains that States must establish systems to inform affected individuals when such notification no longer undermines the legitimate purpose of the surveillance measure, and has specifically recommended the creation of notification systems regarding the surveillance of individuals.

The UN Special Rapporteurship on human rights has emphasized that notification may not be provided immediately if it could jeopardize the success of an investigation. However, it should at least be provided when the investigation is no longer at risk, there is no risk of flight or destruction of evidence, and being informed does not pose an imminent risk to the life or physical integrity of any person. However, in Paraguay, the aforementioned current regulations stipulate that, upon receiving information about an alleged criminal act and in exceptional cases, judicial authorization may be requested to intercept communications (Presidency of the Republic of Paraguay, 1998a); nevertheless, there is no obligation to notify the person under investigation during this initial stage, except when formal charges are filed and the alleged perpetrator is identified.

In accordance with international human rights recommendations, ISPs have a responsibility to act in good faith to safeguard the privacy of their users. This includes notifying them of any interception of their communications, provided that such notification does not compromise the objectives of the criminal investigation. This practice also enables individuals to exercise their right to seek redress should their rights have been unduly infringed. In cases where the company's notification policy cannot be implemented, the ISP must challenge legal obstacles to notifying affected users in court, provided that doing so no longer undermines the purpose of the surveillance measure. Another approach would be to advocate for legislative or regulatory changes to implement legal notification mechanisms.

In the context of requests for personal data, Internet service providers play an essential role in protecting procedural safeguards of affected users. In other words, notification by the company allows users to challenge illegal requests: both unfounded court orders and requests from administrative authorities lacking jurisdiction or justification. In the current situation, users depend on the challenges filed by the companies themselves against requests they consider abusive. If users are notified, they gain the ability to defend themselves as soon as possible against potential violations of their privacy. Furthermore, the notification guarantee is consistent with the right to information for data subjects established in Article 27 of Law No. 7593/2025.

With this in mind, it is important to promote the practice of notifying users through the "Who Has Your Back?" (WHYB) project. In cases where data requests are not accompanied by a confidentiality obligation, notification is permitted under Paraguayan law (given the absence of any legal provision to the contrary). The option to notify users may be necessary not only in cases of data requests in civil proceedings but also in relation to requests made by other government agencies, such as the Ministry of Finance or CONATEL. Notifying users strengthens their ability to legally challenge the inclusion of evidence that is irrelevant or unrelated to the facts of the case.

In this edition, this category is once again classified as a "bonus," because notification is neither a legal obligation imposed on companies nor a widespread practice in Paraguay. It is a measure viewed as innovative and, to some extent, costly, as it requires staff dedicated to handling notifications . For these reasons, its adoption would demonstrate a special commitment to advancing the protection of users' rights. Notifying the user at the earliest legally possible opportunity, and preferably before the data is disclosed, supports the principles of legal defense and fosters a culture of privacy protection.

4. POLICIES FOR THE PROMOTION AND DEFENSE OF HUMAN RIGHTS

Public commitments and public positions on policies and national legislation affecting technology, from a human rights perspective, are essential for respecting and protecting users' human rights and for building trust in the Internet ecosystem.

This criterion assesses whether the ISP has a public institutional position in which it has acknowledged its responsibilities to respect and protect human rights, including the right to privacy. To this end, the assessment examines whether there is any statement of policy that meets the characteristics outlined in Principle 16 of the Guiding Principles on Business and Human Rights (United Nations, 2011), namely:

Policy Commitment 16. As the basis for embedding their responsibility to respect human rights, business enterprises should express their commitment to meet this responsibility through a statement of policy that:

a. Is approved at the most senior level of the business enterprise;

b. Is informed by relevant internal and/or external expertise;

c. Stipulates the enterprise's human rights expectations of personnel, business partners and other parties directly linked to its operations, products or services;

d. Is publicly available and communicated internally and externally to all personnel, business partners and other relevant parties;

e. Is reflected in operational policies and procedures necessary to embed it throughout the business enterprise.

To be considered, a statement of policy must be public and clearly reflect the company's commitment to respecting human rights in the context of its business activities.

This criterion assesses whether the ISP has participated, either individually or collectively, in public processes of legislative advocacy or before regulatory bodies, with the aim of defending the right to privacy. It also examines whether the ISP has taken legal action to defend the privacy of its users.

The assessment also evaluates whether the company participates in any sectoral or multisectoral mechanisms for the promotion, respect and protection of human rights within the scope of its corporate responsibilities, such as the Global Network Initiative[4] or the Telecommunications Industry Dialogue[5].

Furthermore, consideration is given to whether the ISP has policies for participating in local and international discussions on the Internet ecosystem, including the Internet Governance Forum (IGF), where shared principles, standards, rules, decision-making processes and programs that shape the evolution and use of the Internet are openly discussed.

4 Global Network Initiative https://globalnetworkinitiative.org

5 Telecommunications Industry Dialogue www.telecomindustrydialogue.org

5. TRANSPARENCY

Principle 21 of the United Nations Guiding Principles on Business and Human Rights requires companies to adopt best practices regarding transparency from a human rights perspective.

Transparency reports in the ICT sector regarding their impact on users' privacy have become more frequent in recent years[6]. The publication of a transparency report on requests for access to data by security and law enforcement authorities should provide sufficient information to assess the content and scope of surveillance measures by those authorities.

Transparency reports are statements issued by companies that contain a variety of statistics related to data requests. Internet companies around the world have adopted the practice of publishing transparency reports to provide information on how and when they cooperate with governments, generally because they are required by law to disclose information that may be used as evidence in civil and criminal cases. This is already an established best practice among content companies such as Google, Facebook, X (formerly Twitter) and Microsoft, as well as providers such as Vodafone, Verizon and Telefónica.

This criterion evaluates the publication of statistics regarding how many requests for information have been received and complied with, as well as the inclusion of details on the type of requests, the requesting institutions and the authorities' rationale and justification.

6. GUIDELINES FOR REQUESTING PERSONAL INFORMATION

The ISP has guidelines, procedures or protocols for law enforcement agencies and other government bodies that explain how they should request customers' personal information and the conditions under which such personal information may be disclosed.

This criterion differs from the publication of transparency reports, as the latter focus on presenting statistical data on requests for information received and responded. In contrast, the guidelines analyzed seek to evaluate how each company defines the procedures that police or investigative agencies must follow to request information and what specific requirements they must meet during that process. It also examines whether the company, when establishing its rules for local authorities, takes the national context into account or adopts predefined guidelines from abroad. In the latter case, it verifies whether such procedures are stricter and better protect the privacy of its users.

Several regional analyses, such as the Brazilian project "Quem Defende Seus Dados?" (InternetLab, 2025), show that the most advanced practices regarding data requests by authorities are concentrated among a small number of companies that have developed comprehensive public policies alongside robust legal review processes. Among these are global companies, such as Google and Meta, which have policies regarding government authorities, legal compliance criteria and adequate mechanisms for challenging excessive requests.

6 The Implementation Guide for the ICT (Information and Communication Technologies) Sector developed by the European Commission; the Implementation Guide for the Global Network Initiative; and the report "Who Has Your Back?" developed by the Electronic Frontier Foundation.

As for telecommunications companies, for example, Telefónica has developed global policy documents based on a review of legality, proportionality and the vetting of requests. However, the report has revealed that in Latin America, most Internet Service Providers have a low level of compliance, characterized by a lack of publicly available policies with a sufficient level of sophistication, which demonstrates a considerable gap compared to global standards.

7. ACCESIBILITY

The accessibility of information available on the web, regardless of users' disabilities or functional diversity, is essential to strengthening the commitment to transparency and ensuring respect for human rights. Article 9 of the Convention on the Rights of Persons with Disabilities (United Nations, 2006) recognizes access to information and communication technologies, including the web, as a fundamental human right.

Web accessibility involves making content accessible through a design and infrastructure that works for all users, regardless of hardware, software, language, location or cognitive or sensory abilities. This removes the barriers to communication and interaction that many people face on a daily basis and helps make digital spaces more inclusive for a diverse range of users.

Ensuring that ISPs in Paraguay provide accessible data is part of expanding their commitment to transparency and respecting human rights. Designing accessible websites and tools is crucial for Internet service providers, as it enables more people to use and learn about their products and services effectively and satisfactorily. Companies must also promote the participation of people with disabilities in the provision of ICT services, ensuring their right to full civic and social participation.

For this criterion, the official websites of Internet service providers are evaluated using the Web Accessibility Guidelines of the Web Accessibility Initiative (WAI, n.d.), part of the W3C (World Wide Web Consortium).

8. DATA DISCLOSURE PROTOCOL FOR CRIMINAL INVESTIGATIONS

Does the company commit to following the interpretation of the law that provides the greatest protection of the right to privacy when state authorities request personal data, and does it have specific policies in place for such cases?

The provision of personal data in the context of criminal investigations is one of the main points of contention between investigative authorities and those defending the right to privacy. This criterion is of particular importance in this edition due to the recent entry into force of Law No. 7593/2025 on the Protection of Personal Data (Presidency of the Republic of Paraguay, 2025a), which establishes the principles of legality, purpose limitation, proportionality, data minimization and demonstrable accountability, all of which apply to any processing and disclosure of personal data.

The new law stipulates that the requirements of lawfulness and the principles of data processing must be respected when disclosing data to third parties, including public authorities. Therefore, Internet service providers must not only verify the formal jurisdiction of the requesting authority but also assess whether the disclosure of the data is compatible with fundamental rights.

There is significant tension within Paraguay's legal framework. Article 36 of the National Constitution protects the right to communications, establishing that they may only be examined or intercepted by order of a judge, and only under the circumstances prescribed by law. Similarly, Article 200 of the Code of Criminal Procedure establishes that communications may be intercepted only pursuant to a judicial order and that such interception is exceptional (Presidency of the Republic of Paraguay, 1998a).

On the other hand, Article 228 of the same legal framework authorizes judges and the Public Prosecutor's Office to order public or private entities to submit reports in the context of criminal proceedings, a provision that has been used to request logs or connection records without a specific court order and has sparked a legal debate regarding the scope of such powers when dealing with information subject to the right to privacy.

Furthermore, CONATEL Board Resolution No. 2583/2024 imposes obligations on telecommunications service providers regarding the retention and technical availability of certain data. However, data retention does not imply the authority to disclose such data without any restrictions in response to any request from the State. Retention and access are two distinct legal concepts that must be analyzed within the framework of constitutional guarantees and the personal data protection law (CONATEL, 2024).

Similarly, Decree No. 1165/14 (Presidency of the Republic of Paraguay, 2014) establishes that providers must report the purpose of data processing, identify the recipient and use secure means to safeguard such data. These obligations reinforce the company's duty to act responsibly regarding information and its disclosure.

The Inter-American Court of Human Rights, in the cases of Escher et al. v. Brazil (IACHR, 2009) and Asociación Civil CAJAR v. Colombia (IACHR, 2023b), has established that both the content of communications and metadata may contain sensitive information; therefore, any form of interference must comply with the principles of legality, necessity and proportionality, in addition to being subject to strict safeguards.

Within this regulatory, constitutional, criminal procedural, sector-specific, and now data protection framework, ISPs play a decisive role as intermediaries in safeguarding rights. The way they interpret their obligations in response to requests from prosecutors or court authorities directly impacts the effective protection of users' privacy.

This criterion assesses whether the company adopts the most protective interpretation possible within the current legal framework and whether it has internal and public guidelines that structure such a response, especially in light of Law No. 7593/2025.

The existence of structured, clear and publicly accessible protocols demonstrates the company's institutional commitment to due process and to the protection of privacy in the context of criminal investigations.

REPORT FOR EACH ISP

CRITERION 1. Privacy and personal data protection policy

Does the evaluated ISP provide clear and comprehensive information about the collection, use, storage, processing and protection of the user's personal data? Does it clearly specify what information about the user and their communications is collected and stored, as well as the duration for which such data is stored?

In this category, the ISP's publicly available data protection and privacy policies and notices are evaluated. Additionally, the processing of personal data obtained by the ISP when providing telecommunication services to the user is also assessed, which is not limited to the data voluntarily provided by the user when contracting the service.

Evaluation criteria

I. Information on data collection

- a. The company provides clear and comprehensive information on:
- b. what personal data is collected;
- c. in what situations the collection occurs;
- d. whether publicly available data may be collected;
- e. a list in the privacy policy or notice that identifies, by name, the third parties that provide data to the company (including public data providers); and
- f. whether there is an assessment of such third parties' legal compliance regarding personal data protection.

II. Information on processing purposes

The company provides clear and comprehensive information on:

- a. the purpose of the company's processing of personal data; and
- b. the type or manner in which such processing is carried out.

III. Information on storage, security and sharing

The company provides clear and comprehensive information on the storage, security and sharing of personal data, including:

- a. how long and where the data is stored;
- b. under what circumstances the data is deleted;
- c. whether the data may be retained and under what conditions;

d. what administrative and technical security practices are implemented, including the existence of cybersecurity or information technology (IT) policies that provide protections against malware, ransomware, worms and other types of threats;

e. whether there are access controls for personal data, taking into account the different categories of staff;

f. with which third parties the company shares personal data once it has been collected;

g. for what purposes such sharing takes place, including the use of software, digital platforms, networks or cloud services for internal purposes; and

h. under what circumstances personal data may be transferred internationally.

IV. Information on rights

a. The company informs users of their rights regarding personal data protection;

b. the company clearly explains the available means (e.g., emails, forms or web portals) for exercising those rights.

V. Responses to rights requests

a. The company provides clear and comprehensive information regarding the retention of or access to personal data when requested by data subjects, including the origin of the data, confirmation that no record exists, the criteria used and the purpose of processing, within thirty (30) days or immediately in a simplified format, in accordance with Law No. 7593/25;

b. The company responds to requests by users to exercise their rights within a maximum period of one month.

Verification of this subcriterion may be based on actual requests for access to personal data.

VI. Updates to the privacy policy

a. The company agrees to notify users—for example, via email, SMS or other direct means—in the event of changes to its personal data processing practices.

VII. Accessibility

a. The company provides clear and comprehensive information on privacy and the protection of personal data in an accessible manner on its website (for example, through a privacy portal or equivalent section), ensuring that such information is also available in the standard-form contracts or applicable privacy policies.

Performance standard:

Full star		The ISP meets 6 to 7 criteria
Three-quarter star		The ISP meets 4 to 5 criteria
Half star		The ISP meets 2 to 3 criteria
One-quarter star		The ISP meets only 1 criterion
Empty star		The ISP does not meet any of the criteria

REPORT - PRIVACY AND PERSONAL DATA PROTECTION POLICY

STARLINK

Privacy and personal data protection policy		
	Yes	**No**
Information on data collection The company provides clear and comprehensive information on: (a) what personal data is collected; (b) in what situations the collection occurs; (c) whether publicly available data may be collected; (d) a list in the privacy policy or notice that identifies, by name, the third parties that provide data to the company (including public data providers); and (e) whether there is an assessment of such third parties' legal compliance regarding personal data protection.		●
Information on processing purposes The company provides clear and comprehensive information on: (a) the purpose of the company's processing of personal data; and (b) the type or manner in which such processing is carried out.	●	
Information on storage, security and sharing The company provides clear and comprehensive information on the storage, security and sharing of personal data, including: (a) how long and where the data is stored; (b) the grounds or scenarios under which personal data may be transferred internationally; (c) whether the data may be retained and under what conditions; (d) what administrative and technical security practices are implemented, including the existence of cybersecurity or information technology (IT) policies that provide protections against malware, ransomware, worms and other types of threats; (e) whether there are access controls for personal data, taking into account the different categories of staff; (f) with which third parties the company shares personal data once it has been collected; (g) for what purposes such sharing takes place, including the use of software, digital platforms, networks or cloud services for internal purposes; and (h) under what circumstances personal data may be transferred internationally.		●
Information on rights (a) The company informs users of their rights regarding personal data protection; (b) the company clearly sets out the available means (e.g., emails, forms or web portals) for exercising those rights.	●	

Responses to rights requests (a) The company provides clear and comprehensive information regarding the retention of or access to personal data when requested by data subjects, including the origin of the data, confirmation that no record exists, the criteria used and the purpose of processing, within thirty (30 day s or immediately in a simplified format, in accordance with Law No. 7593/25; (b) The company responds to requests by users to exercise their rights within a maximum period of one month. Verification of this subcriterion may be based on actual requests for access to personal data.		●
Updates to the Privacy Policy (a) The company agrees to notify users—for example, via email, SMS or other direct means—in the event of changes to its personal data processing practices.		●
Accessibility (a) The company provides clear and comprehensive information on privacy and the protection of personal data in an accessible manner on its website (for example, through a privacy portal or equivalent section), ensuring that such information is also available in the standard-form contracts or applicable privacy policies.	●	

Starlink provides a public privacy policy (Starlink, 2026) that describes how it processes personal data worldwide for Internet services, including its satellite Internet services. This document outlines the different types of data it collects, the reasons for processing them, the security measures it has in place and how to contact the company, thereby allowing for some assessment of compliance with the evaluation criteria.

However, the analysis must include an essential methodological component: the contractual documentation for the Paraguay section includes an “Agreement for Honduras” in the Spanish-language version of the document (Starlink, n.d.-c), which demonstrates that the company does not provide a contract tailored to the jurisdiction of Paraguay. This fact affects the understanding of the legal framework applicable to users in Paraguay and, consequently, the assessment of accessibility and transparency.

In the evaluation of subcriterion I, we refer to Starlink’s report on the categories of data it could potentially collect, which include identity data, contact data, profile data, financial data, transaction-related data, customer or website technical data, general location data and communications data (Starlink, 2026). It also describes the general sources of data collection, which include collection from users, third parties and through cookies and/or other tracking technologies. However, the subcriterion does not merely call for general statements; it requires the company to explain whether it collects publicly available data, to name the respective third parties from whom it obtains the data, including public data providers, and to indicate its assessment of the legal compliance of the aforementioned third parties. Starlink’s updated policy lists “business partners, subcontractors, advertising networks, analytics providers and search information providers,” but does not name them or provide an assessment of the third parties’ compliance with applicable laws, if any. Therefore, although this information exists, it is neither clear nor complete under the broader regulatory framework, and this subcriterion must also be marked as non-compliant.

With regard to subcriterion II, Starlink meets the requirements. The policy lists the purposes of data collection quite broadly, such as the provision of goods and services, order processing, payments, management and protection of customer relationship services, business protection services, support services and proactive defense against abuse, training of machine learning or artificial intelligence models, commercial communications, compliance with laws and government legal requests. The policy also lists services for protection against fraud and other technical issues, as well as data collection for surveys and analysis to improve products, services and marketing. Additionally, the policy describes how data is processed through the use of cookies and other tracking technologies for the purposes of site operation, advertising, monitoring site and user activity and analyzing site traffic. At this stage, the user gains a general understanding of the purposes of data processing and the main methods used to do so.

Subcriterion III is not fully met. Starlink states that it retains personal information for as long as necessary for the purpose of collection or as permitted by law. Account information is retained for the duration of the account plus an additional two years, according to Starlink. Additionally, the company mentions some general protective measures, such as encrypting information during transmission using Starlink technology, protection against physical breaches and employee response procedures in the event of personal information breaches. The standard requires a transparent and comprehensive explanation of data location and retention schedules, the justification for retention, a tiered system of access restrictions based on employee role and explicit protections against various types of online threats. However, this subcriterion also calls for a complete list of data transfer recipients, the reasons why data transfers are permitted and potential data transfer recipients in different countries.

This policy addresses some of these issues, but there are still significant omissions, such as a failure to clarify the location of data storage or access controls for data storage in terms of the staff seniority level. Furthermore, although the Acceptable Use Policy (Starlink, n.d.-a) and the Traffic Management Policy (Starlink, n.d.-b) specify that SpaceX may monitor data traffic to improve services and defend against viruses or malicious code, this can only be interpreted as a form of network management, not as a comprehensive cybersecurity or personal data protection system.

With regard to data sharing, Starlink states that data may be shared with employees, service providers, partner companies, data processors, internet service providers, advertising and analytics service providers, data backup and storage companies, and companies that assist with payment and communication services. The company also states that data processors and joint data controllers may buy and sell data, provide data to their business partners and use customer data to train their AI, communicate with customers, analyze data and assist customers with their legal rights. However, they did not specify to which third parties they are selling data or how their data would be transferred internationally. Therefore, Starlink is partially compliant but does not fully meet the subcriterion.

Subcriterion IV, information on rights, is met. Starlink informs users that they may have legal rights to access, update, delete, restrict or object to the processing of certain personal information. In addition, the email address privacy@spacex.com is provided as a means to exercise these rights. Reference is also made to specific annexes for certain jurisdictions, including the U.S., EEA+, Mexico, Brazil, Nigeria and South Korea. Although there is no annex for Paraguay, this subcriterion concerns the notification of rights and the means of exercising those rights, both of which are provided by Starlink. It should therefore be considered met.

The requirement regarding responses to requests to exercise rights, subcriterion V, is not met. Although the policy mentions a channel for exercising rights, it does not state that Starlink will provide a response within fifteen days, nor a simplified and immediate response, nor within a maximum of one month. Nor does the policy mention that the response will include information on whether or not the requester's personal data is present in its databases, as well as the criteria and purposes of the processing carried out. The policy even states that it may request additional information to verify the requester's identity, but it does not specify the timeframes or the content of the response required by the criterion.

Subcriterion VI, regarding updates to the privacy policy, is not met. Starlink states that updates to the policy may reflect changes in practices, legal requirements and the services offered, and that the policy should be reviewed periodically. The policy also indicates that, by continuing to use the site or services, users accept the updated terms. This policy places the responsibility for compliance on the user and does not commit the company to directly notifying users of changes to data processing practices via electronic means. The Acceptable Use Policy (Starlink, n.d.-a) states that changes take effect after SpaceX publishes or posts the changes on starlink.com/legal. This also does not include direct notification of updates to the personal data processing policy.

Finally, subcriterion VII, accessibility, is met in formal terms. Starlink makes its privacy policy and additional materials available through its legal portal. The text is organized into clear sections: collected information, sources of collected information, purposes for collecting information, sharing of information, protection of information, user rights, children's policy, retention of information, policy on third-party sites, policy on changes and contact information. Although the document is global in scope and does not include a specific appendix for Paraguay, the information is available in Spanish and is presented in a privacy notice specific to the service. Accordingly, this subcriterion is considered met, although accessibility in practice is somewhat limited by the lack of local adaptation.

In accordance with the established performance standard, Starlink meets
3 out of 7 subcriteria and therefore receives a half-star rating.

CLARO – AMX PARAGUAY S.A

Privacy and personal data protection policy		
	Yes	**No**
Information on data collection The company provides clear and comprehensive information on: (a) what personal data is collected; (b) in what situations the collection occurs; (c) whether publicly available data may be collected; (d) a list in the privacy policy or notice that identifies, by name, the third parties that provide data to the company (including public data providers); and (e) whether there is an assessment of such third parties' legal compliance regarding personal data protection.		●
Information on processing purposes The company provides clear and comprehensive information on: (a) the purpose of the company's processing of personal data; and (b) the type or manner in which such processing is carried out.	●	
Information on storage, security and sharing The company provides clear and comprehensive information on the storage, security and sharing of personal data, including: (a) how long and where the data is stored; (b) the grounds or scenarios under which personal data may be transferred internationally; (c) whether the data may be retained and under what conditions; (d) what administrative and technical security practices are implemented, including the existence of cybersecurity or information technology (IT) policies that provide protections against malware, ransomware, worms and other types of threats; (e) whether there are access controls for personal data, taking into account the different categories of staff; (f) with which third parties the company shares personal data once it has been collected; (g) for what purposes such sharing takes place, including the use of software, digital platforms, networks or cloud services for internal purposes; and (h) under what circumstances personal data may be transferred internationally.		●
Information on rights (a) The company informs users of their rights regarding personal data protection; (b) the company clearly sets out the available means (e.g., emails, forms or web portals) for exercising those rights.	●	

Responses to rights requests (a) The company provides clear and comprehensive information regarding the retention of or access to personal data when requested by data subjects, including the origin of the data, confirmation that no record exists, the criteria used and the purpose of processing, within thirty (30 day s or immediately in a simplified format, in accordance with Law No. 7593/25; (b) The company responds to requests by users to exercise their rights within a maximum period of one month. Verification of this subcriterion may be based on actual requests for access to personal data.		●
Updates to the Privacy Policy (a) The company agrees to notify users—for example, via email, SMS or other direct means—in the event of changes to its personal data processing practices.		●
Accessibility (a) The company provides clear and comprehensive information on privacy and the protection of personal data in an accessible manner on its website (for example, through a privacy portal or equivalent section), ensuring that such information is also available in the standard-form contracts or applicable privacy policies.	●	

Claro has a public privacy policy (AMX Paraguay S.A., n.d.-a) tailored for Paraguay, in which it identifies AMX Paraguay S.A. as the data controller for personal data. This document is structured to explain what data is collected, the purpose, the collection process and the end use, and provides, in the context of telecommunications, a fairly comprehensive overview of personal data processing. Likewise, the terms and conditions for the WiFi Internet service (AMX Paraguay S.A., n.d.-c) and the Mi Claro platform (AMX Paraguay S.A., n.d.-b) offer additional information, particularly regarding the signing of contracts, credit analysis and the use of digital media.

The documents analyzed do not have any indication of when the policy was last updated. Therefore, it is not possible to determine the temporal validity of the applicable policies or the actual status of the personal data processing to which the practices refer. Although this factor does not directly affect the assigned score, it constitutes a significant limitation regarding the assessment of the company's transparency.

Regarding subcriterion I, information on data collection, Claro identifies the types of personal data collected, which are primarily identification, contact and reference data, asset data and/or technical data associated with the use of its services. Additionally, Claro mentions that personal data may be collected or obtained through other means, including public and/or private repositories, and through commercial credit and/or business assessments.

Nevertheless, the evaluation criterion calls for a higher level of detail. Specifically, the company does not mention third parties, nor does it elaborate on the possible assessment of such third parties' legal compliance with data protection laws. Finally, it also fails to categorize the collection of publicly available information in a differentiated manner.

Consequently, while information on data collection is provided, it is not sufficiently clear and complete in accordance with the required standard.

Regarding subcriterion II, information on processing purposes, Claro meets this requirement since its privacy policy explains the primary and secondary purposes of personal data processing. The primary purposes relate to service provision, billing, customer administration, customer service, credit assessment and contractual obligations. The secondary purposes are associated with marketing, research and service improvement.

Moreover, the terms and conditions of Mi Claro (AMX Paraguay S.A., n.d.-b) further expand on these purposes, adding uses such as self-management, behavioral assessment, identity authentication and service personalization.

The information provided is sufficient for users to understand the purpose for which their personal data is used, as well as the processing methods involved.

Regarding subcriterion III, information on storage, security and sharing, Claro provides general information on the sharing of personal data and some references to security measures. In its privacy policy, Claro states that data may be shared with third parties under certain circumstances, such as with the user's consent, for external data processing and to comply with legal obligations. It also mentions that it may transfer information to affiliates, subsidiaries and service providers involved in providing the service.

With respect to security, the company states that it has implemented general measures, such as information protection mechanisms, restrictions on access to personal data and the use of tools designed to safeguard the confidentiality of information.

However, this information does not adequately address the key aspects of the subcriterion. The policy does not establish specific retention periods for personal data, nor does it detail the specific conditions under which such data is deleted or retained. Nor does it clearly describe differentiated access controls based on employees' roles, nor does it precisely describe the technical security measures in place to address specific risks such as malware, ransomware or other threats.

Therefore, the lack of detailed information on the structure of the storage, maintenance and protection of personal data prevents this subcriterion from being considered met.

Regarding subcriterion IV, information on rights, Claro informs users of certain rights related to personal data protection, including access, updating, rectification, cancellation and withdrawal of consent; as such, Claro provides channels through its customer service centers and digital platforms to facilitate the exercise of these rights.

That said, while the process is user-friendly, it lacks components that would make it robust and sound, as evidenced by the fact that the policy does not include a section that methodically explains the scope of data privacy rights and the process by which these rights can be exercised.

The company, however, meets this subcriterion's requirement, which involves explaining these rights and how they can be exercised to the company's customers.

Regarding subcriterion V, responses to rights requests, Claro does not clearly specify any timeframe or process for responding to users' requests to exercise their rights. The policy does not establish a response timeframe or provide guidance on what the response should include. Furthermore, the response should include the source of the data, the criteria applied and the purpose of the processing.

The absence of these elements indicates that the company may recognize these rights but does not ensure that they are exercised through a verifiable process.

Regarding subcriterion VI, updates to the privacy policy, Claro's privacy policy states that it may be modified at any time, with revisions published on the website and users are advised to check it regularly.

However, Claro's policy does not mention a direct obligation to notify users via email, SMS or other direct means of communication in the event of changes to data processing practices.

This approach places the burden of monitoring on users and does not meet the expected standard.

Regarding subcriterion VII, accessibility, Claro displays its privacy policy and other documents on its website in Spanish and in a transparent, corporate format. Furthermore, the various contractual documents are interlinked and allow for the identification of the general framework for the processing of personal data.

The information provided, despite being divided into several documents, remains locatable and accessible to users.

In accordance with the established performance standard, Claro meets
3 out of 7 subcriteria and therefore receives a half-star rating.

TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Privacy and personal data protection policy		
	Yes	**No**
Information on data collection The company provides clear and comprehensive information on: (a) what personal data is collected; (b) in what situations the collection occurs; (c) whether publicly available data may be collected; (d) a list in the privacy policy or notice that identifies, by name, the third parties that provide data to the company (including public data providers); and (e) whether there is an assessment of such third parties' legal compliance regarding personal data protection.		●
Information on processing purposes The company provides clear and comprehensive information on: (a) the purpose of the company's processing of personal data; and (b) the type or manner in which such processing is carried out.	●	
Information on storage, security and sharing The company provides clear and comprehensive information on the storage, security and sharing of personal data, including: (a) how long and where the data is stored; (b) the grounds or scenarios under which personal data may be transferred internationally; (c) whether the data may be retained and under what conditions; (d) what administrative and technical security practices are implemented, including the existence of cybersecurity or information technology (IT) policies that provide protections against malware, ransomware, worms and other types of threats; (e) whether there are access controls for personal data, taking into account the different categories of staff; (f) with which third parties the company shares personal data once it has been collected; (g) for what purposes such sharing takes place, including the use of software, digital platforms, networks or cloud services for internal purposes; and (h) under what circumstances personal data may be transferred internationally.		●
Information on rights (a) The company informs users of their rights regarding personal data protection; (b) the company clearly sets out the available means (e.g., emails, forms or web portals) for exercising those rights.	●	

Responses to rights requests (a) The company provides clear and comprehensive information regarding the retention of or access to personal data when requested by data subjects, including the origin of the data, confirmation that no record exists, the criteria used and the purpose of processing, within thirty (30 day s or immediately in a simplified format, in accordance with Law No. 7593/25; (b) The company responds to requests by users to exercise their rights within a maximum period of one month. Verification of this subcriterion may be based on actual requests for access to personal data.		●
Updates to the Privacy Policy (a) The company agrees to notify users—for example, via email, SMS or other direct means—in the event of changes to its personal data processing practices.		●
Accessibility (a) The company provides clear and comprehensive information on privacy and the protection of personal data in an accessible manner on its website (for example, through a privacy portal or equivalent section), ensuring that such information is also available in the standard-form contracts or applicable privacy policies.	●	

Tigo has established a fairly comprehensive framework for the protection of personal data, which includes its Privacy Policy (Tigo Paraguay, 2025a), its Website Terms and Conditions of Use (Tigo Paraguay, 2025b) and its Single Telecommunications Services Agreement (Tigo Paraguay, 2025c). Together, these documents provide a more complete picture of how personal data is processed both during the contracting process and throughout the provision of services.

One positive aspect is that Tigo's Privacy Policy explicitly states its last update date; the current version is effective as of August 5, 2025. This ensures a degree of transparency, as the document's validity period can be verified, as well as any changes to the company's personal data processing practices.

However, having a more complex document structure does not guarantee compliance in all respects. According to the current standard, the analysis distinguishes between sufficient information regarding the essence of a subcriterion and insufficient information if a crucial structural element is missing.

Regarding subcriterion I, information on data collection, Tigo provides a broad description of the personal data it collects. In its Privacy Policy, it describes categories of personal data and the means of collection, including direct interaction with the user, use of digital services and automatic collection via cookies or other technologies.

The Services Agreement supplements this information by stating that personal, credit and financial data are collected, as well as biometric data, including fingerprints, voice and facial images. It also notes that the provision of this data is mandatory for contracting the service and that the company may verify its accuracy or collect additional information through third parties, such as credit bureaus or specialized entities.

However, the standard requires even greater precision. In particular, the company does not identify the third parties that provide personal data, nor does it provide any description of a mechanism for assessing these third parties' legal compliance. This omission undermines a key aspect of the subcriterion, as it prevents a clear understanding of the external sources of the data and the safeguards in place for data providers.

Tigo meets subcriterion II, information on processing purposes. The Privacy Policy sets forth general purposes for data processing, which are supplemented in greater detail by the terms of the Services Agreement.

In this regard, the agreement explains that data is processed for the purposes of providing the service, managing the contractual relationship, marketing products and services, conducting communications and surveys, analyzing usage, improving the service and preventing fraud.

In addition, it specifies the processing of biometric data for the purposes of identity verification, cybersecurity and crime prevention.

The information disclosed provides service users with a clear understanding of the general objectives and methods of processing.

Regarding subcriterion III, information on storage, security and sharing, Tigo provides details on the sharing of personal data, as well as aspects of storage and security, allowing users to gain a comprehensive understanding of the data management process within the context of its operations.

The Services Agreement states that the user grants the company permission to transfer their personal data to third parties that provide services or products, business partners, affiliated companies, subsidiaries and companies within the same corporate group, whether domestically or abroad, as part of the provision of services.

The Privacy Policy states that data may be shared with third parties for internal and external storage services, data collection, customer service and compliance with legal requirements.

However, the information reveals some significant limitations. The company does not specify how long personal data will be retained, stating only that it will be kept for as long as necessary to fulfill the purpose for which it was processed or to comply with legal requirements. Furthermore, it does not explain the conditions governing data deletion, differentiated access controls or specific measures to protect data against specific threats.

The information does not fully set out all the elements required by the subcriterion and is insufficient to meet the standard's requirement.

Tigo meets subcriterion IV, information on rights, since the Services Agreement expressly states that users have the right to know the mechanisms for accessing, updating, rectifying, deleting, erasing, objecting to and porting their personal data, as outlined in the privacy notice.

This explicit acknowledgment is more comprehensive and better organized than that of most other ISPs analyzed, as it specifies the rights and links them to the processing of personal data.

However, the policy could be improved by better defining each right, as well as the procedures for exercising them.

Regarding subcriterion V, responses to rights requests, Tigo does not meet this subcriterion. It acknowledges rights to a certain extent but does not specify procedures or establish frameworks for responding to requests for access, rectification or deletion within defined timeframes.

This standard requires that response deadlines be indicated, at least the general timeframe for a response and what response mechanisms will be in place. The absence of these elements suggests that there is no guarantee for the exercise of these rights.

Regarding subcriterion VI, updates to the privacy policy, Tigo indicates when it updates its privacy policy; however, there is a lack of evidence that Tigo commits to notifying users when methods of processing personal data are updated.

The Services Agreement states that communication may be conducted via electronic means. However, this is not specifically related to changes to the privacy policy, nor is there an obligation to directly notify users of such changes.

In terms of subcriterion VII, accessibility, Tigo meets the assessed requirements. The Privacy Policy is available on the company's website and can be easily accessed from the footer. Additionally, the company allows users to review the Single Telecommunications Services Agreement before signing up, which contributes to greater transparency in its relationship with users.

Although the various documents related to the processing of personal data, such as the privacy policy, the services agreement and other applicable terms, do not necessarily have the same level of visibility or ease of access, taken together they allow users to gain a reasonably comprehensive understanding of how their personal data is processed during the sign-up process and the provision of services. The relationship between these instruments helps foster an adequate understanding of the data processing practices implemented by the company.

In accordance with the established performance standard, Tigo meets
3 out of 7 subcriteria and therefore receives a half-star rating.

personal

PERSONAL - NÚCLEO S.A.

Privacy and personal data protection policy		
	Yes	**No**
Information on data collection The company provides clear and comprehensive information on: (a) what personal data is collected; (b) in what situations the collection occurs; (c) whether publicly available data may be collected; (d) a list in the privacy policy or notice that identifies, by name, the third parties that provide data to the company (including public data providers); and (e) whether there is an assessment of such third parties' legal compliance regarding personal data protection.		●
Information on processing purposes The company provides clear and comprehensive information on: (a) the purpose of the company's processing of personal data; and (b) the type or manner in which such processing is carried out.	●	
Information on storage, security and sharing The company provides clear and comprehensive information on the storage, security and sharing of personal data, including: (a) how long and where the data is stored; (b) the grounds or scenarios under which personal data may be transferred internationally; (c) whether the data may be retained and under what conditions; (d) what administrative and technical security practices are implemented, including the existence of cybersecurity or information technology (IT) policies that provide protections against malware, ransomware, worms and other types of threats; (e) whether there are access controls for personal data, taking into account the different categories of staff; (f) with which third parties the company shares personal data once it has been collected; (g) for what purposes such sharing takes place, including the use of software, digital platforms, networks or cloud services for internal purposes; and (h) under what circumstances personal data may be transferred internationally.		●
Information on rights (a) The company informs users of their rights regarding personal data protection; (b) the company clearly sets out the available means (e.g., emails, forms or web portals) for exercising those rights.	●	

Responses to rights requests (a) The company provides clear and comprehensive information regarding the retention of or access to personal data when requested by data subjects, including the origin of the data, confirmation that no record exists, the criteria used and the purpose of processing, within thirty (30 day s or immediately in a simplified format, in accordance with Law No. 7593/25; (b) The company responds to requests by users to exercise their rights within a maximum period of one month. Verification of this subcriterion may be based on actual requests for access to personal data.		●
Updates to the Privacy Policy (a) The company agrees to notify users—for example, via email, SMS or other direct means—in the event of changes to its personal data processing practices.		●
Accessibility (a) The company provides clear and comprehensive information on privacy and the protection of personal data in an accessible manner on its website (for example, through a privacy portal or equivalent section), ensuring that such information is also available in the standard-form contracts or applicable privacy policies.	●	

Personal provides a set of documents consisting of its Privacy Policy (Personal Paraguay, n.d.-a), General Terms and Conditions (Personal Paraguay, n.d.-b) and App Terms and Conditions (Personal Paraguay, n.d.-c). Together, these documents outline the main aspects of personal data processing in connection with the provision of the service, although they are less integrated than the documentation provided by other ISPs assessed.

Unlike Tigo and similarly to Claro, the privacy policy does not clearly and explicitly state a date of last modification, which makes it difficult to assess the current validity of the practices described. This constitutes a shortcoming in terms of transparency.

Regarding subcriterion I, information on data collection, Personal provides information on the categories of personal data it collects through its Privacy Policy and associated documents. The data collected includes identification and contact information, data necessary to provide services and information generated when using platforms and applications.

The App Terms and Conditions supplement this information and state that data may also be collected regarding the use of digitally provided services, how users interact with the platforms and user behavior.

However, this subcriterion requires further detail. Personal does not formally name the third parties with which it shares personal data. Nor does it mention a mechanism to ensure that third parties act lawfully. It also does not explain the separate collection of data from public sources.

Without these specific details, it is impossible to understand the external source of the personal data and the protections in place for the third parties that provide it.

Personal meets subcriterion II, information on processing purposes, since the Privacy Policy and the Terms and Conditions indicate that the processing of personal data is intended to provide services, manage service contracts, serve customers, bill, communicate, offer products and services and improve services.

The app's terms of use describe the purposes in the context of using the digital platform, including personalization, behavioral analysis and improving the user experience.

This information makes the purpose and context of personal data processing clear.

Similarly, regarding subcriterion III, information on storage, security and sharing, Personal does not meet this subcriterion. Although it describes the processing of personal data in general terms and mentions the possibility of sharing data with third parties in the provision of services or in cases of compliance with the law, this is insufficient to meet the substance of the subcriterion.

The documentation does not establish specific time limits for data storage and does not specify under what circumstances data may be deleted or retained for longer periods; nor does it specify technical security measures or differentiated access controls, nor does it detail the third parties with whom the information is shared.

From this perspective, the available data does not adequately and sufficiently explain the storage of personal data, the security of storage and data management throughout the storage lifecycle.

The Privacy Policy informs individuals of their personal data protection rights and details, to a certain extent, the procedural framework for how these rights should be exercised.

The rights to access, rectify and update data are recognized and described, along with the means and channels available for users to submit requests regarding their personal data.

However, more transparent information should be provided regarding the scope of each right and the corresponding procedural framework for exercising them.

Regarding subcriterion V, responses to rights requests, Personal does not meet this subcriterion. Although it acknowledges these rights, it has not established deadlines or methods for responding to requests from users to exercise their rights.

The standard requires information on response times, the minimum content of responses and specific mechanisms for handling such requests. If any of these elements are missing, the effective exercise of these rights is not guaranteed.

Regarding subcriterion VI, updates to the Privacy Policy, Personal does not meet this subcriterion. While it may update its policies and terms, there is no obligation to inform users of changes related to its operations concerning the collection and processing of their personal data.

The absence of direct notification systems essentially places the responsibility on users to periodically review the documents to detect changes and/or other updates. This does not meet the appropriate standard in this regard.

Regarding subcriterion VII, accessibility, Personal meets this subcriterion. The Privacy Policy and the Terms and Conditions are published on the company's website and are easily accessible to users.

Furthermore, the documents are organized into user-friendly sections on the website, allowing users to easily find relevant information.

In accordance with the established performance standard, Personal meets
3 out of 7 subcriteria and therefore receives a half-star rating.

CRITERION 2. Judicial authorization

Does the ISP commit to disclosing customer information, metadata and communications content only upon presentation of a court order?

This category assesses whether the ISP requires authorities to present judicial authorization prior to the disclosure of data regarding the content of communications or their metadata. Whether the company, in its contract or any official document available to the public, makes clear to users the circumstances under which judicial or administrative authorities may access their data.

Evaluation criteria

I. The ISP commits to providing data on the content of a user's communications to judicial authorities, subject to a prior court order;

II. Whether it distinguishes between the disclosure of data and metadata and commits to doing so only subject to a prior court order.

Performance Standard:

Full star		The ISP meets all criteria
Half star		The ISP meets one of the criteria
Empty star		The ISP does not meet any of the criteria

REPORT - JUDICIAL AUTHORIZATION

STARLINK

Judicial authorization		
	Yes	**No**
The ISP commits to providing data on the content of a user's communications to judicial authorities, subject to a prior court order.		●
Whether it distinguishes between the disclosure of data and metadata and commits to doing so only subject to a prior court order.		●

Starlink regulates access to its users' personal data primarily through its Privacy Policy (Starlink, 2026) and its Terms of Service (Starlink, n.d.-c). These documents contain provisions regarding the disclosure of information to authorities, but they do not establish sufficient safeguards regarding the requirement for a prior court order.

Regarding subcriterion I, disclosure of communications content, Starlink makes no mention of disclosing communications content exclusively in response to a court order.

According to its Privacy Policy, the company may disclose personal information to comply with legal, regulatory or governmental requirements. This wording, such as "the company is required by law" or "to comply with legal obligations," does not limit disclosure to cases where a court order exists, but leaves open the possibility of providing data in response to different types of governmental requests.

This approach is problematic under the evaluated standard, as it does not distinguish between levels of legal requirements nor does it guarantee that users' communication data remains subject to prior judicial review of access.

Given the absence of an express requirement for a court order, we can conclude that the company may have overly broad discretion to determine when to disclose the data, which negatively impacts users' privacy.

Regarding subcriterion II, metadata distinction and court order requirements, Starlink also fails to meet this subcriterion. In the documents evaluated, there is no identifiable distinction between the content of communications and metadata.

In its privacy policy, the company uses broad and generic categories, for example, in relation to "personal information" or "user data", without necessarily distinguishing between the various types of data or the levels of protection that may apply. It also does not specify any distinction regarding the provision of metadata and does not require a court order for access by authorities.

This omission is significant, as the subcriterion requires not only a distinction between content and metadata but also a commitment to subject both to the requirement of a prior court order.

By failing to meet any of these conditions, the company does not meet the established standard.

In accordance with the established performance standard, Starlink does not meet any of the established criteria and therefore receives an empty-star rating.

CLARO - AMX PARAGUAY S.A.

Judicial authorization		
	Yes	No
The ISP commits to providing data on the content of a user's communications to judicial authorities, subject to a prior court order.		●
Whether it distinguishes between the disclosure of data and metadata and commits to doing so only subject to a prior court order.		●

Claro Paraguay does not mention in its privacy policy or in its public contractual documents any commitment to limit the authorities' access to communication content or metadata to situations in which a prior court order exists. Its privacy policy (AMX Paraguay S.A., n.d.-a) grants the company broad discretion, mentioning the possibility of sharing personal data to comply with legal provisions, guidelines, procedures or government requirements. This wording does not limit the request to a court order but rather allows for a broad scope of government requests.

For a more comprehensive analysis, the 2025 Communications Transparency Report (América Móvil, 2025) from Claro Paraguay's parent company was reviewed. According to the report, América Móvil protects the privacy of communications and describes its policy regarding the processing, receipt, analysis and response to requests made by authorities. However, "competent authorities" refers to public authorities with the power—by law, by a court order or by a prior requirement—to request data from users. In general, this definition does not establish restrictions requiring a prior court order to access the data.

The report notes that América Móvil conducts a due diligence process for requests from authorities, and that the disclosure of information may be required by a "request or order" from a competent authority that meets the essential elements. This wording is significant because it distinguishes between a "request" and an "order," and does not stipulate that all disclosures of information must necessarily be based on a court order.

Regarding subcriterion I, disclosure of communications content, Claro does not meet this subcriterion. The public documentation analyzed does not allow for the conclusion that the disclosure of communications content to authorities is subject exclusively and in all cases to a prior court order. Although some documents refer to the need for a written order from a competent authority for certain actions, both the privacy policy and the Communications Transparency Report use broader language, including references to requirements, legal proceedings and requests from competent authorities. Consequently, the company does not expressly, uniformly and unequivocally establish that any disclosure of communications content necessarily depends on a prior court order, a requirement mandated by this evaluation criterion.

Regarding subcriterion II, metadata distinction and court order requirements, Claro also fails to meet this subcriterion. Although the Transparency Report distinguishes between categories such as “disclosure of retained data,” “real-time geolocation” and “interception of private communications,” it does not specify with sufficient clarity what types of data each category encompasses nor does it expressly state that the disclosure of retained data is subject to a prior court order.

This distinction suggests that the company differentiates between the content of communications and other categories of information associated with communications. However, the documentation analyzed does not outline a specific policy for metadata nor does it publicly commit to subjecting its disclosure to the same standard of protection applicable to the content of communications. This omission is particularly significant given that metadata can reveal sensitive information about users’ activities, relationships, location and behavioral patterns.

According to the established performance standard, Claro does not meet any of the criteria, just as in the previous edition, and therefore receives no stars.

TIGO – TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Judicial authorization		
	Yes	**No**
The ISP commits to providing data on the content of a user's communications to judicial authorities, subject to a prior court order.		●
Whether it distinguishes between the disclosure of data and metadata and commits to doing so only subject to a prior court order.		●

Tigo Paraguay's privacy policy makes no specific mention of the need for a court order to intercept communications. In fact, its privacy notice (Tigo Paraguay, 2025a) stipulates that the company may provide personal data in many circumstances, including requests from competent authorities, without a court order being a necessary condition.

This overly broad wording allows for the disclosure of data in response to various types of government requests, which does not meet the standard required under this criterion.

To supplement the analysis, the Annual Report on Disclosure to Judicial Authorities (Millicom International Cellular S.A., 2024) from Tigo Paraguay's parent company was reviewed. In that report, Millicom states that, in Paraguay, subsidiaries only disclose the content of communications upon presentation of a court order, and that protocols are in place to verify the legitimacy of such orders before any interception begins.

Furthermore, this report takes into account and distinguishes between different types of requests. These include requests for the interception of communications, access to mobile financial services and the collection of various types of data. It also indicates that requests for such data are evaluated for legality before the requested information is disclosed.

However, this report has many serious issues that affect the assessment. First, it does not appear on Tigo Paraguay's website, but rather on Millicom's corporate website. Second, it is not included in the contracts or privacy statements available to users in Paraguay. Therefore, this report, by definition, cannot be considered fully integrated into the transparency framework.

In this regard, even if the corporate group claims that standards are higher at the corporate level, in practice, they are not clearly stipulated in Tigo Paraguay's local documentation.

Tigo does not meet subcriterion I, disclosure of communications content, because, although Millicom's Law Enforcement Disclosure Report (LED) report indicates that communications content is disclosed only upon a court order, Tigo Paraguay's privacy policy and agreements do not enshrine this safeguard.

The criterion stipulates that this information must be readily available to users through the ISP's public documentation. Therefore, it is not possible to consider this subcriterion met based on information that is not publicly available.

Regarding subcriterion II, metadata distinction and court order requirements, Tigo also fails to meet this subcriterion. While Millicom's LED report distinguishes between different categories of information, including communications content, customer metadata and other types of data, Tigo Paraguay's public documentation does not clearly and accessibly state that the disclosure of metadata is always subject to a prior court order.

Furthermore, although Millicom states that requests undergo a legality review before information is disclosed, there is no public and unequivocal commitment guaranteeing that all categories of metadata will be disclosed only in compliance with a court order. This lack of clarity is particularly significant given that metadata can reveal sensitive information about users' activities, location, relationships and behavioral patterns.

In accordance with the established performance standard, Tigo does not meet any of the criteria set forth and therefore receives an empty-star rating.

personal

PERSONAL - NÚCLEO S.A.

Judicial authorization		
	Yes	No
The ISP commits to providing data on the content of a user's communications to judicial authorities, subject to a prior court order.		●
Whether it distinguishes between the disclosure of data and metadata and commits to doing so only subject to a prior court order.		●

Unlike other ISPs analyzed, Personal operates under a more limited regulatory framework regarding government access to private data. Neither its Privacy Policy (Personal Paraguay, n.d.-a) nor its Terms and Conditions (Personal Paraguay, n.d.-b, n.d.-c) disclose the specific circumstances under which the company discloses information to public authorities.

In the documents reviewed, the company refers to general principles related to compliance with legal or regulatory obligations, without clarifying whether the transmission of data, and in particular data related to communications, is subject to the existence of a court order.

This lack of precision is significant, as the criterion under review requires a specific, unambiguous and understandable guarantee for users regarding the circumstances under which their data could be handed over to the authorities.

Regarding subcriterion I, disclosure of communications content, Personal, like the other ISPs, does not meet this subcriterion. In its Privacy Policy and contracts, there is no mention indicating that communications content will only be disclosed to public authorities upon the existence of a pre-existing court order.

The company simply states that it may disclose personal information to comply with its legal obligations or requests from public authorities. This wording does not indicate any hierarchy of legal requirements and does not guarantee that sensitive data, including the content of communications, will be accessed only with the approval of an independent judicial authority.

The lack of a clear reference to a court order implies that the company is not providing users with a guarantee that their communications will be protected against potential access by the state.

Regarding subcriterion II, metadata distinction and court order requirements, Personal also fails to meet this subcriterion. The documents analyzed do not identify a clear distinction between the content of communications and metadata, nor do they establish specific conditions for the processing or disclosure of the latter.

Furthermore, there are no provisions requiring that the transmission of metadata be preceded by a court order. The absence of such a distinction is significant, as metadata, which includes call logs, location data and IP addresses can, and often does, contain highly sensitive user-related data.

The lack of distinction in this matter does not ensure that the company is implementing differentiated protection standards based on the type of data, which is inconsistent with the criterion being evaluated.

Based on its published statements, Personal does not appear to take a clear stance on the need to obtain a court order when providing data on the content of communications or metadata.

In accordance with the established performance standard, Personal does not meet any of the established criteria and therefore receives an empty-star rating.

CRITERION 3. User notification

To earn one star in this category, companies must meet at least one of the following actions: Have a policy that ensures notification to users affected by government surveillance measures as soon as permitted by law. Demonstrate that they have taken legal action to remove legal or regulatory barriers that hinder such notifications. Show that they have advocated for notification mechanisms before Congress or other regulatory bodies.

Evaluation criteria

I. The company commits to notifying users before complying with requests for account information and connection logs in cases where notification is not prohibited by law, or to issuing a notification as soon as legally possible.

The company commits to notifying users before complying with requests for account information and connection logs in cases where notification is not prohibited by law, or to notifying them as soon as it is legally permitted.

Performance standard:

Full star		The ISP meets all criteria
Empty star		The ISP does not meet any of the criteria

REPORT - USER NOTIFICATION

STARLINK

User notification		
	Yes	**No**
Does the ISP notify users about the disclosure of personal data to third parties? The company commits to notifying users before complying with requests for account information and connection logs in cases where notification is not prohibited by law, or to issuing a notification as soon as legally possible.		●

Starlink governs the processing and disclosure of personal data primarily through its Privacy Policy (Starlink, 2026) and its Terms of Service (Starlink, n.d.-c). These documents describe its processes for managing and disclosing personal information. In them, the company reserves the right to disclose private information to comply with legal, regulatory or governmental obligations.

In the documents reviewed, there is no provision establishing a commitment to notify users when the government requests their information, regardless of when such a request is made.

The privacy policy is limited to explaining the conditions under which the company may disclose information, but it does not include dynamic transparency measures for users regarding government requests for data access. In particular, it does not provide for mechanisms for subsequent or deferred notification that would allow users to be informed once any legal or procedural restrictions preventing such notification have ceased.

The documents analyzed also lack any reference to legal, regulatory or institutional safeguards in these contexts that would promote user notification mechanisms.

The absence of safeguards reduces transparency regarding how personal information is processed and significantly hinders users' ability to understand and, ultimately, challenge the government's access to their information.

In accordance with the established performance standard, Starlink does not meet the criterion and therefore receives an empty-star rating.

CLARO - AMX PARAGUAY S.A.

User notification		
	Yes	No
Does the ISP notify users about the disclosure of personal data to third parties? The company commits to notifying users before complying with requests for account information and connection logs in cases where notification is not prohibited by law, or to issuing a notification as soon as legally possible.		●

Claro Paraguay regulates the processing and disclosure of personal data through its privacy policy (AMX Paraguay S.A., n.d.-a) and contractual terms (AMX Paraguay S.A., n.d.-c, n.d.-b). In the privacy policy and contracts, the company states that personal information may be shared to comply with the company's legal and regulatory obligations or to meet requests from authorities.

However, there is no provision in the reviewed documentation indicating that the company will commit to informing users when their personal information is requested by the government, whether before or after such information has been provided.

The privacy policy describes the circumstances under which data may be disclosed, such as to comply with a legal requirement or a request from authorities, but it does not specify the means that would be used to proactively inform users about these matters. There is no provision regarding whether users may be notified in accordance with the law, nor regarding the specific conditions under which notification would not be provided in the event that legal restrictions are lifted.

The privacy policy describes the circumstances under which data may be disclosed, such as to comply with a legal requirement or a request from authorities, but it does not specify how users would be proactively informed about these matters. There is no provision on whether users may be notified where permitted by law, nor on whether they will be notified once any legal restrictions preventing notification have been lifted.

An analysis of the 2025 Communications Transparency Report (América Móvil, 2025) also finds no evidence of user notification policies. Although the report describes internal procedures for receiving, assessing and processing requests from authorities, it focuses solely on verifying the legality of those requests and does not establish a procedure for notifying affected users.

The report describes its internal processes regarding the receipt, evaluation and processing of requests from authorities. However, these internal processes only describe the requests and do not provide mechanisms for affected users to be informed about them.

Similarly, there are no references to legal or regulatory efforts to promote notification mechanisms, nor to public advocacy efforts for this purpose.

In this context, the lack of any commitment to notification constitutes a structural omission that prevents users from knowing whether their data has been accessed by the government, even when there are no legal barriers to informing them.

In accordance with the established performance standard, Claro does not meet the criterion and therefore receives an empty-star rating.

TIGO – TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

User notification		
	Yes	**No**
Does the ISP notify users about the disclosure of personal data to third parties? The company commits to notifying users before complying with requests for account information and connection logs in cases where notification is not prohibited by law, or to issuing a notification as soon as legally possible.		●

The Privacy Policy (Tigo Paraguay, 2025a), its Terms and Conditions (Tigo Paraguay, 2025b) and supplementary documentation (Tigo Paraguay, 2025c) describe how the company collects and discloses user data. The policy states that the company may share user data to comply with legal, regulatory or other official requirements.

However, the documents available to users in Paraguay lack a provision or statement describing the company's intention to inform users about the transfer of data to government authorities, whether before or after such a transfer.

As part of this analysis, the Annual Law Enforcement Disclosure Report (LED) from Millicom (Millicom International Cellular S.A., 2024), the parent company of Tigo Paraguay, was reviewed. This report outlines the corporate group's internal processes for receiving and processing data requests from authorities, as well as the types of data that may be requested, including the content and metadata of communications.

However, it does not reflect the company's commitment to notifying users. Since the document focuses on the legality of requests and the company's internal compliance controls, it does not address the lack of a user's right to know when the government is accessing their data.

Similarly, the reviewed documents contain no references to legal, regulatory or institutional advocacy efforts to promote user notification mechanisms in this context.

Therefore, the structural omission of any reference to notification mechanisms means that users will not know if their personal data has been requested by a State, or if it has been the subject of a government request, even when there is no legal prohibition against notification.

In accordance with the established performance standard, Tigo does not meet the criterion and therefore receives an empty-star rating.

personal

PERSONAL - NÚCLEO S.A.

User notification		
	Yes	**No**
Does the ISP notify users about the disclosure of personal data to third parties? The company commits to notifying users before complying with requests for account information and connection logs in cases where notification is not prohibited by law, or to issuing a notification as soon as legally possible.		●

Personal governs the processing and disclosure of personal data through its Privacy Policy (Personal Paraguay, n.d.-a), its General Terms and Conditions (Personal Paraguay, n.d.-b) and the App Terms and Conditions (Personal Paraguay, n.d.-c). According to the company's statements in these documents, the sharing of personal data may occur to comply with legal, regulatory or other obligations to the competent authorities.

However, in the documents reviewed, there is no clause establishing or describing the obligation to inform users about the data requested by public authorities, not even after the data has been shared.

The privacy policy generally describes the conditions under which the company discloses information, but it lacks protections for consumer privacy. For example, the policy does not provide for deferred or retroactive notifications, nor does it address the user's right to be informed following a government request for information within the established legal timeframe.

Similarly, the same can be said about the Terms and Conditions, which are general and specific to the app. They are not supplemented by additional provisions that would establish communication with the user in such cases.

According to the established performance standard, Personal does not meet the criterion and therefore receives no stars.

CRITERION 4. Policies for the promotion and defense of human rights

Does the ISP have a public position on respecting and promoting human rights on the Internet, particularly against mass surveillance or unchecked surveillance of communications?

This criterion assesses whether the company has an institutional policy that acknowledges its responsibility to protect and respect human rights, including the right to privacy, and whether it participates in forums or mechanisms aimed at promoting these rights within the scope of its corporate responsibilities.

It also considers whether the company has intervened, individually or collectively, in public processes related to legislative advocacy or before regulatory bodies to defend the right to privacy, as well as whether it has taken legal measures to protect the privacy of its users.

Furthermore, this criterion evaluates whether the company carries out activities such as awareness campaigns, informational sessions or advertising initiatives aimed at raising awareness about the importance of privacy and digital rights. This criterion seeks to measure the company's comprehensive commitment to privacy from various perspectives.

Evaluation criteria

I. Whether the ISP promotes policy or legal initiatives to protect the privacy of its users before Congress, for example through legislative proposals or participation in hearings, or before the courts;

II. Whether the ISP carries out activities, events, advertising campaigns or publishes reports with the aim of raising public awareness about the right to privacy and/or the protection of personal data;

III. Whether the company has challenged, through judicial proceedings, legislation or legal interpretations that it considers to violate the privacy of Internet users. The challenge was based on the grounds that the legislation is disproportionate, does not clearly, precisely and specifically define the cases and circumstances under which data must be provided and/or does not provide adequate safeguards against potential abuses;

IV. Whether the company challenged, either judicially or administratively, at least once during the period under review, abusive requests for access to user data. Such challenges were based on the grounds that the requests exceeded the legal authority of the requesting entity and/or were disproportionate due to a lack of clarity and precision regarding the data requested and the rationale. In addition, any other reason that compromises users' right to privacy may be grounds for challenge;

V. Whether the company participates in any sectoral or multisectoral mechanism for the promotion, respect and protection of human rights within the scope of its corporate responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).

Performance standard:

Full star		The ISP meets four or five criteria
Three-quarter star		The ISP meets three criteria
Half star		The ISP meets two criteria
One-quarter star		The ISP meets one criterion
Empty star		The ISP does not meet any of the criteria

REPORT – POLICIES FOR THE PROMOTION AND DEFENSE OF HUMAN RIGHTS

STARLINK

Policies for the promotion and defense of human rights		
	Yes	No
Whether the ISP promotes policy or legal initiatives to protect the privacy of its users before Congress, for example through legislative proposals or participation in hearings, or before the courts.		●
Whether the ISP carries out activities, events, advertising campaigns or publishes reports with the aim of raising public awareness about the right to privacy and/or the protection of personal data.		●
Whether the company has challenged, through judicial proceedings, legislation or legal interpretations that it considers to violate the privacy of Internet users. The challenge was based on the grounds that the legislation is disproportionate, does not clearly, precisely and specifically define the cases and circumstances under which data must be provided and/or does not provide adequate safeguards against potential abuses		●
Whether the company has challenged, either judicially or administratively, at least once during the period under review, abusive requests for access to user data. Such challenges were based on the grounds that the requests exceeded the legal authority of the requesting entity and/or were disproportionate due to a lack of clarity and precision regarding the data requested and the rationale. In addition, any other reason that compromises users' right to privacy may be grounds for challenge.		●
Whether the company participates in any sectoral or multisectoral mechanism for the promotion, respect and protection of human rights within the scope of its corporate responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).		●

Starlink provides no public, verifiable evidence that it has an active policy that defends or promotes any form of human rights regarding individual privacy, data protection or resistance to abuses in government data requests. Compared to the other ISPs analyzed, there are no documented transparency reports, human rights reports, ESG reports or any institutional documents demonstrating that the company has specific commitments to defending individuals' rights to free expression, protecting privacy or safeguarding personal data in connection with the company's provision of internet service.

Regarding subcriterion I, policy or legal initiatives to protect privacy, no policy or legal initiatives undertaken by Starlink or SpaceX to protect the privacy of their users were identified before Congress, the courts or other institutional bodies. The available evidence is limited primarily to terms of service, privacy provisions, contractual terms, operational policies and legal compliance, rather than advocacy aimed at addressing gaps in the protection of digital rights.

The conclusion of the review of official documents is that there is no evidence of any public action by Starlink to promote legislation or engage in institutional advocacy to strengthen legal protections for privacy against the collection of user data by state agencies. Therefore, there is no evidence that this subcriterion is met.

Regarding subcriterion II, activities, campaigns, advertisements or reports, Starlink also fails to meet this subcriterion. Although there are public documents on privacy and sustainability published by SpaceX, these do not constitute campaigns, sessions, reports or activities aimed at promoting the right to privacy and data protection.

SpaceX's public document on space sustainability (SpaceX, n.d.) addresses the sustainability of the space environment, the mitigation of orbital debris and the protection of the space environment. This public document does not address the protection of user privacy or the protection of personal data. Similarly, SpaceX's privacy policy (SpaceX, 2024) outlines data rights and processing practices but does not constitute a public awareness initiative regarding privacy or data protection.

Therefore, no public actions were identified that meet the required standard.

Regarding subcriterion III, challenging legislation or legal interpretations, no verifiable public evidence was identified showing that Starlink or SpaceX has challenged any law or legal interpretation on the grounds that such laws are disproportionate, incorrect or insufficient in terms of privacy laws.

For this subcriterion, the company's participation in general discussions about regulations in the satellite or connectivity industry is insufficient. Concrete, verifiable legal action regarding the privacy of internet users is required. This type of evidence was also not found in public records or other official records.

Regarding subcriterion IV, challenging abusive requests for access to user data, Starlink also fails to meet this subcriterion. No transparency reports, government request reports or other public documentation were identified in which the company states that it has challenged abusive requests for access to user data, either judicially or administratively.

This omission is particularly significant given that Starlink provides a global internet service and does not issue an independent report on government requests for data access, nor does it disclose the criteria for potentially rejecting, challenging or opposing excessive requests.

Finally, regarding subcriterion V, participation in sectoral or multisectoral mechanisms, no evidence was found that Starlink or SpaceX participate in sectoral or multisectoral mechanisms specifically aimed at promoting, respecting and protecting human rights within the scope of their corporate responsibilities.

A review of institutional records shows that the Global Network Initiative publishes its membership roster (Global Network Initiative, n.d.), but neither Starlink nor SpaceX is listed among its members. The United Nations Global Compact also maintains a public database of corporate participants (United Nations Global Compact, n.d.), but neither Starlink nor SpaceX was identified as a participant.

Although SpaceX/Starlink may participate in technical or regulatory forums in the space or telecommunications sectors, no participation was identified in human rights mechanisms equivalent to the GNI, the Telecommunications Industry Dialogue, the Global Compact or other similar forums.

Therefore, Starlink receives an empty-star rating, as none of the subcriteria are met.

CLARO - AMX PARAGUAY S.A.

Policies for the promotion and defense of human rights		
	Yes	No
Whether the ISP promotes policy or legal initiatives to protect the privacy of its users before Congress, for example through legislative proposals or participation in hearings, or before the courts.		●
Whether the ISP carries out activities, events, advertising campaigns or publishes reports with the aim of raising public awareness about the right to privacy and/or the protection of personal data.	●	
Whether the company has challenged, through judicial proceedings, legislation or legal interpretations that it considers to violate the privacy of Internet users. The challenge was based on the grounds that the legislation is disproportionate, does not clearly, precisely and specifically define the cases and circumstances under which data must be provided and/or does not provide adequate safeguards against potential abuses		●
Whether the company has challenged, either judicially or administratively, at least once during the period under review, abusive requests for access to user data. Such challenges were based on the grounds that the requests exceeded the legal authority of the requesting entity and/or were disproportionate due to a lack of clarity and precision regarding the data requested and the rationale. In addition, any other reason that compromises users' right to privacy may be grounds for challenge.		●
Whether the company participates in any sectoral or multisectoral mechanism for the promotion, respect and protection of human rights within the scope of its corporate responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).	●	

Claro shows significant progress in the broad areas of human rights, privacy and digital security through documents and initiatives from its parent company, América Móvil. However, in the most recent period, there have been no public legal or political advocacy efforts to protect users' privacy against abusive regulations, interpretations of the law or government demands.

Regarding subcriterion I, policy or legal initiatives to protect privacy, there have been no policy or legal initiatives sponsored by Claro Paraguay in recent years aimed at addressing the protection of user privacy in Congress, the judicial system or other relevant forums.

Claro meets subcriterion II, activities, campaigns, advertisements or reports. América Móvil's 2024 Sustainability Report includes a section titled "Privacy Protection and Responsible Use of Customer Data." Through sub-reports and stated corporate policies, the report details the establishment of data protection teams at subsidiaries, various controls and mandatory training on privacy and personal data protection. It also reports that by the end of 2024, 93% of employees, as well as 1,035 business partners, had received training on privacy and personal data protection (América Móvil, 2024).

Furthermore, the report notes that América Móvil supports the protection of privacy, information security and the right to freedom of expression. It also mentions that the company does not interfere with its customers' communications in any way, such as by monitoring or restricting communications, or through other means of manipulation.

Although many of these actions are part of internal training programs and corporate reports, they constitute sufficient public evidence of activities and reports related to privacy, data protection and digital rights.

In contrast, under subcriterion III, challenging legislation or legal interpretations, there is no public evidence that Claro Paraguay or América Móvil have challenged legislation or legal interpretations in court regarding the privacy of internet users and/or disproportionality.

The 2025 Transparency Report (América Móvil, 2025) states that the company has legal review procedures for requests from authorities, but does not mention that it has taken legal action against laws or legal interpretations that limit privacy.

The 2025 Transparency Report states that América Móvil rejects requests that violate the law or are inappropriate, and that the company has its own verification procedures.

However, the subcriterion requires that the company have effectively challenged, questioned or rejected at least one abusive request during the period under review. The available documentation only allows for the identification of internal mechanisms for reviewing, verifying and potentially rejecting requests. Furthermore, according to the information published by América Móvil for Paraguay, no rejected requests were recorded during the period evaluated, unlike what was observed in some other countries where the corporate group operates. Therefore, there is no public evidence to conclude that the company has effectively challenged or rejected an abusive request in Paraguay during the period analyzed.

Regarding subcriterion V, participation in sectoral or multisectoral mechanisms, Claro does meet this subcriterion through América Móvil. The 2024 Sustainability Report states that América Móvil aligns its sustainability strategy with the principles of the United Nations Global Compact and the Sustainable Development Goals. Furthermore, the report indicates that the company actively participates in the GSMA, including sector-specific working groups.

Based on the above, Claro meets two of the five established criteria and therefore receives a half-star rating.

TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Policies for the promotion and defense of human rights		
	Yes	No
Whether the ISP promotes policy or legal initiatives to protect the privacy of its users before Congress, for example through legislative proposals or participation in hearings, or before the courts.		●
Whether the ISP carries out activities, events, advertising campaigns or publishes reports with the aim of raising public awareness about the right to privacy and/or the protection of personal data.	●	
Whether the company has challenged, through judicial proceedings, legislation or legal interpretations that it considers to violate the privacy of Internet users. The challenge was based on the grounds that the legislation is disproportionate, does not clearly, precisely and specifically define the cases and circumstances under which data must be provided and/or does not provide adequate safeguards against potential abuses		●
Whether the company has challenged, either judicially or administratively, at least once during the period under review, abusive requests for access to user data. Such challenges were based on the grounds that the requests exceeded the legal authority of the requesting entity and/or were disproportionate due to a lack of clarity and precision regarding the data requested and the rationale. In addition, any other reason that compromises users' right to privacy may be grounds for challenge.		●
Whether the company participates in any sectoral or multisectoral mechanism for the promotion, respect and protection of human rights within the scope of its corporate responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).	●	

Tigo Paraguay has a relatively well-developed corporate structure regarding human rights through its parent company, Millicom. However, as with other criteria analyzed, there is a gap between corporate commitments and their local implementation or visibility, which effectively reduces compliance with the evaluated criteria.

In subcriterion I, policy or legal initiatives to protect privacy, no recent initiatives by Tigo Paraguay have been documented that directly promote the protection of user privacy before Congress, the judiciary or other institutional bodies.

Although previous reports documented the company's participation in certain regulatory processes, such as the approval of regulations on telecommunications user protection and the role of Cybersecurity and user privacy protection, no initiatives to protect digital rights or engage in public policy advocacy were documented during the period evaluated.

Millicom's own statements regarding its intention to support processes to strengthen the regulatory framework and cybersecurity do not correspond to any demonstrated local action.

Regarding subcriterion II, activities, campaigns, advertisements or reports, compliance with this subcriterion is based primarily on the existence of Millicom's corporate policies, rather than on local evidence directly attributable to Tigo Paraguay.

In particular, Millicom has a human rights policy (Millicom International Cellular S.A., 2023b) that incorporates commitments regarding privacy, personal data protection and freedom of expression, in line with international standards. Likewise, the Law Enforcement Disclosure Report (LED) (Millicom International Cellular S.A., 2024) serves as an institutional transparency mechanism that addresses the handling of requests from authorities and the protection of communications, providing relevant information on data governance and the company's approach to digital rights.

At the local level, Tigo's corporate website (Tigo Paraguay, n.d.) indicates that there are programs focused on corporate social responsibility, particularly in the areas of inclusion and digital education. However, the information provided is insufficient to verify whether these programs were implemented during the period analyzed, as no implementation or update dates are provided.

Therefore, despite the existence of corporate commitments and transparency mechanisms at the corporate group level, the lack of clear, up-to-date and verifiable information on specific campaigns or initiatives carried out by Tigo Paraguay limits the scope of this subcriterion at the local level.

Regarding subcriterion III, challenging legislation or legal interpretations, no verifiable public evidence was found that Tigo Paraguay or Millicom have challenged legislation or legal interpretations in court on the grounds that they violate users' right to privacy.

While the LED report mentions the possibility of filing complaints with judicial bodies for violations of the law, this reference does not prove the existence of a specific action and/or litigation strategy to protect digital rights.

Tigo also fails to meet subcriterion IV, challenging abusive requests for access to user data. However, Millicom reports that it has internal procedures to assess the legality of data access requests and that it may reject those that do not meet legal requirements.

The standard requires evidence that the company has challenged abusive requests through judicial or administrative channels during the period under review. The document does not prove the existence of a specific challenge, but rather demonstrates the existence of internal mechanisms for review and rejection.

Finally, Tigo does meet subcriterion V, participation in sectoral or multisectoral mechanisms. Millicom participates in relevant sectoral forums such as the GSMA (GSMA, n.d.), which means it is part of an international ecosystem where sector guidelines, as well as practices and theories relating to sustainability and digital governance, are discussed.

Based on the above, Tigo meets two of the five established criteria and therefore qualifies for a half-star rating.

personal

PERSONAL - NÚCLEO S.A.

Policies for the promotion and defense of human rights		
	Yes	No
Whether the ISP promotes policy or legal initiatives to protect the privacy of its users before Congress, for example through legislative proposals or participation in hearings, or before the courts.		●
Whether the ISP carries out activities, events, advertising campaigns or publishes reports with the aim of raising public awareness about the right to privacy and/or the protection of personal data.		●
Whether the company has challenged, through judicial proceedings, legislation or legal interpretations that it considers to violate the privacy of Internet users. The challenge was based on the grounds that the legislation is disproportionate, does not clearly, precisely and specifically define the cases and circumstances under which data must be provided and/or does not provide adequate safeguards against potential abuses		●
Whether the company has challenged, either judicially or administratively, at least once during the period under review, abusive requests for access to user data. Such challenges were based on the grounds that the requests exceeded the legal authority of the requesting entity and/or were disproportionate due to a lack of clarity and precision regarding the data requested and the rationale. In addition, any other reason that compromises users' right to privacy may be grounds for challenge.		●
Whether the company participates in any sectoral or multisectoral mechanism for the promotion, respect and protection of human rights within the scope of its corporate responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).	●	

Personal Paraguay demonstrates a poorly developed public policy framework for protecting human rights in the areas of privacy and personal data protection. Compared to other Internet service providers, no institutional documents, corporate reports or public evidence were identified that would indicate a structured strategy in this area at the local level.

Regarding subcriterion I, policy or legal initiatives to protect privacy, there is no evidence that Personal Paraguay has undertaken initiatives to promote user privacy before Congress, the judiciary or any other institution. Furthermore, no recent participation by Personal Paraguay has been detected in the legislative process or in regulatory processes aimed at developing and implementing regulatory frameworks related to digital rights or the protection of personal data.

Regarding subcriterion II, activities, campaigns, advertisements or reports,there is no public evidence during the period analyzed that Personal Paraguay has launched initiatives, events, programs or reports to raise awareness about personal data protection or privacy protection.

Regarding subcriterion III, challenging legislation or legal interpretations, no evidence was found to demonstrate that Personal Paraguay challenged legislation or legal interpretations deemed disproportionate or contrary to users' right to privacy.

Regarding subcriterion IV, challenging abusive data access requests, no public records, reports or descriptions from government institutions were found to confirm that, during the period under review, Personal Paraguay challenged an abusive data access request on behalf of its users, either through administrative or judicial channels.

Personal does meet subcriterion V, participation in sectoral or multisectoral mechanisms. Through its corporate group, it participates in the GSMA, a global mobile industry organization that promotes standards, best practices and forums for dialogue on sustainability, digital governance and the development of the telecommunications ecosystem (GSMA, n.d.).

Therefore, Personal receives a one-quarter star rating, as it meets one of the criteria.

CRITERION 5. Transparency

Does the ISP publish transparency reports containing information on how many times governments have requested data on its users and how often the company provided such data to governments?

The transparency report discloses the origin of requests to block or remove content from the Internet—including child pornography, copyright infringement, compliance with the company's own policies, etc. Although ISPs in Paraguay are under no obligation to produce proactive transparency reports, this could be an opportunity to demonstrate that they are committed to building trust in their relationships with customers based on transparency.

Evaluation criteria

I. The ISP publishes transparency reports so that users can learn about its cooperation with government authorities regarding the data provided;

II. The ISP publishes transparency reports informing about its cooperation with government authorities, specifying:

   a. the number of requests and disclosures categorized by data type—whether account information or connection logs;

   b. the number of requests and disclosures categorized by the government authority that made the request;

   c. the number of requests and disclosures categorized by the reason cited by the government authority—such as the presentation of evidence in civil, criminal or administrative cases, etc.

Performance standard:

Full star		The ISP meets all criteria
Half star		The ISP meets one of the criteria
Empty star		The ISP does not meet any of the criteria

REPORT - TRANSPARENCY

STARLINK

Transparency		
	Yes	**No**
The ISP publishes transparency reports so that users can learn about its cooperation with government authorities regarding the data provided.		●
The ISP publishes transparency reports informing about its cooperation with government authorities, specifying: (a) the number of requests and disclosures categorized by data type—whether account information or connection logs; (b) the number of requests and disclosures categorized by the government authority that made the request; (c) the number of requests and disclosures categorized by the reason cited by the government authority—such as the presentation of evidence in civil, criminal or administrative cases, etc.		●

Starlink does not publish transparency reports detailing the number of data requests made to it by government agencies, nor how often the company provides this type of information.

The documents that are available, including the privacy policy and terms of service, state that the company may provide user data if required to do so by law or in response to a request from the appropriate authorities. However, these terms do not constitute transparency reports, as they do not contain quantitative or systematic information about requests for data access.

Furthermore, there are no institutional reports, corporate documents or specific sections on the Starlink website or that of its parent company, SpaceX, that detail statistics on government data requests, their origin or their rationale.

The lack of transparency reports demonstrates a lack of public access to data needed to measure or describe the scope, volume or even the manner in which Starlink provides data to various government institutions. This severely hinders the ability of end users and civil society to assess whether the data provided is balanced and in compliance with international standards and practices.

Therefore, in the absence of a transparency report, the requirements of this subcriterion are not met with regard to describing the information requested by type, the authority that requested the information and the reason behind the request.

In accordance with the established performance standard, Starlink does not meet any of the criteria and therefore receives an empty-star rating.

CLARO - AMX PARAGUAY S.A.

Transparency		
	Yes	**No**
The ISP publishes transparency reports so that users can learn about its cooperation with government authorities regarding the data provided.	●	
The ISP publishes transparency reports informing about its cooperation with government authorities, specifying: (a) the number of requests and disclosures categorized by data type—whether account information or connection logs; (b) the number of requests and disclosures categorized by the government authority that made the request; (c) the number of requests and disclosures categorized by the reason cited by the government authority—such as the presentation of evidence in civil, criminal or administrative cases, etc.	●	

Claro Paraguay, through its parent company América Móvil, publishes regular transparency reports. These reports contain data on requests for information from government authorities and how the company has responded to those requests.

The 2025 Communications Transparency Report (América Móvil, 2025) is a publicly available source that allows users to assess the company's level of cooperation with judicial authorities, thereby meeting the first subcriterion.

Regarding subcriterion I, publication of transparency reports, América Móvil publishes transparency reports that show the total number of requests for information received from government authorities and the percentage of requests that were granted and/or denied.

It also provides statistics by country, which helps users find information on Paraguay, including the number of requests and their classification by type of authority. In addition, it includes descriptions of the internal review of requests, including criteria of legality and proportionality.

Regarding subcriterion II, content and disaggregation of the report, the 2025 Transparency Report presents disaggregated information that meets the standards required by this subcriterion.

In particular, the report includes: a classification of requests by type of data requested (e.g., retained data, geolocation or communications interception); identification of the authorities making the requests (including judicial and prosecutorial authorities); and a description of the applicable legal framework and the types of requests processed.

Within the scope of the analysis, Claro has established itself as the ISP most committed to transparency by disseminating, through its parent company América Móvil, detailed reports on government data requests, which are published periodically and in an accessible manner to describe their scale and characteristics.

There are still some areas for improvement, such as providing more details to break down the motivations and categories of the requests, but the quality of the data exceeds international industry best practices and that of the ISPs covered in this report.

Therefore,Claro receives a full-star rating for meeting all established criteria.

TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Transparency		
	Yes	**No**
The ISP publishes transparency reports so that users can learn about its cooperation with government authorities regarding the data provided.	●	
The ISP publishes transparency reports informing about its cooperation with government authorities, specifying: (a) the number of requests and disclosures categorized by data type—whether account information or connection logs; (b) the number of requests and disclosures categorized by the government authority that made the request; (c) the number of requests and disclosures categorized by the reason cited by the government authority—such as the presentation of evidence in civil, criminal or administrative cases, etc.		●

Tigo Paraguay, through its parent company, Millicom, publishes the Law Enforcement Disclosure Report (LED) (Millicom International Cellular S.A., 2024), which serves as a mechanism for institutional transparency regarding the company's cooperation with government authorities on data access.

This document allows for an assessment of compliance with the first subcriterion but has significant shortcomings regarding the level of data disaggregation, which limits compliance with the second subcriterion.

Regarding subcriterion I, publication of transparency reports, Millicom periodically publishes the Law Enforcement Disclosure Report (LED), which provides data on the number of information requests made by government agencies.

This report covers the countries in which the company operates, including Paraguay, and provides information on the total number of requests received, as well as the general categories of the requests.

This report allows users to understand the parameters of the data requests processed and the framework of the company's interactions with the government, thereby meeting the standard required by this subcriterion.

Although the LED report provides some categorization of requests, for example, distinguishing between communications interception and metadata, as well as mobile financial services, the level of disaggregation remains insufficient.

Specifically, the report highlights the following shortcomings: the number of requests submitted is not broken down by country, but rather by region (South America); the differentiation by data type is neither detailed nor consistent in most cases; the categorization of requesting authorities is not carried out systematically in most cases; and the grounds for the requests remain unclear, for example, whether they involve civil, criminal or administrative proceedings.

These limitations hinder a complete understanding of the context and circumstances surrounding requests for access to data.

Therefore, although the report represents a notable step toward transparency, it does not yet meet the disaggregation standard for this criterion.

Consequently, Tigo receives a half-star rating for meeting one of the criteria.

personal

PERSONAL - NÚCLEO S.A.

Transparency		
	Yes	**No**
The ISP publishes transparency reports so that users can learn about its cooperation with government authorities regarding the data provided.		●
The ISP publishes transparency reports informing about its cooperation with government authorities, specifying: (a) the number of requests and disclosures categorized by data type—whether account information or connection logs; (b) the number of requests and disclosures categorized by the government authority that made the request; (c) the number of requests and disclosures categorized by the reason cited by the government authority—such as the presentation of evidence in civil, criminal or administrative cases, etc.		●

Personal Paraguay does not publish transparency reports that would allow users to assess how many requests government agencies have made for user data, or how frequently the company provides data to these authorities.

Compared to other ISPs analyzed that have published reports at the local level (or at the level of their parent companies), there are no reports containing quantitative data on government data access requests on the company's website or in publicly available corporate documentation.

Personal does not meet subcriterion I, publication of transparency reports, due to its failure to disclose transparency and institutional reports. Furthermore, no specific sections of this website were found that provide information on how the website handles government data requests.

Since the ISP does not publish transparency reports, it also fails to meet subcriterion II, content and disaggregation of the report, as the publicly available information does not allow for determining: the number of data requests received; the classification of requests by data type (content or metadata); the authorities making the requests or the purposes of such requests.

In accordance with the performance standard, Personal receives an empty-star rating, as none of the criteria are met.

CRITERION 6. Guidelines for requesting personal information

Does the ISP provide clear and complete information on the guidelines, procedures or protocols intended for law enforcement agencies and other government bodies that explain how they should request personal information from its customers? What are the conditions for the disclosure of such personal information?

The evaluation will assess whether the ISP has guidelines, procedures and protocols that determine how each company cooperates with the State, whether by providing information to the criminal prosecution system or for other types of investigations, and, where applicable, what specific requirements must be met for that purpose. It will also assess whether the company, when establishing its own rules for local authorities, takes the national context into account or whether the pre-established guidelines are based on foreign procedures; and, if so, verify whether those guidelines are more stringent in protecting the privacy of its users.

Evaluation criteria

I. Whether the ISP has guidelines, procedures or protocols that determine how it will receive requests for information from its customers;

II. Whether the guidelines, procedures or protocols are publicly available;

III. Whether these guidelines, procedures or protocols explain in detail the steps to be followed in response to a request and the procedure for providing the data to the requesting authority.

Performance standard:

Full star		The ISP meets all criteria
Half star		The ISP meets two of the criteria
One-quarter star		The ISP meets one of the criteria
Empty star		The ISP does not meet any of the criteria

REPORT - GUIDELINES FOR REQUESTING PERSONAL INFORMATION

STARLINK

Guidelines for requesting personal information		
	Yes	**No**
Whether the ISP has guidelines, procedures or protocols that determine how it will receive requests for information from its customers.		●
Whether the guidelines, procedures or protocols are publicly available.		●
Whether these guidelines, procedures or protocols explain in detail the steps to be followed in response to a request and the procedure for providing the data to the requesting authority.		●

Starlink does not disclose guidelines, instructions or protocols to government agencies regarding how they should handle requests for specific user data or internal processes.

The available documents—namely, its privacy policy (Starlink, 2026) and terms of service (Starlink, n.d.-c)—indicate that the company may disclose personal data to comply with a legal obligation or to respond to requests from the relevant government authorities. However, these clauses are not protocols or instructions for government agencies, nor do they stipulate how such agencies should request the information.

In particular, there are no documents equivalent to data access guidelines that specify formal request requirements, validation standards, submission channels or internal evaluation procedures.

Starlink does not meet subcriterion I, existence of guidelines or protocols, as no public evidence was found that the company has specific guidelines or protocols governing how it receives requests for information from authorities.

Since no guidelines or protocols were identified, subcriterion II, public availability, is also not met, as there are no public documents that authorities or citizens can consult to learn about the procedures for requesting information.

Finally, Starlink also fails to meet subcriterion III, level of detail of procedures, since the company does not provide detailed information on the steps authorities must follow to request data, nor on the internal procedures for providing such information.

Therefore, Starlink receives an empty-star rating, as it does not meet any of the criteria.

CLARO - AMX PARAGUAY S.A.

Guidelines for requesting personal information		
	Yes	**No**
Whether the ISP has guidelines, procedures or protocols that determine how it will receive requests for information from its customers.	●	
Whether the guidelines, procedures or protocols are publicly available.	●	
Whether these guidelines, procedures or protocols explain in detail the steps to be followed in response to a request and the procedure for providing the data to the requesting authority.	●	

Claro Paraguay, through its parent company América Móvil, has public policies and procedures governing how requests for data access from government entities are received and processed.

Most of these policies are contained in the 2025 Communications Transparency Report (América Móvil, 2025), which also describes the company's step-by-step internal procedures for handling legal requests.

Therefore, Claro meets subcriterion I, existence of guidelines or protocols. The Transparency Report states that América Móvil has implemented a formal mechanism for receiving, processing and responding to requests from authorities, which includes assessing the legal basis of the request, the jurisdiction of the requesting authority and the proportionality of the request.

Furthermore, it notes that, to be considered valid, requests must meet specific requirements, which demonstrates the existence of an internal framework for handling such requests.

Claro meets subcriterion II, public availability, through its parent company, América Móvil. The Transparency Report is a public and easily accessible document published online that provides authorities, users and civil society organizations with information on the company's general protocols for interacting with the government regarding data access.

This availability helps ensure transparency and predictability in the processes by establishing the public requirements that requests must meet.

Regarding subcriterion III, level of detail of procedures, Claro also meets this subcriterion. The Transparency Report describes the sequence of steps followed in processing data access requests: receipt and formal registration of the request; verification of the requesting authority and its legal authority; assessment of compliance with formal and substantive requirements; determination of whether to approve or reject the request; and disclosure of the requested information once the request has been approved.

The documents analyzed allow for a relatively clear identification of the stages in the process of receiving, evaluating and responding to requests from authorities, which allows this subcriterion to be considered met, although a higher level of operational detail is recommended.

Based on the performance standard, Claro receives a full-star rating for meeting all criteria.

TIGO – TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Guidelines for requesting personal information		
	Yes	**No**
Whether the ISP has guidelines, procedures or protocols that determine how it will receive requests for information from its customers.	●	
Whether the guidelines, procedures or protocols are publicly available.	●	
Whether these guidelines, procedures or protocols explain in detail the steps to be followed in response to a request and the procedure for providing the data to the requesting authority.		●

Tigo Paraguay, through its parent company, Millicom, has general guidelines for handling requests for data access from authorities, which are primarily reflected in the Law Enforcement Disclosure Report (LED) (Millicom International Cellular S.A., 2024).

However, these guidelines have limitations in terms of their level of detail and specificity, which impacts compliance with the third subcriterion.

Tigo meets subcriterion I, existence of guidelines or protocols. The LED Report describes the internal procedures for receiving and evaluating requests from authorities, including reviewing legality, assessing requests in accordance with legal requirements and rejecting those that fail to meet them.

In addition, the company outlines mechanisms for challenging requests that contain legal inconsistencies, which also demonstrates the existence of an internal system for managing requests.

Tigo also meets subcriterion II, public availability. The LED report is a public document accessible through Millicom's corporate website, providing a general overview of how the company manages requests for access to data.

However, it should be noted that this document is not published directly on Tigo Paraguay's local website, which may limit its accessibility to users in the country. Furthermore, a Spanish-language version is not available; it is only published in English.

Regarding subcriterion III, level of detail of procedures, Tigo does not meet this requirement. Although the LED Report includes general descriptions of the company's internal procedures, it does not adequately explain the steps authorities must follow to request data, nor does it outline the complete procedure for providing the information.

More specifically, the document describes general principles but does not define a specific protocol; does not prescribe the formal requirements a request must meet; does not precisely detail the channels for receiving requests or the guidelines for timely responses; and adopts a narrative rather than a procedural approach.

Although general guidelines exist, they do not clearly identify the operational procedure or the specific steps to be followed in response to requests from authorities; therefore, the subcriterion is not considered met.

Consequently, Tigo receives a half-star rating.

personal

PERSONAL - NÚCLEO S.A.

Guidelines for requesting personal information		
	Yes	**No**
Whether the ISP has guidelines, procedures or protocols that determine how it will receive requests for information from its customers.		●
Whether the guidelines, procedures or protocols are publicly available.		●
Whether these guidelines, procedures or protocols explain in detail the steps to be followed in response to a request and the procedure for providing the data to the requesting authority.		●

Personal Paraguay does not provide guidelines or instructions for authorities on how to request users' personal data, nor does it provide the terms and procedures for disclosing such data.

Unlike all other internet service providers analyzed, which have such documents, either locally or from their parent company, no similar guide for authorities or data access protocols was found on the company's website or in publicly available documents.

Therefore, Personal receives an empty-star rating.

CRITERION 7. Accessibility

Does the ISP have a website with an interface that features perceivable and understandable information, as well as functional and operable navigation regarding privacy policies and the terms and conditions of its products and services?

This criterion evaluates whether the ISP provides perceivable information and equivalent alternatives for presenting content, and whether it offers a navigable and functional interface with understandable information that is compatible with the users' tools for accessing its privacy policies and the terms and conditions of its products and services.

Evaluation criteria

I. The ISP has a website interface that provides perceivable information and equivalent alternatives for presenting content, purpose or function;

II. The ISP has a website with a navigable, functional interface that supports keyboard navigation;

III. The ISP has a website with understandable information that appears and operates in a predictable manner;

IV. The content on the ISP's website is compatible with the user's current tools (different browsers, assistive technologies and other user agents).

Standard performance:

Full star		The ISP meets three or all of the criteria
Half star		The ISP meets two of the criteria
One-quarter star		The ISP meets one of the criteria
Empty star		The ISP does not meet any of the criteria

REPORT - ACCESSIBILITY

STARLINK

Accessibility		
	Yes	**No**
The ISP has a website interface that provides perceivable information and equivalent alternatives for presenting content, purpose or function.	●	
The ISP has a website with a navigable, functional interface that supports keyboard navigation.	●	
The ISP has a website with understandable information that appears and operates in a predictable manner.	●	
The content on the ISP's website is compatible with the user's current tools (different browsers, assistive technologies and other user agents).	●	

The design, structure and functionality of the Starlink website demonstrate a high level of accessibility. Users can navigate the site and find useful content, such as legal documents, thanks to its clear and logical design and straightforward information structure.

The technical evaluation using the WAVE Web Accessibility Evaluation Tool did not detect any critical accessibility errors, yielding a score of 9.9 out of 10 (Web Accessibility Tool, n.d.-c). Although some minor alerts were identified, they do not compromise overall functionality or the user experience.

Regarding subcriterion I, perceivable information, the site has good contrast, provides legible typography and presents information in an understandable structure, facilitating the perception of the information.

As for subcriterion II, functional navigation, the site is also easy to use, free of access barriers and features a logical and orderly menu structure.

Regarding subcriterion III, comprehensibility, the information is presented in an easy-to-read and predictable structure, using language that is easily understood.

Regarding subcriterion IV, compatibility, the assessment indicates that the site supports conventional browsers, and no significant structural anomalies were observed. The usability test conducted by the WAVE accessibility tool found no errors that negatively affect the ability to locate information or interact with the site using assistive technologies.

In accordance with the performance standard, Starlink receives a full-star rating.

CLARO - AMX PARAGUAY S.A.

Accessibility		
	Yes	No
The ISP has a website interface that provides perceivable information and equivalent alternatives for presenting content, purpose or function.	●	
The ISP has a website with a navigable, functional interface that supports keyboard navigation.		●
The ISP has a website with understandable information that appears and operates in a predictable manner.		●
The content on the ISP's website is compatible with the user's current tools (different browsers, assistive technologies and other user agents).		●

There are notable deficiencies on Claro's website that affect both the ease of navigation and the site's ability to function in a way that is compatible with assistive technologies. Although information can be displayed to the user at a basic level, the experience is problematic due to a series of structural issues that prevent full access to the content.

The technical evaluation using the WAVE Web Accessibility Evaluation Tool identified multiple accessibility issues, including structural errors, contrast problems and alerts related to content organization, resulting in a score of 5.8 out of 10 (Web Accessibility Tool, n.d.-a). These results indicate a low-to-medium level of accessibility compared to current standards.

Regarding subcriterion I, perceivable information, the site partially meets this subcriterion. The content is perceivable and the text is legible, but some contrast issues have been identified that affect readability and visibility for users with low vision.

Regarding subcriterion II, functional navigation, Claro does not meet this subcriterion. The site has functional navigation issues due to complex structures, problems with the organization of headings and issues with keyboard navigation.

Claro does not meet subcriterion III, comprehensibility. This is because the site's structure is not always predictable, and the organization of the content can create ordering and navigation problems that particularly affect users who rely on assistive technologies.

Finally, regarding subcriterion IV, compatibility, the identified errors affect the site's compatibility with user tools, including contrast errors, a lack of appropriate labels and structural issues.

That said, in this case, Claro receives a one-quarter star rating.

TIGO – TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Accessibility		
	Yes	**No**
The ISP has a website interface that provides perceivable information and equivalent alternatives for presenting content, purpose or function.	●	
The ISP has a website with a navigable, functional interface that supports keyboard navigation.	●	
The ISP has a website with understandable information that appears and operates in a predictable manner.	●	
The content on the ISP's website is compatible with the user's current tools (different browsers, assistive technologies and other user agents).	●	

The Tigo website offers a high level of accessibility, with a clear, well-structured and functional interface that allows for smooth navigation and effective access to relevant content.

The technical evaluation using the WAVE Web Accessibility Evaluation Tool identified a minimal number of issues, including a single error and a few minor alerts, resulting in a score of 9.1 out of 10 (Web Accessibility Tool, n.d.-d). These results reflect strong performance in terms of accessibility.

Based on subcriterion I, perceivable information, the site has very good readability. All elements have adequate contrast and the content is organized in a visually clear manner, allowing for proper perception of the information.

For subcriterion II, functional navigation, the main navigation and its elements allow for smooth access, facilitating navigation without significantly hindering exploration.

Regarding subcriterion III, comprehensibility, the content is clearly structured, legible and predictable. The predictability of the site's structure makes it easy to fill in gaps in information.

And based on subcriterion IV, compatibility, it has been observed that the site is compatible with standard browsers and is adapted to various device screen sizes. The errors detected do not significantly affect use with assistive technologies.

Therefore, Tigo receives a full-star rating.

personal

PERSONAL - NÚCLEO S.A.

Accessibility		
	Yes	No
The ISP has a website interface that provides perceivable information and equivalent alternatives for presenting content, purpose or function.		●
The ISP has a website with a navigable, functional interface that supports keyboard navigation.		●
The ISP has a website with understandable information that appears and operates in a predictable manner.		●
The content on the ISP's website is compatible with the user's current tools (different browsers, assistive technologies and other user agents).		●

The Personal website has significant accessibility issues that affect both the perception of information and navigation, as well as compatibility with assistive technologies.

A technical evaluation using the WAVE Web Accessibility Evaluation Tool identified a high number of errors, including structural flaws, contrast issues and multiple alerts, resulting in a score of 3.9 out of 10 (Web Accessibility Tool, n.d.-b). These results indicate a low level of accessibility compared to current standards.

Regarding subcriterion I, perceivable information, this subcriterion is not met due to the large number of contrast and presentation errors, which primarily affect readability for people with low vision.

Personal does not meet subcriterion II, functional navigation, due to the presence of multiple structural errors, as well as a lack of content organization, which makes navigation, particularly navigation using a keyboard and assistive technology, very difficult.

Subcriterion III, comprehensibility, is also not met. The site's structural design is not entirely predictable and contains inconsistencies that may hinder understanding of the information.

Finally, regarding subcriterion IV, compatibility, the errors detected have a negative impact on the site's level of compatibility with assistive technologies and screen readers, as well as with various user agents.

Consequently, an empty-star rating is assigned.

CRITERION 8. Data disclosure protocol for criminal investigations

Does the ISP commit to following the most protective interpretation of the right to privacy in response to requests for personal data from government authorities, and does it have specific policies in place for such cases?

The provision of personal data in the context of criminal investigations constitutes one of the points of greatest tension between criminal prosecution and the protection of the right to privacy. This criterion assesses whether ISPs adopt a restrictive and rights-protective interpretation of the current regulatory framework when responding to requests for access to data from public authorities.

In this edition, this criterion takes on special relevance following the entry into force of **Law No. 7593/2025 on the Protection of Personal Data**, which establishes mandatory guiding principles for all processing and disclosure of personal data, including its transfer to public authorities. Among these principles are legality, purpose limitation, proportionality, data minimization and demonstrable accountability.

This analysis must be understood in light of the national legal framework, which establishes stringent standards: the National Constitution (Presidency of the Republic of Paraguay, 1992), Articles 33 and 36, protect privacy and the inviolability of communications; the Code of Criminal Procedure (Presidency of the Republic of Paraguay, 1998b), Articles 200 and 228, requires judicial oversight for interception; and Law No. 7593/2025 on the Protection of Personal Data in Paraguay (Presidency of the Republic of Paraguay, 2025b) imposes the principles of legality, proportionality and data minimization in the processing of personal data.

Evaluation criteria

I. Registration data (subscriber information)

This subcriterion assesses whether the company:

a. states that registration data will only be disclosed to duly identified competent authorities, limiting disclosure to cases expressly authorized by law;

b. and/or requires a court order when the request goes beyond the circumstances expressly authorized by law for administrative or regulatory requests or when it poses risks to the right to privacy.

II. Geolocation data

This subcriterion assesses whether the company:

a. clearly distinguishes geolocation data from other types of personal data;

b. and stipulates that its disclosure—especially in real time—requires a court order, in accordance with constitutional standards for the protection of communications.

III. Connection logs (metadata)

This subcriterion assesses whether the company commits to:

a. disclosing connection logs only pursuant to a court order;

b. alternatively, establishing clear and restrictive limits on their disclosure, in line with the constitutional protection of metadata as part of communications.

IV. Prohibition of generic orders

This subcriterion assesses whether the company:

a. commits to rejecting or challenging requests for access to data that do not specifically identify the individual concerned;

b. or that are disproportionate, overly broad or lack sufficient justification.

V. Specific protocols and transparency

This subcriterion assesses whether the company:

a. has public protocols or guidelines governing the disclosure of data to authorities in the context of criminal investigations;

b. and whether these protocols contain clear, structured and accessible information about the applicable criteria and procedures.

Performance standard:

Full star		The ISP meets five of the criteria
Three-quarter Star		The ISP meets four of the criteria
Half star		The ISP meets three of the criteria
One-quarter star		The ISP meets one of the criteria
Empty star		The ISP does not meet any of the criteria

REPORT - DATA DISCLOSURE PROTOCOL FOR CRIMINAL INVESTIGATIONS

STARLINK

Data disclosure protocol for criminal investigations		
	Yes	**No**
Registration data (subscriber information) This subcriterion assesses whether the company: (a) states that registration data will only be disclosed to duly identified competent authorities, limiting disclosure to cases expressly authorized by law; (b) and/or requires a court order when the request goes beyond the circumstances expressly authorized by law for administrative or regulatory requests or when it poses risks to the right to privacy.		●
Geolocation data This subcriterion assesses whether the company: (a) clearly distinguishes geolocation data from other types of personal data; (b) and stipulates that its disclosure—especially in real time—requires a court order, in accordance with constitutional standards for the protection of communications.		●
Connection logs (metadata) This subcriterion assesses whether the company commits to: (a) disclosing connection logs only pursuant to a court order; (b) alternatively, establishing clear and restrictive limits on their disclosure, in line with the constitutional protection of metadata as part of communications.		●
Prohibition of generic orders This subcriterion assesses whether the company: (a) commits to rejecting or challenging requests for access to data that do not specifically identify the individual concerned; (b) or that are disproportionate, overly broad or lack sufficient justification.		●
Specific protocols and transparency This subcriterion assesses whether the company: (a) has public protocols or guidelines governing the disclosure of data to authorities in the context of criminal investigations; (b) and whether these protocols contain clear, structured and accessible information about the applicable criteria and procedures.		●

Starlink does not have publicly available information specifying the procedures for sharing personal data in connection with criminal investigations. The available documents, the privacy policy (Starlink, 2026) and terms of service (Starlink, n.d.-c), indicate that the company may share personal data to comply with legal obligations or requests from competent authorities. This legal language is vague and lacks details regarding what data might be disclosed, the reasons and justifications behind such disclosure, who would receive it or the legal basis for such disclosures. Therefore, the company does not publicly state that its stance is protective of or restrictive regarding the right to privacy.

Regarding subcriterion I, on registration data, Starlink does not specify under what circumstances it discloses basic subscriber data or account information. It does not specify to which authorities such data may be disclosed, or whether these authorities are distinct from administrative, prosecutorial or judicial authorities, or under what circumstances a court order is required. This lack of information makes it difficult to assess whether the company restricts the provision of registration data to legally justified cases or whether it imposes any additional restrictions in the event of government requests.

Subcriterion II, which refers to geolocation data, does not provide information on the processing or disclosure of such data. The company does not distinguish between historical and real-time geolocation data, nor does it specify whether access to such data requires a prior court order. The company's silence on this matter is particularly concerning because geolocation data can reveal a person's movements, place of residence, interpersonal relationships and daily activities or routines. This suggests that stricter safeguards are required.

Regarding subcriterion III, which pertains to connection logs, Starlink also does not apply differentiated principles for the provision of metadata, technical logs or information on service usage. The aforementioned documents do not specify whether this data collection is limited to a court order or whether this data is treated with the same level of protection as the content of communications. The lack of differentiation is concerning because connection logs can expose users to sensitive information about their digital activity, even if the logs do not contain the content of communications.

Regarding subcriterion IV on the prohibition of generic orders, the company has not made any public statement on whether it accepts, rejects or limits requests that are excessively broad, generic or disproportionate. It also does not disclose whether it requires such requests to specify the individual whose data is being sought, the type of data requested, the duration or the purpose of the measure. Without this information, it cannot be concluded that Starlink has implemented safeguards against excessive and potentially abusive government requests.

Regarding subcriterion V on specific protocols and transparency, Starlink does not create, share or publish guides, protocols or guidelines to provide information to public authorities or users about the process by which it responds to data requests in criminal investigations. The absence of guidelines or structured documentation means that it is unclear how information is received, reviewed, confirmed and/or provided. This places the organization at a low level of transparency in a dimension that is particularly sensitive to privacy.

Consequently, Starlink does not meet any of the evaluated subcriteria. Its public documentation does not set out clear, differentiated and rights-protective rules for the disclosure of personal data to authorities in criminal investigations. Accordingly, Starlink receives an empty-star rating.

CLARO - AMX PARAGUAY S.A.

Data disclosure protocol for criminal investigations		
	Yes	**No**
Registration data (subscriber information) This subcriterion assesses whether the company: (a) states that registration data will only be disclosed to duly identified competent authorities, limiting disclosure to cases expressly authorized by law; (b) and/or requires a court order when the request goes beyond the circumstances expressly authorized by law for administrative or regulatory requests or when it poses risks to the right to privacy.		●
Geolocation data This subcriterion assesses whether the company: (a) clearly distinguishes geolocation data from other types of personal data; (b) and stipulates that its disclosure—especially in real time—requires a court order, in accordance with constitutional standards for the protection of communications.		●
Connection logs (metadata) This subcriterion assesses whether the company commits to: (a) disclosing connection logs only pursuant to a court order; (b) alternatively, establishing clear and restrictive limits on their disclosure, in line with the constitutional protection of metadata as part of communications.		●
Prohibition of generic orders This subcriterion assesses whether the company: (a) commits to rejecting or challenging requests for access to data that do not specifically identify the individual concerned; (b) or that are disproportionate, overly broad or lack sufficient justification.	●	
Specific protocols and transparency This subcriterion assesses whether the company: (a) has public protocols or guidelines governing the disclosure of data to authorities in the context of criminal investigations; (b) and whether these protocols contain clear, structured and accessible information about the applicable criteria and procedures.	●	

Claro Paraguay, through América Móvil, provides a moderate level of detail regarding its policies on data requests from authorities. While other internet service providers lack such policies, Claro Paraguay's transparency reports (América Móvil, 2025) and corporate documents, such as its sustainability report (América Móvil, 2024), include references to its internal processes. However, these policies are general and lack the specificity needed to conclude that the company adopts a clearly restrictive approach to data requests and is therefore aligned with the strongest protections of the right to privacy in Paraguay.

Regarding subcriterion I, registration data, Claro has not transparently disclosed the circumstances under which it might provide customer data or basic account information. Claro has stated that it operates within the law, but the description is so vague that it is impossible to determine whether Claro restricts data disclosure to certain types of authorities or in which situations a court order is required. Nor is there a clear distinction between the different types of requests to verify a restrictive policy in this area.

This conclusion is not altered by the fact that the report identifies Article 228 of the Code of Criminal Procedure as the legal basis. That provision authorizes the Public Prosecutor's Office to request information from public and private entities in the context of criminal investigations, but it does not establish specific criteria regarding categories of data, levels of protection or the requirement for judicial oversight. Therefore, the mere reference to this provision does not allow for verification that the company adopts a restrictive and protective interpretation with respect to the registration data.

The absence of regulations regarding geolocation data is even more pronounced in subcriterion II. There are no regulations on the processing or transmission of location data. Nor is there any provision to differentiate between location data that is generated and location data that already exists. Nor is there any information regarding the need for judicial oversight of this type of data. Given that geolocation data is one of the most sensitive types of data, this lack of regulations is one of the most significant shortcomings in privacy protection.

Although América Móvil's report identifies real-time geolocation as a distinct category of requests, it does not elaborate on the legal conditions applicable to its disclosure nor does it specify whether a court order is required to access this information. Nor does it distinguish between historical data and real-time data. Consequently, the regulatory reference is insufficient to demonstrate a policy aligned with enhanced privacy protection standards.

Regarding subcriterion III, connection logs, although América Móvil's transparency reports include references to different types of requests, including those involving metadata, there is no specific rule restricting the disclosure of such information to requests made pursuant to a court order, nor are there criteria that treat metadata in a manner consistent with the standards established by constitutional and inter-American case law. Therefore, it cannot be said that the company adopts a restrictive interpretation in this regard.

Similarly, although the report distinguishes the category of retained data or metadata, the cited regulations are not accompanied by an explanation of the safeguards applicable to these records or of the need for judicial oversight regarding access to them. This lack of precision is particularly significant given that constitutional and inter-American case law recognizes that metadata can reveal sensitive information about individuals' private lives.

Regarding subcriterion IV, prohibition of generic orders, there are some positive developments. In its reports, América Móvil explains the legal basis for the requests it may receive, suggesting that some internal controls may be in place to identify inappropriate requests. Although there is no formal commitment to reject generic, overly broad or disproportionate requests, and no explicit public mechanism or criteria for identifying them, the existence of legal review mechanisms provides some preliminary legal safeguards. Therefore, this subcriterion is met to a certain extent.

Finally, regarding subcriterion V, specific protocols and transparency, there is no full compliance, although some progress is evident. The publication of transparency reports is an important means of ensuring accountability, as they show how requests from authorities are handled and what types of controls are in place, albeit in general terms. However, these reports do not provide a structured, detailed and accessible protocol describing the process for requests, evaluations and data submission. Furthermore, there are no publicly accessible guidelines for authorities or the general public that would allow them to fully understand the criteria applied. In this regard, despite the low level of progress in advancing transparency, since the protocol is not yet fully developed, this subcriterion is considered partially met.

Claro demonstrates an intermediate level of compliance with this criterion. Unlike other ISPs, it has internal review mechanisms and a certain degree of transparency, but these do not translate into clear, differentiated and rights-protective rules governing the disclosure of data in criminal investigations. The company does not clearly define how it handles different types of data, nor does it establish explicit commitments regarding risks such as generic requests or the absence of judicial oversight.

Accordingly, Claro receives a three-quarter star rating for meeting two of the criteria.

TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)

Data disclosure protocol for criminal investigations		
	Yes	**No**
Registration data (subscriber information) This subcriterion assesses whether the company: (a) states that registration data will only be disclosed to duly identified competent authorities, limiting disclosure to cases expressly authorized by law; (b) and/or requires a court order when the request goes beyond the circumstances expressly authorized by law for administrative or regulatory requests or when it poses risks to the right to privacy.		●
Geolocation data This subcriterion assesses whether the company: (a) clearly distinguishes geolocation data from other types of personal data; (b) and stipulates that its disclosure—especially in real time—requires a court order, in accordance with constitutional standards for the protection of communications.		●
Connection logs (metadata) This subcriterion assesses whether the company commits to: (a) disclosing connection logs only pursuant to a court order; (b) alternatively, establishing clear and restrictive limits on their disclosure, in line with the constitutional protection of metadata as part of communications.		●
Prohibition of generic orders This subcriterion assesses whether the company: (a) commits to rejecting or challenging requests for access to data that do not specifically identify the individual concerned; (b) or that are disproportionate, overly broad or lack sufficient justification.	●	
Specific protocols and transparency This subcriterion assesses whether the company: (a) has public protocols or guidelines governing the disclosure of data to authorities in the context of criminal investigations; (b) and whether these protocols contain clear, structured and accessible information about the applicable criteria and procedures.	●	

Tigo Paraguay, through Millicom, demonstrates an intermediate level of development in managing data access requests from authorities. This is primarily reflected in the Law Enforcement Disclosure Report (LED) (Millicom International Cellular S.A., 2024). Unlike companies that have no documentation at all, in this case it is actually possible to identify some policies and cite some internal processes. However, these aspects do not constitute a clear, detailed and explicitly aligned regulatory framework that can be interpreted as aimed at guaranteeing the right to privacy in the Paraguayan context.

Regarding subcriterion I, registration data, the LED report states that the company assesses the legality of requests before disclosing the data. However, this statement is quite general, and it is not possible to identify specific, publicly available rules governing the circumstances under which registration data is disclosed or the specific circumstances in which a court order is required. The company also does not clearly distinguish between the different types of requesting authorities. The lack of detail makes it impossible to assess whether the company's policy takes a restrictive and protective approach in this area.

Regarding subcriterion II, geolocation data, the document does not specify regulations governing the provision of this type of data. The document does not specify the distinction between real-time geolocation data and historical geolocation data. The document does not specify whether geolocation data, in general, is subject to a stronger standard of protection, such as a standard requiring a court order. Given the obvious sensitivity of the data, this can be considered a significant shortcoming.

Regarding subcriterion III, connection logs, the LED report classifies these as including metadata and other types of technical information. This classification in itself does not provide a meaningful rule limiting the provision of metadata to cases where a court order is issued. Furthermore, there are no developed criteria that explicitly recognize the protected nature of metadata as consistent with constitutional and inter-American standards. Therefore, it cannot be asserted that a restrictive policy exists regarding this type of data.

However, Millicom shows some positive developments under subcriterion IV regarding the prohibition of generic orders. The company's report states that it evaluates the legal basis of the orders it receives and that, in cases of legal inconsistencies or potential legal violations, it will challenge those orders and may even seek judicial review. This indicates the existence of internal control mechanisms for handling government requests. However, the company lacks an explicit commitment to reject generic, vague or disproportionate orders, as well as publicly available criteria for identifying such orders. Therefore, although some basic mechanisms exist, they are not robust, and the company is considered to be partially compliant with this subcriterion.

Finally, regarding subcriterion V, specific protocols and transparency, the LED report represents a significant step forward in transparency, as it describes, in general terms, how the company responds to requests for access to data and makes some internal processes visible. However, this report does not provide a structured, systematic and deliberately accessible protocol for understanding the processes for receiving, evaluating and providing information. There is also a lack of publicly available guidelines addressed to authorities or the public that specify the standards used in criminal proceedings. Therefore, although there has been some progress in terms of transparency, it is very basic in nature and insufficient to meet the standard; consequently, the company is assessed as partially compliant with this subcriterion.

Accordingly,Tigo receives a three-quarter star rating for meeting two criteria.

personal

PERSONAL - NÚCLEO S.A.

Data disclosure protocol for criminal investigations		
	Yes	**No**
Registration data (subscriber information) This subcriterion assesses whether the company: (a) states that registration data will only be disclosed to duly identified competent authorities, limiting disclosure to cases expressly authorized by law; (b) and/or requires a court order when the request goes beyond the circumstances expressly authorized by law for administrative or regulatory requests or when it poses risks to the right to privacy.		●
Geolocation data This subcriterion assesses whether the company: (a) clearly distinguishes geolocation data from other types of personal data; (b) and stipulates that its disclosure—especially in real time—requires a court order, in accordance with constitutional standards for the protection of communications.		●
Connection logs (metadata) This subcriterion assesses whether the company commits to: (a) disclosing connection logs only pursuant to a court order; (b) alternatively, establishing clear and restrictive limits on their disclosure, in line with the constitutional protection of metadata as part of communications.		●
Prohibition of generic orders This subcriterion assesses whether the company: (a) commits to rejecting or challenging requests for access to data that do not specifically identify the individual concerned; (b) or that are disproportionate, overly broad or lack sufficient justification.		●
Specific protocols and transparency This subcriterion assesses whether the company: (a) has public protocols or guidelines governing the disclosure of data to authorities in the context of criminal investigations; (b) and whether these protocols contain clear, structured and accessible information about the applicable criteria and procedures.		●

Personal Paraguay demonstrates a limited capacity to manage data requests from authorities in the context of legal proceedings. Compared to other companies in the study, no local or parent company documents were identified, where applicable, that establish instructions, criteria or protocols governing how the company processes requests for access to data.

Regarding subcriterion I, registration data, Personal has not publicly disclosed the circumstances under which it discloses subscriber or account data. There are no criteria establishing which authorities are authorized to request such data or the situations in which a court order would be required. This makes it impossible to confirm whether or not the company imposes restrictions or controls on the sharing of such information.

Regarding subcriterion III, connection logs, there are no rules governing the disclosure of metadata or technical logs relating to service use. There are no rules establishing restrictions, conditions or court order requirements for this type of data. It is therefore not possible to determine whether the company's policy is consistent with constitutional standards for the protection of communications.

Regarding subcriterion IV, prohibition of generic orders, no explicit commitments to reject or challenge broad, generic or disproportionate requests are identified. The company does not state whether it requires a minimum level of specificity in requests or whether it has control mechanisms in place to address potential abuses by authorities.

Finally, regarding subcriterion V, specific protocols and transparency, Personal does not publish any guides, protocols or guidelines governing the disclosure of data to authorities in criminal investigations. Nor are there any documents describing the procedure for receiving, evaluating and responding to such requests, nor is there any information intended for authorities or users.

Consequently, Personal receives an empty star rating, as it does not meet any of the criteria.

CONCLUSION

This edition of the study shows the same pattern observed in previous editions among Paraguayan Internet service providers (ISPs), confirming persistent disparities depending on the type of company, as well as in the evolution of their policies and their willingness to adopt transparency practices. Compared with previous editions, this year's study includes Starlink and excludes local providers such as COPACO and VOX. This has partially reshaped the basis for comparison but has not altered the main conclusions.

Overall, among companies with an international presence, América Móvil (Claro) and Millicom (Tigo) remain the companies that have made the most progress on certain indicators, particularly in transparency and policy formulation. However, this progress has been partial, slow and, in many cases, more formal than substantive. By contrast, Personal continues to lag behind across almost all dimensions, while Starlink stands out by performing better on criteria related to policies and publicly available documentation, although it continues to show low levels of transparency regarding government access to user data.

Privacy and personal data protection policy

Most of the ISPs reviewed have some form of privacy policy. However, there are significant shortcomings, such as a lack of clarity in the policy documents, the presence of contradictions and the absence of important elements. Claro, Tigo and Personal have documents available, but none address relevant data retention periods or processing criteria, which undermines fundamental principles of Law No. 7593/2025, such as data minimization and purpose limitation.

In the case of Tigo, there is a lack of clarity and internal contradictions regarding the scope of the contractual documents and privacy policies, while Personal's documents are underdeveloped and lack clarity. On the other hand, Starlink provides documents that are generally clear but lack adaptations to the Paraguayan context regarding the absence of local safeguards, which in turn limits their evaluation in terms of substantive compliance.

Judicial authorization

This analysis reaffirms a trend established in previous editions: Internet service providers do not consistently adopt a rights-protective stance regarding the requirement for a court order in relation to the processing of metadata.

While a court order is generally required to access the content of communications, in line with Articles 33 and 36 of the National Constitution and the Code of Criminal Procedure, this requirement does not extend (or does not clearly extend) to other types of data (connection logs, geolocation, etc.).

Furthermore, the analysis does not resolve the remaining ambiguities regarding the role of the Public Prosecutor's Office as the authority requesting the data and the tension this creates in relation to the principle of prior judicial review, which has been established both at the national level and through the case law of the Inter-American Court of Human Rights (Escher v. Brazil, CAJAR v. Colombia).

User notification

As in previous editions, the Internet service providers examined do not notify customers when their data is accessed.

This failure raises concerns regarding transparency and due process, and illustrates a misalignment with international standards that establish notification as a basic safeguard against violations of citizens' privacy.

Policies for the promotion and defense of human rights

Internet service providers' commitment to promoting human rights tends to be driven more by international corporate standards than by a concrete local commitment.

Tigo and Claro receive the highest scores on this indicator, thanks to their alignment with global standards and their membership in industry initiatives. However, no substantial actions and/or explicit public positions were identified at the local level, particularly with regard to privacy protection.

Personal receives an even lower score, as no initiatives of significant importance were identified in the region.

Transparency

The lack of transparency remains one of the main weaknesses observed among the ISPs analyzed. In Paraguay, only Claro and Tigo publish transparency reports on government requests for user data. These documents are prepared by the parent companies of both groups and represent significant progress in terms of accountability.

However, there are significant differences between them. América Móvil's report includes specific information on Paraguay, such as references to the applicable regulatory framework and breakdowns of different categories of requests, which allows for a more precise understanding of some of the company's practices in the country. In contrast, Millicom's report provides a more limited level of detail regarding Paraguay and presents information primarily from a regional perspective. Even so, in both cases, limitations persist due to the lack of comprehensive information on certain categories of data and on the specific criteria used to respond to requests from authorities, making it difficult to fully assess the extent of the companies' cooperation with government authorities and the safeguards they apply.

Starlink and Personal do not even publish transparency reports, indicating a complete lack of accountability.

Guidelines for requesting personal information

There is a notable distinction among ISPs regarding the existence of guidelines for authorities. Claro and Tigo have developed guidelines to some extent, thanks once again to the driving influence of their parent companies, but Personal and Starlink lack any kind of specific public guidelines, which has a negative impact on the predictability and transparency of data access procedures.

Accessibility

The accessibility analysis reveals significant variations among providers. Both Tigo and Starlink exceed expectations in terms of accessibility and are backed by technical evaluations. Claro has significant shortcomings, while Personal has poor accessibility and multiple structural flaws that undermine its user experience.

This criterion demonstrates that accessibility is not uniform and is determined by a company's technical priorities and how much it is willing to invest.

Data disclosure protocol for criminal investigations

The inclusion of this criterion allows for a better identification of structural deficiencies in the sector. In general, ISPs lack transparent, distinct and publicly available policies governing the disclosure of information in the context of criminal proceedings and a rights-protective interpretation of the right to privacy.

Claro and Tigo show some progress, but they do not establish formal rules regarding different types of data, nor do they make formal commitments regarding risks such as overly broad orders or disproportionate requests. In the case of Personal and Starlink, there is a complete lack of development in this area.

RECOMMENDATIONS

This assessment indicates that Internet service providers in Paraguay have made some progress; however, problematic practices persist regarding transparency, data protection and limits on state intervention. To address these issues, companies must improve their privacy policies to ensure they are clear, comprehensive and consistent, and align them with Law No. 7593/2025 and incorporate key aspects, such as data retention periods and the legal bases for data processing.

It is also important for them to adopt a stricter interpretation of the legal framework and ensure that content, metadata and all other forms of data are accessed only under judicial oversight and in accordance with the principle of proportionality. In this regard, the absence of notification mechanisms to users is one of the most significant shortcomings in this area. Therefore, it is recommended that efforts be directed toward developing such mechanisms as a minimum standard for transparency and due process.

Regarding transparency, Internet service providers should publish public reports, particularly regarding information on data requests received and responded to. Likewise, transparency also requires the development of protocols for the disclosure of data in criminal investigations, where differences in data types are clarified and abusive requests are rejected.

It is also recommended that guidelines be developed for authorities and that stronger internal processes be adopted for evaluating requests, as well as improvements in the accessibility of their digital platforms, ensuring access to information for all users.

Finally, ISPs should take on a more active role in promoting human rights through awareness-raising initiatives, participation in sector-specific forums and actions in response to improper requests. Ultimately, strengthening data protection in Paraguay depends not only on the regulatory framework but also on its effective implementation by companies, which requires a shift from a formal to a substantive approach to protecting the right to privacy.

BIBLIOGRAPHY

América Móvil. (2024). Sustainability Report 2024. https://sostenibilidad.americamovil.com/portal/su/pdf/Sustainability-Report-2024.pdf

América Móvil. (2025). Informe de transparencia en las comunicaciones 2025. https://sostenibilidad.americamovil.com/portal/su/pdf/Informe-de-Transparencia-de-las-Comunicaciones-2025.pdf

AMX Paraguay S.A. (n.d.-a). Políticas de Privacidad. Claro Paraguay. Retrieved April 26, 2026, from https://www.claro.com.py/personas/politicas-de-privacidad

AMX Paraguay S.A. (n. d.-b). Términos y Condiciones Mi Claro. Claro Paraguay. Retrieved April 26, 2026, from https://www.claro.com.py/personas/legal-y-regulatorio/mi-claro

AMX Paraguay S.A. (n. d.-c). Términos y condiciones: Servicio de Internet WiFi. Claro Paraguay. Retrieved April 26, 2026, from https://www.claro.com.py/personas/legal-y-regulatorio/servicio-de-internet-wifi

Banco Central del Paraguay. (2023, February 21). Resolución No 3/2023. https://www.bcp.gov.py/documents/20117/381887/Resolucion+3+acta+8%281%29.pdf/540aadf3-e563-4cee-f7f2-783b72cd4656?t=1742583379310

CONATEL. (2021, October). Plan Nacional de Telecomunicaciones 2021-2025 (PNT 21-25). https://www.conatel.gov.py/conatel/wp-content/uploads/2022/01/pnt21-25-1.pdf

CONATEL. (2024, September 20). Resolución N° 2583/2024 POR LA CUAL SE ESTABLECE LA OBLIGATORIEDAD PARA TODOS LOS LICENCIATARIOS DEL SERVICIO DE ACCESO A INTERNET Y TRANSMISIÓN DE DATOS DE CONSERVAR LOS REGISTROS DE CONEXIÓN. https://www.conatel.gov.py/conatel/wp-content/uploads/2024/09/resolucion-directorio-nro-2583-2024.pdf

CONATEL. (2025). Indicadores de mercado. Periodo 2025. https://www.conatel.gov.py/conatel/indicadores/

EFF. (2024, April 3). In Historic Victory for Human Rights in Colombia, Inter-American Court Finds State Agencies Violated Human Rights of Lawyers Defending Activists. | Electronic Frontier Foundation. https://www.eff.org/deeplinks/2024/04/historic-victory-human-rights-colombia-inter-american-court-finds-state-agencies

Global Network Initiative. (n. d.). Members. Global Network Initiative. Retrieved April 26, 2026, from https://globalnetworkinitiative.org/who-we-are/members/

GSMA. (n. d.). Our Members. Membership. Retrieved April 26, 2026, from https://www.gsma.com/get-involved/gsma-membership/our-members/

INE. (2024). Tecnología de la Información y Comunicación en el Paraguay 2024. https://www.ine.gov.py/Publicaciones/Biblioteca/documento/280/Tics%202024_INE.pdf

Human Rights Council , United Nations. (2016, June 27). The promotion, protection and enjoyment of human rights on the Internet . https://docs.un.org/en/A/HRC/32/L.20

Inter-American Commission on Human Rights. (2013, December 31). Special Rapporteurship for Freedom of Expression. Freedom of Expression and the Internet. https://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf

Inter-American Commission on Human Rights. (2025, September 7). Special Rapporteurship for Freedom of Expression. The Impact of Digital Surveillance on Freedom of Expression in the Americas https://www.oas.org/en/iachr/expression/reports/vigilanciarelecidh.pdf

Inter-American Court of Human Rights. (2009, July 6). Case of Escher et al. v. Brazil. Judgment of July 6, 2009. https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf

Inter-American Court of Human Rights. (2023a, October 18). Resumen oficial emitido por la Corte Interamericana. https://corteidh.or.cr/docs/casos/articulos/resumen_506_esp.pdf

Inter-American Court of Human Rights. (2023b,October 18). Case of Members of the "José Alvear Restrepo" Lawyers Collective (CAJAR) v. Colombia. Judgment of October 18, 2023 https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2025/07/corte-idh-caso-miembros-de-la-corporacin-colectivo-de-abogad_en.pdf

InternetLab. (2025). Quem Defende Seus Dados? https://quemdefendeseusdados.org.br/pt/

La Política Online. (2024, January 8). Tigo es víctima de un hackeo de su base de datos y se reaviva el debate sobre regulación en ciberseguridad—La Política Online. https://www.lapoliticaonline.com/paraguay/economia-py/tigo-es-victima-de-un-hackeo-de-su-base-de-datos-y-se-reaviva-el-debate-sobre-regulacion-en-ciberseguridad/

Millicom International Cellular S.A. (2023, June 30). Human Rights Policy. https://www.millicom.com/media/5601/mic-tpl-gov-policy-human-rights-policy_vf-june-16-002.pdf

Millicom International Cellular S.A. (2024). Law Enforcement Disclosure Report (LED). https://ww2-cdn.tigocloud.net/2024_LED_Report2_0b0376e254.pdf

Necessary and Proportionate. International Principles on the application of Human Rights to communications surveillance. (May, 2014). https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf

Personal Paraguay. (n. d.-a). Privacidad de datos. Personal Paraguay. Retrieved April 26, 2026, from https://www.personal.com.py/institucional/privacidad-de-datos.html

Personal Paraguay. (n. d.-b). Términos y Condiciones. Personal Paraguay. Retrieved April 26, 2026, from https://www.personal.com.py/institucional/terminos-y-condiciones.html

Personal Paraguay. (n. d.-c). Términos y condiciones de Aplicaciones de Personal. Personal Paraguay. Retrieved April 26, 2026, from https://www.personal.com.py/institucional/terminos-y-condiciones-apps.html

Presidencia de la República del Paraguay. (1989, August 8). Ley No 1 / APRUEBA Y RATIFICA LA CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS O PACTO DE SAN JOSÉ DE COSTA RICA. https://www.bacn.gov.py/leyes-paraguayas/2619/aprueba-y-ratifica-la-convencion-americana-sobre-derechos-humanos-o-pacto-de-san-jose-de-costa-rica

Presidencia de la República del Paraguay. (1992, June 20). CONSTITUCIÓN DE LA REPÚBLICA DEL PARAGUAY. Baccn. https://www.bacn.gov.py/leyes-paraguayas/9580/constitucion-nacional-

Presidencia de la República del Paraguay. (1995, December 29). LEY No 642/95 DE TELECOMUNICACIONES. https://www.conatel.gov.py/conatel/wp-content/uploads/2025/05/ley-nro.-642-95-de-telecomunicaciones.pdf

Presidencia de la República del Paraguay. (1998a). Código Procesal Penal de la República del Paraguay—Ley 1286/98.

Presidencia de la República del Paraguay. (1998b). LEY No 1286/1998 CÓDIGO PROCESAL PENAL DE LA REPÚBLICA DEL PARAGUAY. https://www.pj.gov.py/ebook/libros_files/codigo-procesal-penal.pdf

Presidencia de la República del Paraguay. (2013, March 1). LEY N° 4868 COMERCIO ELECTRÓNICO. https://www.bacn.gov.py/leyes-paraguayas/961/ley-n-4868-comercio-electronico

Presidencia de la República del Paraguay. (2014, January 27). Decreto No. 1.165/14 POR EL CUAL SE APRUEBA EL REGLAMENTO DE LA LEY No 4868 DEL 26 DE FEBRERO DE 2013 «DE COMERCIO ELECTRÓNICO». https://www.acraiz.gov.py/adjunt/Leyes%20y%20Decretos/decreto__1165_2014_ce0.pdf

Presidencia de la República del Paraguay. (2020, October 27). Ley No 6534/2020 DE PROTECCIÓN DE DATOS PERSONALES CREDITICIOS. Baccn. https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios

Presidencia de la República del Paraguay. (2021a, June 1). Ley No 6738 / ESTABLECE LA MODALIDAD DEL TELETRABAJO EN RELACIÓN DE DEPENDENCIA. https://www.bacn.gov.py/leyes-paraguayas/9582/ley-n-6738-establece-la-modalidad-del-teletrabajo-en-relacion-de-dependencia

Presidencia de la República del Paraguay. (2021b, December 30). LEY No 6822 DE LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS, DEL DOCUMENTO ELECTRÓNICO Y LOS DOCUMENTOS TRANSMISIBLES ELECTRÓNICOS. https://www.acraiz.gov.py/adjunt/Leyes%20y%20Decretos/Ley%20Nro%206822-2021pdf.pdf

Presidencia de la República del Paraguay. (2025a,November 27). Gaceta N° 287. https://www.gacetaoficial.gov.py/index/detalle_publicacion/93911

Presidencia de la República del Paraguay. (2025b, November 27). Ley No 7593/2025 / DE PROTECCIÓN DE DATOS PERSONALES EN LA REPÚBLICA DEL PARAGUAY. Baccn. https://www.bacn.gov.py/leyes-paraguayas/12924/ley-n-7593-2025-de-protecci-n-de-datos-personales-en-la-rep-blica-del-paraguay

Sequera. M (2024). Starlink in Paraguay: are there risks or concerns about this technology? TEDIC. https://www.tedic.org/en/starlink-in-paraguay-are-there-risks-or-concerns-about-this-technology/

SpaceX. (n. d.). Commitment to space sustainability. Retrieved from https://starlink.com/public-files/Commitment%20to%20Space%20Sustainability.pdf?srsltid=AfmBOoqpB5Q028-H-SxQqZ4xSmgt7_sfCiUnVSNilFMMvi8iml6zPidz&utm

SpaceX. (2024, April 1). SpaceX website privacy policy. https://www.spacex.com/assets/media/privacy_policy_spacex.pdf?

Starlink. (n. d.-a). Política de Uso Aceptable de Starlink. Starlink. Retrieved April 23, 2026, from https://starlink.com/legal/documents/DOC-1001-59234-61?regionCode=PY

Starlink. (n. d.-b). Política de Uso Razonable y Política de Gestión Del Tráfico. Starlink. Retrieved April 23, 2026, from https://starlink.com/legal/documents/DOC-1469-65206-75?regionCode=PY

Starlink. (n. d.-c). Términos de servicio de Starlink. Starlink. Retrieved April 23, 2026, from https://starlink.com/legal/documents/DOC-1526-27522-68?regionCode=PY

Starlink. (2026, January 15). Política de privacidad de Starlink. Starlink. https://starlink.com/legal/documents/DOC-1000-41799-67?regionCode=PY

TEDIC. (2017). ¿QUIÉN DEFIENDE TUS DATOS? 2017. https://qdtd.tedic.org/imagenes/pdfs/QDTD-2017.pdf

TEDIC. (2020). ¿QUIÉN DEFIENDE TUS DATOS? 2020. https://qdtd.tedic.org/imagenes/pdfs/QDTD-2020.pdf

TEDIC. (2022). ¿QUIÉN DEFIENDE TUS DATOS? 2022. https://qdtd.tedic.org/imagenes/pdfs/QDTD-2022_v2.pdf

TEDIC. (2024a). ¿WHO HAS YOUR BACK? 2024. https://www.tedic.org/wp-content/uploads/2025/02/QDTD_Paraguay_2024-ENG-WEB.pdf

TEDIC. (2025, November 28). The law on the protection of personal data in Paraguay: a collective achievement based on evidence and plural participation https://www.tedic.org/en/the-law-on-the-protection-of-personal-data-in-paraguay-a-collective-achievement-based-on-evidence-and-plural-participation/

Tigo Paraguay. (n. d.). Responsabilidad Corporativa. Tigo Paraguay. Retrieved April 26, 2026 from https://www.tigo.com.py/conocenos/responsabilidad-corporativa

Tigo Paraguay. (2025a, August 5). Politica de privacidad. Tigo Paraguay. Tigo. https://www.tigo.com.py/legales#terminos-y-condiciones-politica-de-privacidad

Tigo Paraguay. (2025b, August 5). Términos y Condiciones de Uso web. Tigo. Tigo. https://www.tigo.com.py/legales#terminos-y-condiciones-uso-de-web

Tigo Paraguay. (2025c, December). CONTRATO ÚNICO DE SERVICIOS DE TELECOMUNICACIONES. https://discovery-content-py.tigocloud.net/uploads/TIGO_Contrato_unico_diciembre_2025_final_2165d13302.pdf

United Nations. (1948, December 10). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations. (2006, December 12). Convention on the Rights of Persons with Disabilities https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities

United Nations. (2011). Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework. United Nations. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

United Nations. (2013, April 17). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40. https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

United Nations General Assembly. (2016, February 1). Resolution 70/125. Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. https://docs.un.org/en/a/res/70/125

United Nations Global Compact. (n. d.). Our Participants. Retrieved April 26, 2026, from https://unglobalcompact.org/what-is-gc/participants

WAI. (n. d.). Accessibility Principles from the Web Accessibility Initiative (WAI). W3C (World Wide Web Consortium). Retrieved from https://www.w3.org/WAI/fundamentals/accessibility-principles/

Web Accessibility Tool. (n. d.-a). Assessment results Claro Py. WAVE. Retrieved from https://wave.webaim.org/report#/https://www.claro.com.py/personas

Web Accessibility Tool. (n. d.-b). Assessment results Personal Py. WAVE. Retrieved from https://wave.webaim.org/report#/https://www.personal.com.py/

Web Accessibility Tool. (n. d.-c). Assessment results Starlink. WAVE. Retrieved from https://wave.webaim.org/report#/https://starlink.com/py

Web Accessibility Tool. (n. d.-d). Assessment results Tigo Py. WAVE. Retrieved from https://wave.webaim.org/report#/https://www.tigo.com.py/

Technology & Human Rights

ISBN 978-99989-999-5-4