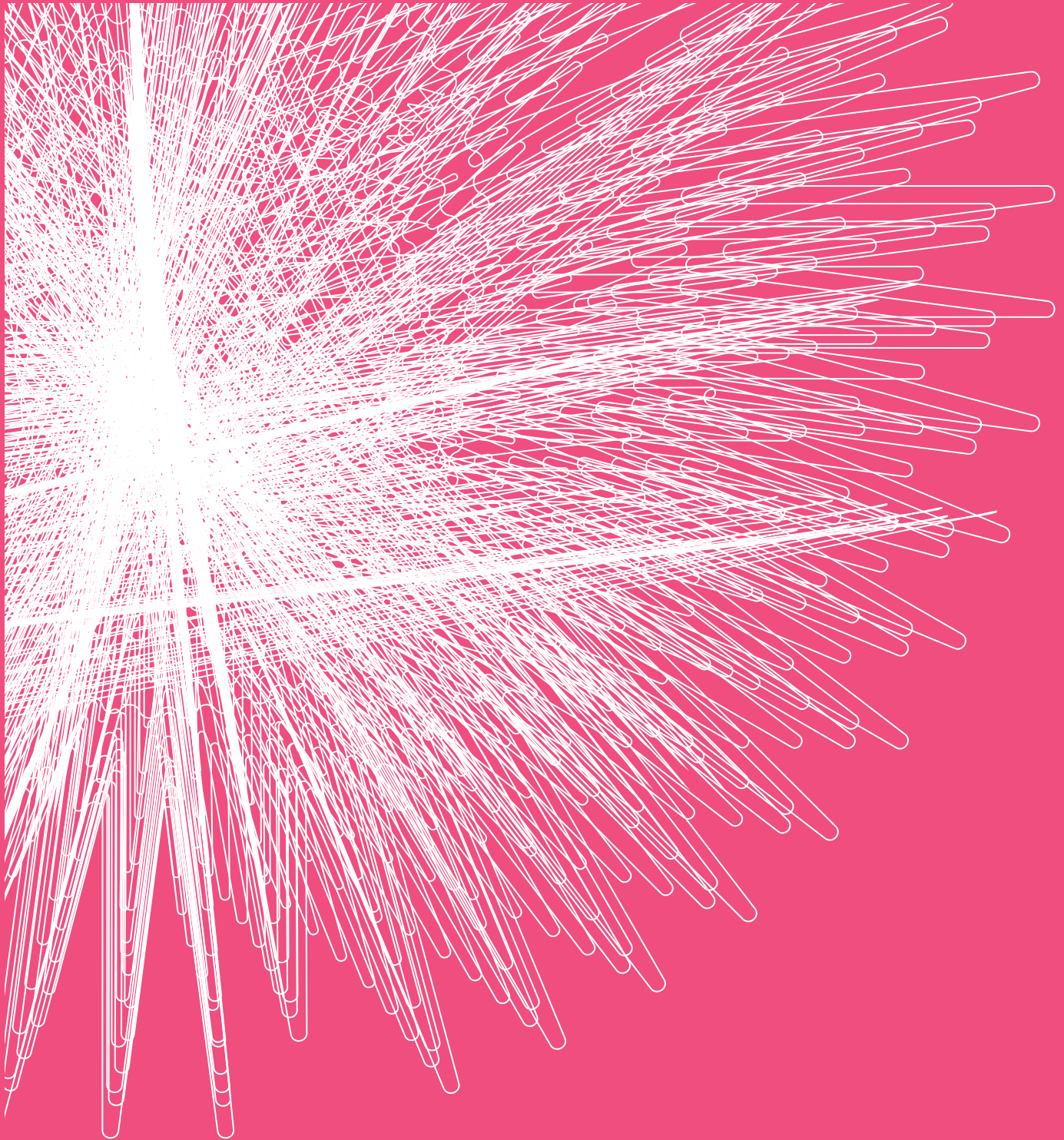


WHO HAS YOUR BACK?

Paraguay 2024



WHO HAS YOUR BACK?

Paraguay 2024

“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.

Electronic Frontier Foundation (EFF) is a leading international nonprofit digital rights organization. It works with technologists, activists, and lawyers to defend freedom of expression online, combat illegal surveillance, and advocate for users and innovation.

WHO HAS YOUR BACK? Paraguay 2024

JANUARY 2025

RESEARCH

Antonia Bogado
Maricarmen Sequera

COORDINATION

Maricarmen Sequera

COLLABORATION AND REVIEW

Veridiana Alimonti (EFF)

DESIGN AND LAYOUT

Horacio Oteiza

COMMUNICATION

Araceli Ramírez

Research available at:

<https://qdt.d.tedic.org>



This work is available under the Creative Commons Attribution 4.0 International (CC BY-SA 4.0) license:

<https://creativecommons.org/licenses/by-sa/4.0/deed.en>

This license allows for the distribution, remixing, adaptation, and creation of derivative works, even for commercial purposes, as long as credit is given and new creations are licensed under the same terms.

TABLE OF CONTENTS

INTRODUCTION	6
COMPARATIVE OVERVIEW	8
METHODOLOGY	9
NATIONAL CONTEXT	10
EVALUATION CRITERIA	20
REPORT FOR EACH ISP	29
REPORT - PRIVACY AND PERSONAL DATA PROTECTION POLICY	30
CLARO – AMX PARAGUAY S.A	30
COPACO S.A. - COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	32
PERSONAL - NÚCLEO S.A.	34
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	36
VOX - HOLA PARAGUAY S.A.	39
REPORT - JUDICIAL AUTHORIZATION	41
CLARO - AMX PARAGUAY S.A.	41
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	43
PERSONAL - NÚCLEO S.A.	44
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	45
VOX - HOLA PARAGUAY S.A.	47
REPORT - NOTIFICATION TO USERS	49
CLARO - AMX PARAGUAY S.A.	49
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A	50
PERSONAL - NÚCLEO S.A.	51
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	52
VOX - HOLA PARAGUAY S.A.	53
REPORT - POLICIES FOR THE PROMOTION AND DEFENSE OF HUMAN RIGHTS	55
CLARO - AMX PARAGUAY S.A.	55
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	57
PERSONAL - NÚCLEO S.A.	58
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	59
VOX - HOLA PARAGUAY S.A.	61
REPORT - TRANSPARENCY	63
CLARO - AMX PARAGUAY S.A.	63
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	65
PERSONAL - NÚCLEO S.A.	66
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	67
VOX - HOLA PARAGUAY S.A.	68

REPORT - GUIDELINES FOR REQUESTING PERSONAL INFORMATION	70
CLARO - AMX PARAGUAY S.A.	70
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	71
PERSONAL - NÚCLEO S.A.	72
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	73
VOX - HOLA PARAGUAY S.A.	74
REPORT - ACCESSIBILITY	76
CLARO - AMX PARAGUAY S.A.	76
COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.	78
PERSONAL - NÚCLEO S.A.	80
TIGO - TELEFÓNICA CELULAR DEL PARAGUAY S.A. (TELECEL S.A.)	82
VOX - HOLA PARAGUAY S.A.	84
CONCLUSION	86
RECOMMENDATIONS	89

INTRODUCTION

“Who has your back?” is an Electronic Frontier Foundation (EFF)¹ initiative. Although the methodology applied for this study differs from the one used in the United States, since the legal reality in Paraguay is notably different from that of the United States.

In its fourth edition, the project evaluated the same telephony and Internet service companies that had been evaluated in previous editions. Specifically, companies with a market greater than 15,000 customers nationwide were considered, including: COPACO², VOX³, PERSONAL⁴, TIGO⁵ and CLARO⁶.

The research in the framework of this project focuses on answering the following questions: How do Internet Service Providers (ISPs⁷) protect our privacy? How do they safeguard our personal data? Are there clear procedures in place for this? Do they actively participate in the defense of our rights in public debate forums?

Various reports and resolutions from the United Nations have emphasized the importance of Internet access as an indispensable tool for the full exercise of human rights, while at the same time contributing to achieving greater levels of social benefits and inclusion^{8, 9}. In this context, the recurrent evaluation of technology and telecommunications from a rights-based perspective becomes essential, as they are fundamental to our current form of interaction and communication, playing a crucial role in guaranteeing equitable access to information, social participation and global connectivity.

Since the previous edition, a small adjustment was made to allow the comparison of criteria at the regional level, a modification that remains in this research. A results table has been incorporated to compare the performance of companies in the different categories and evaluation criteria for the four editions of this research (2017¹⁰, 2020¹¹, 2022¹² and 2024). These are based on their public commitment to compliance with the law, the adoption of good practices favorable to Internet service users, transparency in their practices and policies, accessibility in their web platforms, among other aspects.

1 EFF official website: <https://www.eff.org>

2 COPACO <https://www.copaco.com.py>

3 Hola Paraguay - VOX <https://www.vox.com.py>. Authors' comments: It is important to note that in 2020, VOX was acquired by COPACO. Throughout the investigation, it is observed that both state-owned companies handle similar information and show a low level of compliance with the evaluated criteria.

4 PERSONAL – NUCLEO <https://www.personal.com.py>

5 TIGO – TELECEL <https://www.tigo.com.py>

6 CLARO- AMX Paraguay. <https://www.claro.com.py>

7 There is no public subscription data for the ISP Starlink to date. More information about this ISP can be found at: <https://www.tedic.org/starlink-en-paraguay-existen-riesgos-o-preocupaciones-sobre-esta-tecnologia/>

8 United Nations. : Human Rights Council. Resolution on the Promotion and Protection of Human Rights on the Internet. UN Doc. A/HRC/32/L.20. June 27, 2016. Available at: <http://www.ohchr.org/EN/HRBodies/HRC/Pages/Documents.aspx>; United Nations. General Assembly. 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. UN Doc. A/RES/70/125. February 1, 2016. Para. 9. Available at http://unctad.org/es/PublicationsLibrary/ares70d125_es.pdf.

9 United Nations (2011). Guiding Principles on Business and Human Rights. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf

10 Who has your back? 2017 Edition: <https://qtdt.tedic.org/imagenes/pdfs/QDTD-2017.pdf>









































11 Who has your back? 2020 Edition: <https://qtdt.tedic.org/imagenes/pdfs/QDTD-2020.pdf>

12 Who has your back? 2022 Edition: https://qtdt.tedic.org/imagenes/pdfs/QDTD-2022_v2.pdf

Each company was evaluated on the basis of the 7 categories outlined and justified in the evaluation criteria section, which were developed considering the requirements of the regulatory framework in force in Paraguay and international best practices in terms of privacy protection and personal data processing. For this evaluation, the service agreements, sustainability reports and other documents that were available on the companies' websites until January 2024 were analyzed. Press releases and specialized media on the subject were also evaluated.

With the preliminary results in hand, TEDIC contacted the companies and requested a review and comments on them, with special emphasis on the methodologies and results obtained up to May 2024. Finally, these comments and opinions of the companies were incorporated in the conclusion and corresponding scores.

COMPARATIVE OVERVIEW

Comparative overview								
ISP	Criteria							Percentage of compliance*
	Privacy Policy	Judicial Authorization	Notification to users	Policies for the promotion and protection of human rights	Transparency	Guidelines for requesting personal information	Accessability	
								55%
								14%
								41%
								73%
								5%

* The percentage calculation was made by considering the total number of criteria met by each ISP in relation to the total number of existing criteria (22 criteria in total), and the values were rounded up to the nearest whole number.

METHODOLOGY

This research focused on the analysis of the main telecom companies and Internet service providers in Paraguay: Vox, Copaco, Personal, Tigo and Claro. These firms provide their users with Internet, telephony, and television services, and some of them also offer electronic wallets, commonly known as mobile financial services. These companies were specifically selected from a total of 231¹³ Internet service providers in Paraguay, based on the criterion that they have a market of more than 15,000 customers nationwide. The information on the number of users for each company was obtained from the market indicator report published by CONATEL on its website¹⁴, updated until 2023.

Internet service providers collect data from their users for commercial purposes and to comply with legal regulations, and are responsible for the processing and use of this information. Based on this context, the research focused on a qualitative analysis of the privacy policies and other relevant documents of the aforementioned companies. This analysis was conducted within the framework of the seven categories defined in this research. The analyzed privacy policies act as guiding frameworks for the handling of information collected about users. These policies are intended to inform users about how their personal data are handled. In particular, they detail what data are collected, how they are obtained, their purpose, the limits of processing, the rights of users and how they can exercise them. They also specify with whom the data is shared and describe the data-sharing process.

The collected data were extracted from the privacy policies published in each company's website. However, sustainability reports published during the last 5 years were also analyzed. These reports were published by Millicom International Cellular S.A.¹⁵ and América Móvil¹⁶, the parent companies of Tigo and Claro, respectively.

Additionally, press articles were analyzed, and data was collected from sectoral or multi-sectoral organizations that promote respect for and protection of human rights in the business sector, such as the Global Network Initiative¹⁷, the Telecommunications Industry Dialogue¹⁸ or GSMA¹⁹.

After analyzing and contextualizing the data collected, with the corresponding justification for the criteria, the companies were scored in each of the categories listed below.

13 CONATEL. National Registry of Telecommunications Services. List of Internet and Data Transmission Service Licensees. Retrieved from https://www.conatel.gov.py/conatel/wp-content/uploads/2024/01/rnst_internet-tx-datos_5_enero_2024.pdf

14 CONATEL. Market Indicators. 2023 Period. Retrieved from: <https://www.conatel.gov.py/conatel/indicadores/>

15 Millicom. Annual Report 2023. Retrieved from: <https://www.millicom.com/media/5769/ar-2023-w-mic-sa.pdf>

16 América Móvil. Sustainability Report 2023. pp. 88-90. Retrieved from: <https://sustentabilidad.americamovil.com/portal/su/pdf/Informe-de-Sustentabilidad-2023.pdf>

17 Global Network Initiative. Retrieved from: <https://globalnetworkinitiative.org>

18 Telecommunications Industry Dialogue. Retrieved from: www.telecomindustrydialogue.org

19 GSMA Membership. Retrieved from: <https://www.gsma.com/membership/membership-types/operator-membership/>

NATIONAL CONTEXT

1. ACCESS AND CONNECTIVITY

In order to approach this research and apply the methodology designed, as well as to understand its approach and the results of this research, it is essential to contextualize ourselves within the national situation.

According to the National Statistics Institute (INE, its Spanish acronym)²⁰, in 2023, 78.1% (3,816,000) of the population used the Internet, out of which 76.9% (1,831,038) were men and 79.2% (1,985,009) were women. Based on the area of residence, 83.8% (2,593,093) of the urban population accessed the Internet, as opposed to 68.2% (1,222,954) of the rural population.

Regarding progress in connectivity indexes, it is worth mentioning that according to the National Telecommunications Plan Paraguay 2021-2025 (PNT 21-25)²¹, prepared by the National Telecommunications Commission²² (CONATEL, its Spanish acronym) in October 2021, significant progress has been made in recent years. In 2023, fixed broadband Internet penetration reached 14% per 100 inhabitants, an increase of 4% compared to 2022. On the other hand, mobile broadband Internet penetration was 84.4% in 2023, significantly higher than the 64.5% recorded in 2022. Although no updated data is reported as of 2024, these figures are of great importance for the national context, as they reflect the evolution of connectivity in the country.

The PNT 21-25 also points out that the predominant access technologies in fixed broadband by cable are currently HFC connections, followed by FTTX connections and finally ADSL²³ connections. This analysis allows for a more complete understanding of network capacity and efficiency in the country and could contribute to the formulation of strategies and policies to improve connectivity and ensure equitable and efficient access to telecommunications services at the national level.

The following tables show CONATEL's²⁴ data on fixed and mobile broadband, number of people accessing mobile Internet, as well as their gross income.

20 Government of Paraguay. (2024). Unified Public Information Portal. Public information request number 85665. <https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/85665>

21 National Telecommunications Plan 2021-2025 (PNT 21-25). Retrieved from <https://www.conatel.gov.py/conatel/wp-content/uploads/2022/01/pnt21-25-1.pdf>

22 Regulatory body for telecommunications in Paraguay.

23 PNT 21-25, p. 35.

24 Government of Paraguay. (2024). Unified Public Information Portal. Public information request number 85730. <https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/85730>

TABLE 1. Fixed broadband and Mobile broadband**FIXED BROADBAND INTERNET PENETRATION***

2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
1,4%	1,8%	2,0%	2,3%	2,7%	3,1%	3,6%	4,0%	4,8%	5,3%	7,8%	9,9%	10%	14%

* Fixed broadband subscriptions / population x 100

MOBILE BROADBAND INTERNET PENETRATION**

2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
S/D	9,5%	15,0%	20,9%	31,4%	43,6%	45,1%	46,4%	53,7%	60,31%	61,2%	63,5%	64,5%	84,4%

** Mobile broadband subscriptions / population x 100

Source: COPACO (2024).

TABLE 2. Mobile Internet users

SERVICE PROVIDER	MOBILE ACCESS TECHNOLOGY	DEC-19	DEC-20	DEC-20	DEC-22	JUN-23	DEC-23
TELECEL S.A.	SMARTPHONE - 3G	600.123	438.675	337.776	260.725	230.461	195.627
	FEATURE PHONE - 3G	73.744	25.653	26.599	18.887		
	MODEM / DATACARD - 3G	14.195	2.199	1.437	828		
	MODEM / TABLET - 3G	2.962	2.054	1.118	764	930	785
	SMARTPHONE - 4G	1.405.764	1.826.795	2.141.687	2.354.176	2.311.423	2.471.414
	FEATURE PHONE - 4G	57.355	33	26	24		
	MODEM / DATACARD - 4G	4.211	4.922	4.533	5.199		
	MODEM / TABLET - 4G	1.268	2.656	3.635	3.871	4.676	4.922
	FEATUREPHONES (GPRS)					111.463	108.029
	TABLETAS 2G					387	413
	SMARTPHONE - 2G					7.251	10.571
	Otros (Dongles)					81.915	85.489
	TOTAL TELECEL S.A.	2.159.622	2.302.987	2.516.811	2.644.474	2.748.506	2.877.250
NÚCLEO S.A	SMARTPHONES 4G/LTE	1.091.384	1.163.490	1.263.514	1.272.778	1.289.574	1.323.861
	SMARTPHONES 3G	157.471	89.052	51.014	32.496	25.622	20.910
	TABLETS 4G	1.338	1.851	3.007	3.235	3.476	3.273
	TABLETS 3G	2.262	1.468	835	535	450	362
	Featurephones (GPRS)						23.039
	Otros (Dongles)						113.552
	TOTAL NÚCLEO S.A.	1.252.455	1.255.861	1.318.370	1.309.044	1.319.122	1.484.997
AMX PARAGUAY S.A	SMARTPHONES 4G/LTE	765.988	828.217	811.335	842.469	9.612	882.987
	SMARTPHONES 3G	75.128	45.026	22.412	11.784	839.153	6.856
	TABLETS 4G	505	2.178	2.809	2.798	243	2.910
	TABLETS 3G	13	2.121	301	191	2.723	136
	TOTAL AMX PY S.A.	841.634	877.542	836.857	857.242	851.731	892.889
HOLA PARAGUAY S.A.	3G	42.994	-	-	-	16.580	16.524
	4G	17.029	-	-	-	570	564
	TOTAL HOLA PARAGUAY S.A.*	60.023	-	-	-	17.150	17.088

* Estimado en base a la evolución del año 2018

GRAND TOTAL Smartphones+Tablets	4.313.734	4.436.390	4.672.038	4.810.760	4.936.509	5.272.224
--	------------------	------------------	------------------	------------------	------------------	------------------

Source: CONATEL (2024).

TABLE 3. Gross income

CATEGORY	2019	2020	2021	2022	2023
FIXED-LINE TELEPHONY	₡ 237.477.501.909	₡ 184.099.712.051	₡ 159.548.131.244	₡ 107.846.752.601	₡ 18.609.789.900
MOBILE TELEPHONY (includes 3G mobile internet)	₡ 2.347.175.260.029	₡ 2.077.073.263.425	₡ 1.956.472.685.933	₡ 1.902.909.356.836	₡ 1.988.262.795.800
4G/LTE MOBILE INTERNET	₡ 1.207.241.636.012	₡ 1.118.258.524.407	₡ 1.300.359.257.326	₡ 1.500.443.071.163	₡ 1.645.006.517.200
FIXED INTERNET	₡ 1.239.386.495.561	₡ 1.297.025.979.759	₡ 1.512.569.906.432	₡ 1.612.103.123.142	₡ 1.498.272.574.100
CABLE DISTRIBUTION (Cable TV)	₡ 511.660.035.132	₡ 452.179.640.357	₡ 314.142.490.807	₡ 281.169.221.990	₡ 509.154.125.500
DTH (Satellite TV)	₡ 597.373.795.592	₡ 584.569.359.761	₡ 570.789.818.816	₡ 549.186.605.732	₡ 506.550.488.100
RADIO DISTRIBUTION (Paid UHF TV)	₡ 60.776.659.113	₡ 13.194.487.406	₡ 1.977.716.000		---
Total Paid Tv	₡ 1.169.810.489.837	₡ 1.049.943.487.524	₡ 886.910.025.623	₡ 830.355.827.722	₡ 1.015.704.613.600

Source: CONATEL (2024).

It is worth noting that the Ministry of Information and Communication Technology (MITIC, its Spanish acronym) in 2022 designed a National ICT Plan 2022-2030 (PNTIC, its Spanish acronym)²⁵ of Paraguay by which it proposes an ambitious digital transformation for full Internet access for the entire population, as well as the development of regulatory frameworks for other technologies. However, its implementation still faces certain limitations²⁶.

In international indicators, Paraguay ranks level 3 (score between 55 and 85) in the Global Cybersecurity Index 2024 prepared by the International Telecommunication Union (ITU)²⁷.

Regarding the gender digital divide indicators, the differences in the access and use of digital devices, Internet and other technologies are practically imperceptible²⁸. According to the data in Table No. 1, both the Internet usage indicator (UIT) and the combined mobile access and gender gap indicator (GSMA) reach a value of 1, reflecting a high level of equality between men and women in the technological sphere. In addition, most of the other indicators are also at outstanding levels.

25 MITIC (2022). National Plan for Information and Communication Technologies 2022-2030: Retrieved from: <https://mitic.gov.py/plan-nacional-de-tic-2022-2030/>

26 The PNTIC includes the need for sanctions, repair mechanisms, and evaluations based on human rights standards but lacks details on how these measures will be carried out and who will be responsible for overseeing them. The lack of concrete actions and clarity in execution raises doubts about the country's ability to address technological challenges, protect individuals' rights, and maintain digital competitiveness. A more coordinated and structured approach would be key to ensuring the ethical and effective adoption of ICT and reducing inequalities.

27 International Telecommunication Union (2024). *Global Cybersecurity index 2024. 5th Edición*. ISBN 978-92-61-38751-8 (Electronic version). https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

28 World Economic Forum. 2024. Global Gender Gap. <https://www.weforum.org/publications/global-gender-gap-report-2024/> In 2024, Paraguay obtained a score of 0.707 in the Global Gender Gap Index. This index, which assesses parity in 146 countries, measures progress toward gender equality across various dimensions: economic participation and opportunities, educational attainment, health, and political empowerment.

TABLE 4. Gender Digital Divide

INDICATOR	INDEX
Gender divide - Internet – Online	0,984
Gender divide - Internet – Offline	0,868
Gender divide - Internet – Combined	0,978
Gender divide - Internet – UIT	1
Gender divide - Mobile – Online	0,999
Gender divide - Mobile – Offline	0,94
Gender divide - Mobile – combined	1
Gender divide – GSMA	1

Source: World Economic Forum (2024).²⁹

As observed, CONATEL, MITIC and INE have the challenge of conducting updated connectivity studies so that access and connectivity policies are consistent with the needs and rights of users. These studies are essential to identify real gaps in access and use of digital technologies, as well as to understand the specific demands of various sectors of the population.

2. REGULATORY FRAMEWORK

For this study, it is essential to conduct a brief yet substantial analysis of the laws related to privacy and personal data protection of Internet users. This analysis should also include specific telecommunication regulations and other relevant legal instruments that directly influence the management and processing of users' information. These regulatory frameworks establish the obligations of service providers and the rights of users, providing the legal context in which this research takes place.

2.1. International legal framework

In the current international legal framework approved and ratified by Paraguay, instruments such as the Universal Declaration of Human Rights³⁰ and the American Convention on Human Rights³¹ protect the right to privacy and the inviolability of communications. The jurisprudence of the Inter-American Court of Human Rights (IACHR) has reinforced these protections, establishing relevant precedents for States parties, including Paraguay, in relation to the protection of privacy and State surveillance, as cited below:

29 Digital Gender Gaps. (2024). Brecha de género en el acceso a Internet de la UIT y combinada. <https://www.digitalgendergaps.org/>

30 United Nations, Universal Declaration of Human Rights. Recovered from https://paraguay.un.org/sites/default/files/2020-01/declaracion_universal_de_derechos_humanos_-_version_castellano.pdf

31 Law No. 1/1992, which approves and ratifies the American Convention on Human Rights or Pact of San José, 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-costica-rica>

Case Escher v. Brazil (2009)

This case, resolved by the Inter-American Court of Human Rights (IACHR) in 2009³², 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 grounds, extended beyond the permitted period and were leaked to the media.

The Court condemned Brazil 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 decision that both the content and metadata are protected under Inter-American human rights law:

114. As this Court has previously stated, although telephone conversations are not expressly provided for in Article 11 of the Convention, they are a form of communication included within the scope of protection of private life. Article 11 protects conversations conducted through telephone lines installed in private residences or offices, whether their content is related to the private affairs of the interlocutor, or to business or professional activity. Thus, Article 11 applies to telephone conversations regardless of their content and may even include both the technical operations aimed at recording such content -through listening and recording- and any other element of the communicative process itself. For example, the destination of outgoing calls or the origin of incoming calls, the identity of the interlocutors, the frequency, time and duration of the calls, aspects that can be verified without the need to record the content of the conversations. In short, the protection of private life is materialized in the right that parties other than the interlocutors do not unlawfully know the content of telephone conversations or other aspects, such as those already mentioned, inherent to the communication process.

Restrepo Case (CAJAR) v. Colombia (2023)

The Court issued a historic ruling against Colombia, holding the State responsible for a campaign of surveillance, harassment and persecution of members of the “José Alvear Restrepo” Lawyers’ Collective (CAJAR) for more than two decades^{33, 34}. These actions, which included threats and harassment, violated fundamental rights such as life, personal integrity, privacy, freedom of expression and association, especially affecting women human rights defenders and those who were forced into exile.

32 IACHR(2009) Judgment of July 6, 2009. Escher et al. v. Brazil Case. Full version: https://corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf

33 IACHR (2024) Official summary issued by the Inter-American Court. https://corteidh.or.cr/docs/casos/articulos/resumen_506_esp.pdf

34 IACHR (2024) Judgment of October 18, 2023. Case of members of the ‘José Alvear Restrepo’ Lawyers’ Collective Corporation vs. Colombia. Full version: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf

The decision sets a precedent as the first to hold a State responsible for violating the right to defend human rights. It also 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 the Colombian 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, setting key standards for intelligence activities in the region.

The Court highlighted that practices such as covert surveillance, interception of communications and collection of personal data constitute serious interference with human rights. These actions require clear regulations and effective controls to prevent abuses. Citing European jurisprudence, it underlined that even the existence of laws allowing secret surveillance represents 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 online users or locate electronic devices. It also covers access to sensitive metadata, such as emails, GPS locations, IP addresses and application data.

However, the Court did not clearly differentiate between targeted and mass surveillance, missing the opportunity to explicitly condemn the latter, leaving 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 life, 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 origin, use, retention time 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. In addition, any restriction on this right must be justified, limited in time and comply with 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 that the fact that documents belong to intelligence agencies is sufficient to classify them as confidential, demanding that restrictions be based on their specific content³⁵.

35 EFF (2024). In a historic victory for human rights in Colombia, the Inter-American Court declares that state agencies violated the human rights of lawyers defending activists. <https://www.eff.org/deeplinks/2024/04/historic-victory-human-rights-colombia-inter-american-court-finds-state-agencies?language=es>

Both rulings underscore the importance of protecting human rights, ensuring the protection of privacy and limiting State surveillance to prevent abuses. Paraguay³⁶, like many legislations in the Latin American region, provides less protection for metadata than for content. However, with these cases, and under the principle of conventionality, the Paraguayan State must implement measures to avoid massive and disproportionate surveillance, ensure the protection of personal data, provide judicial guarantees so that people, especially human rights defenders can carry out their work without fear of reprisals or arbitrary interference.

2.2. National legal framework

In addition to the aforementioned international legal framework in force, the Constitution of the Republic of Paraguay establishes specific provisions to protect the documentary and intrinsic privacy of individuals from third parties and from the authorities, except when public order is compromised. Among these provisions are the Right to Privacy (Article 33) and the Right to the Inviolability of Documentary Heritage and Private Information (Article 36). The latter becomes particularly relevant when analyzed in the context of Evaluation Criterion No. 2: Judicial Authorization.

The National Constitution also recognizes *Habeas Data* (Article 135) as a constitutional guarantee, ensuring individuals the right to access, rectify, request cancellation or oppose the processing of their data, among other rights. These provisions are essential complementary measures for the protection of personal data in the country.

It is important to note that, according to article 45 of the Constitution itself, the lack of legal regulation may not be invoked to deny or undermine rights or guarantees inherent to the human personality that are not expressly stated. This is particularly relevant in Paraguay, where there is still no general law on the protection of personal data. Although, in May 2021, a bill was presented in Paraguay known as the Personal Data Protection Law³⁷, which seeks to establish a comprehensive framework for the regulation of data handling and was recently approved in general by the Chamber of Deputies. However, its detailed study has been postponed until 2025, leaving the country, for the time being, without specific legislation on this matter.

The most direct current regulation in this regard is Law No. 6.534/2020 on the Protection of Personal Credit Data. This law, which repeals the previous Law No. 1.682/2001 and its amendments³⁸, establishes a new framework for the protection of personal data and information in Paraguay, placing more emphasis on addressing aspects related to the credit information of individuals, regardless of their nationality, residence or domicile, in banking and financial institutions and credit bureaus. Although this law is sector-specific, it provides relevant definitions on the subject, such as personal data and sensitive personal data, and complements other laws and provisions within the national regulatory framework.

36 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 IACHR. The country has been condemned by the IACHR in several cases, such as the case of the Yakye Axa Indigenous Community and others related to violations of the rights of indigenous communities and labor rights. These rulings have led to legal reforms and public policies to align the Paraguayan legal framework with international standards. Full version of the ruling: https://corteidh.or.cr/docs/casos/articulos/seriec_125_esp.pdf

37 For more information, visit the website of the Personal Data Coalition > <https://www.datospersonales.org.py>, and the Legislative Information System of Paraguay > <https://silpy.congreso.gov.py/web/expediente/123459>

38 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. Currently, this repeal has left a gap in the current regulations.

In the aforementioned regulatory context, it is important to highlight Resolution No. 3/2023 of the Central Bank of Paraguay and Resolution No. 1502/2022 of the Consumer Protection Secretariat, which regulate and complement the Law on the Protection of Personal Credit Data, in their role as enforcement authorities. These regulations not only define the procedures applicable to these entities regulated by the law, but also the mechanisms to guarantee the rights of data owners. Their importance lies in the fact that ISPs, when including the verification of creditworthiness in their contracts for the provision of Internet services, must comply with the standards established by the legislation in force on the treatment of information, considering the nature of these contracts.

In accordance with the aforementioned constitutional provisions, it is worth mentioning Law 642/95 “On Telecommunications”, which also guarantees the inviolability of the secrecy of correspondence and documentary property, except by court order (Article 89). This provision is applicable both to telecommunications personnel and to any person or user who has knowledge of the existence or content of such communications. In addition, the regulation specifies that inviolability implies the prohibition to open, subtract, interfere, change text, divert course, publish, use, try to know or enabling a third party to gain knowledge 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).

In the same sense, we must consider Law No. 4.868/2013 on Electronic Commerce and its complementary provisions, as well as Law No. 6.822/2021 on Trust Services for Electronic Transactions, Electronic Document and Electronic Transmissible Documents and its complementary provisions. According to Law No. 6.738/2021, which regulates teleworking in employment relationships, these regulations have a limited scope and do not comprehensively address the protection of data in the country.

The Electronic Commerce Law, in its Article 9, establishes that ISPs must comply with certain additional obligations, in addition to the current rules on Internet Access and Data Transmission Services established by the Competent Authority. These obligations include informing their customers permanently, easily, directly and free of charge about different technical tools that improve information security, such as protection against computer viruses and spyware, and the restriction of unsolicited e-mails. They must also inform about the tools available to filter and restrict access to unwanted content and services on the Internet or harmful to children and adolescents. The ISPs can comply with this information obligation by including the required information on their main webpage.

In the same line, the Regulatory Decree No. 1.165/14 of the Electronic Commerce Law, in its Article 11, establishes the Duty to Inform and Data Protection, indicating that the supplier of goods and services via electronic distance must inform the consumer or user about the purpose and processing of their personal data, in accordance with the current legislation on the matter. In addition, it must communicate who will receive the data provided and who will be responsible for the custody or storage of the information provided. It is also 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.

Given that there is still no Law on the Comprehensive Personal Data Protection, fragmented efforts for a proactive protection are also identified in some State institutions. For example, MITIC Resolution No. 733/2019 establishes an information security governance model to improve cybersecurity and risk management in the public sector.

Additionally, regulations such as Decree No. 8709/2018, which regulates the Information Exchange System (SII), include key principles such as purpose limitation, data minimization and ARCO rights (access, restriction, cancellation and opposition). This system handles both public and private data, as opposed to open data, which only covers public government information.

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

In relation to the criminal regulatory framework, Article 200 of the Criminal Procedure Code establishes that the interception of communications requires a well-founded resolution from the judge, regardless of the technical means used to obtain them. The result of the interception must be delivered solely to the judge who ordered it, who may request a written version of the recording and order the destruction of the entire recording or of those parts not related to the procedure, after they have been accessed by the Public Prosecutor's Office, the accused and their defense. The same legal body, in Article 228, grants the judge and the Public Prosecutor's Office the power to request reports from persons or public or private entities. These reports may be requested verbally or in writing, detailing the procedure, the name of the accused, the place of delivery of the report, the deadline for its presentation and the consequences for non-compliance.

These norms underline the exceptional nature of communication interception and the protection of these communications against the disclosure of their contents, in line with international and constitutional provisions that guarantee a protective approach in criminal legislation. Furthermore, although not binding, recent jurisprudence also highlights the importance of the court order as a requirement for the legality of the intervention, ensuring the safeguarding of the constitutional guarantee of the inviolability of private communication³⁹.

Likewise, it is worth mentioning that contracts for the acquisition of Internet services fall under the category of consumer contracts, and are therefore covered by Law No. 1.334/1998 on Consumer and User Protection, as amended. This legislation protects consumers against clauses established unilaterally by the supplier, without the possibility of modification by the consumer. In this context, it is relevant when assessing how ISPs protect users rights and considering aspects such as transparency in commercial practices, the resolution of claims or disputes and the rights of access to information.

CONATEL Resolution No. 2583/2024⁴⁰ establishes the obligation for all Internet access and data transmission services to retain connection records. This resolution seeks to record data traffic such as IP address (date and time of assignment and release of the address), in case of NAT (Network Address Translation) the corresponding private and public address mappings, as well as its mandatory storage of up to 6 months as a minimum period. Severe sanctions will be applied in case the ISP does not cooperate. However, the resolution does not specify which authorities are empowered to request and process this data, nor 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 possible violations of privacy rights and personal data protection.

39 CSJ, Criminal Chamber, Agreement and Judgment No. 777 of November 30, 2022, opinion of Minister Manuel Ramírez Candia.

40 CONATEL (2024). Board Resolution No. 2583/2024. Retrieved from <https://www.conatel.gov.py/conatel/resolucion-directorio-n-2583-2024/>

National jurisprudence has also addressed significant cases in the area of personal data protection, setting valuable precedents. A relevant case is the litigation filed before the Civil Chamber of the Supreme Court of Justice⁴¹, where an individual sued a financial institution for unauthorized disclosure of their financial and credit data. This case becomes important when examining service contracts between ISPs and users, as these contracts are usually standardized, with clauses similar to those in the aforementioned case. The resolution highlights the importance of the Consumer Protection Law, which requires that the clauses in these contracts be explicit and detailed, especially those related to data transfer.

In relation to the criterion of privacy and protection of personal data, especially regarding the storage, location and deletion of data, the pioneering decision of the Court of Appeals in Civil and Commercial Matters, Third Chamber of the Capital⁴² stands out. It addresses the concept of the right to be forgotten and distinguishes its scope from the right to the protection of personal data. It stresses that this right is not limited only to the protection of privacy, but also tackles the real risk of the creation and manipulation of detailed profiles, which could be used by third parties, especially organizations with various interests. Furthermore, it highlights the connection between the temporality of data and informational self-determination, being defined as variants of the right to privacy adapted to the information society. In essence, the right to be forgotten seeks to prevent the indiscriminate dissemination of personal data and information on the Internet when its publication lacks relevance or public interest.

The adoption of higher standards by the analyzed companies, which go beyond the requirements of national regulations and are often aligned with the practices of their international peers, such as the publication of transparency reports and privacy policies, stands out as a good practice that reflects their commitment to transparency. In terms of their participation in the public debate, four of the five ISP companies studied (TELECEL S.A., NÚCLEO S.A., AMX PARAGUAY S.A. and COPACO S.A.) were involved in the approval of the telecommunications user protection regulation together with the competent authority, CONATEL⁴³. However, so far, they have not issued opinions nor have they been involved in initiatives to strengthen the regulatory framework on personal data protection, indicating the need for greater involvement in privacy and data protection issues.

In summary, the legislation, public participation and specific regulations in Paraguay influence how telecommunications companies manage, among other aspects, the privacy and data protection of their users' data. This contextual understanding is important to accurately assess their performance and contribute to strategies that strengthen the protection of users' rights in Paraguay.

41 J.D.B. c. Itaú Bank on Compensation for damages and losses (Ac. and Sent. N° 89/2021)

42 R., L. G. and E. A., N. G. c. ABC Color and Ultima Hora s/ Hábeas Data (Ac. and Sent. N° 152) (PY/JUR/448/2021).

43 CONATEL, Resolution N° 871/2014. Retrieved from <https://www.conatel.gov.py/conatel/wp-content/uploads/2019/10/rd.530.2016-reglamento-proteccion-al-usuario.pdf>

EVALUATION CRITERIA

In this research, the evaluation consists of seven criteria, each with its corresponding parameters that allow analyzing the extent to which the companies comply or do not comply with each criterion. Among the criteria are: privacy policy and protection of personal data, judicial authorization, notification to users, policies for the promotion and defense of human rights, transparency, guidelines for requesting personal information and accessibility.

The criteria on “privacy policy” and “requirement of judicial authorization” are the only ones that contemplate currently applicable legislation, for the rest of the criteria there is no regulatory framework that addresses all the evaluated parameters. In this regard, the criteria will examine the implementation of best practices that have been developed at the international level -mainly from the initiative of the Electronic Frontier Foundation (EFF)- and that companies are willing to incorporate into their policies.

For this evaluation, service contracts, sustainability reports and other documents that were available on the companies’ websites up to March 5, 2024 were reviewed. News that circulated in the press and specialized media were also searched, and the reports from *Who Defends your Data* from previous years⁴⁴ were reviewed to verify updates and qualitative progress and to conduct a final comparison.

In the first stage, a preliminary evaluation was carried out in order to obtain a first score for each of the companies analyzed in this study and, thus, to understand in which parameters of each criterion they could improve in order to achieve a higher score. This process lasted 3 months and covered until April 30, 2024.

After the preliminary evaluation, TEDIC contacted the companies to request a meeting with the purpose of explaining what the study consists of and to present the preliminary results obtained from the 2024 analysis and its comparison over time with previous editions. In this meeting, the companies were asked to provide accurate information on their work to protect the privacy of users, as well as to complement the information that is publicly available or even to clarify any ambiguity that may arise from it.

All companies were contacted via email. This first step is considered fundamental to know the company’s perspective and give the opportunity to clarify any doubts regarding their privacy policies.

44 Available in: <https://qdt.tedic.org/#investigacion>

Each of the seven evaluation criteria for the companies are developed below:

1. PRIVACY AND PERSONAL DATA PROTECTION POLICY

ISPs have a privacy and personal data protection policy, using clear language and free of technicalities. It informs individuals about the collection, use, storage and processing of their personal data. In particular, this instrument should be seen as an opportunity to clearly inform users about their rights, rather than just a legal formality. ISPs also have a privacy policy in place regarding government authorities. It describes the legal procedure for handing over the data of its users to the justice in the event of a criminal investigation, upon request from the competent judge.

In this regard, both the Constitution of the Republic in its Article 33 -on the privacy of individuals- and international treaties protect the right to privacy as one of the pillars of modern democracies. Likewise, international organizations for the protection of Human Rights have pointed out that companies must establish and implement service conditions that are transparent, clear, accessible, as well as adhere to the international norms and principles of Human Rights; including the conditions under which interferences with users' privacy rights may occur⁴⁵. It is essential for ISPs to have policies that comply with these protocols when providing personal information and data to the authorities.

On the other hand, metadata are part of the communication and have the character of inviolability as stated in Article 36 of the National Constitution:

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

Companies must store the metadata of users for a minimum of 6 months according to Article 10 of the E-Commerce Law No. 4868/2013 and CONATEL Resolution No. 2583/2024 . In this scenario, it is essential that ISPs describe and disclose what personal information is being retained, as well as the measures in place to safeguard this data against possible attacks or risks that may affect such information.

In a contentious case⁴⁶ in which Brazil was condemned for the illegal use of wiretapping in criminal proceedings, the Inter-American Court pointed out that the right to privacy protects both the content of the electronic communication and other data pertaining to the technical process of communication, such as metadata or traffic data.

In the CAJAR v. Colombia case⁴⁷, the IACHR Court 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 autonomy as an autonomous human right, emphasizing that individuals have control over who accesses and uses their personal data. It also stressed that mass 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 spying techniques used by Colombia, which include the indiscriminate collection of personal information and access to non-public databases. It also stressed

45 IACHR. Special Rapporteurship for Freedom of Expression. Freedom of Expression and the Internet. December 31, 2013. OAS/ Ser.L/V/II, par. 112.

46 IACHR. Case Escher and others v. Brazil. Judgment of July 6, 2009 (Preliminary Exceptions, Merits, Reparations, and Costs), par. 114.

47 Inter-American Court of Human Rights. Case of Members of the 'José Alvear Restrepo' Collective Lawyers' Corporation vs. Colombia. Judgment of October 18, 2023. Full version: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf

the importance of clear standards in the collection and processing of metadata, stating that metadata contains sensitive information that can reveal people's habits, relationships and movements. As in the Escher case, this national jurisprudence places these data in an instance of constitutional and human rights protection.

The Ministry of Industry and Commerce is the institution responsible for the enforcement of the Electronic Commerce Law, which is responsible for the coordination of inspections and controls to the different ISPs. It must also apply sanctions for offenses not specifically provided for in the Consumer Protection Law and established in the E-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 that regulate the provision of personal data to State agents. These protocols should clearly define the forms and conditions of access to personal data in the context of investigations or similar actions. The existence of clear and public protocols, such as those adopted by several technology companies, is a key indicator of the company's commitment to privacy and the protection of its users' data. This aspect will be specifically addressed in criterion 6 of this research.

In this first criterion, therefore, as it is a matter of legal controversy, the issue is developed through different points which aim to discriminate against different levels of protection, clarity and commitment regarding access to data for investigations. The criteria seek to reflect the company's commitment to transparency concerning the authorities deemed competent, current regulatory disputes and limitations set out in the legislation (particularly regarding which investigations would be exempt from the need for a court order for access to registry data), as well as the commitment expressed in their guidelines on location data, connection records, and the publication of protocols for data delivery in judicial investigations.

Finally, in this edition, under this criterion, it is also considered whether companies comply with the provisions established regarding the notification of risk or leakage of personal data⁴⁸. It will be evaluated whether they have implemented mitigation actions and protocols for notifying the authorities in the event of security breaches that compromise the personal information of service users.

48 La Política Online. (2024) Tigo is a victim of a database hack, reigniting the debate on cybersecurity regulation. <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/>

2. JUDICIAL AUTHORIZATION

Surveillance without the person's consent entails risks of abuse by the authorities, therefore the authorization of a competent judge is essential. To request personal information there must be an authorization from the competent judge as expressed in the criminal law and the Constitution of the Republic of Paraguay. The interception of the private communication of individuals is exceptional in nature and is subject to the penalty of nullity in the trial. This criterion implies verifying whether the ISP has policies that comply with the protocols for delivering information to the judicial authority. That is to say, details of the criminal file, case number, data of the person, the type of criminal base that the investigated person incurs, legal argumentation and signature of the judge of the case.

The judiciary, both in individual and collective litigation, is an important space for the defense and consolidation of users' rights against abuses and illegal actions. With this in mind, we have tried to evaluate the position of companies in privacy and data protection lawsuits.

Article 36 of the National Constitution on the inviolability of communications obliges State authorities to request information from ISPs only through a duly justified court order.

Surveillance without consent entails risks of abuse by the authorities, which is why the authorization of a competent judge is essential. In order to request personal information there must be an authorization from the competent judge as expressed in the criminal law and the Constitution of the Republic of Paraguay. The following table explains the procedure for access in compliance with the standards of the principle of due process, as well as the applications of the Paraguayan criminal procedure code:



Due process for interception of information or access to personal data (Including metadata).

3. NOTIFICATION TO USERS

The ISP should have a notification policy for users affected by State surveillance measures, at the earliest time permitted by law. It must demonstrate that it has litigated legal or regulatory impediments to carry out the notification and publish in an accessible manner that it has promoted user notification mechanisms to Congress or other regulatory entities. Notifying users that their personal data or Internet connection records have been requested by administrative or judicial authorities provides a broad defense against abuses and irregularities.

In light of the constitutional principle of due process, many laws establish the duty to notify those affected of measures affecting their rights. For its part, 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 punishable act.

In the context of data requests, ISPs play a crucial role in protecting the due process rights of affected users. This is because, by notifying them of such requests, companies enable users to challenge unlawful 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 depend on the companies themselves to challenge requests that they consider abusive. If notified by the companies, users have the possibility of defending themselves against possible violations of their privacy. This right of notification to persons affected by surveillance measures has been recognized by specialists in Human Rights on the Internet and was embodied in a document called "Necessary and proportionate" and reads as follows:

It is impossible for individuals to effectively challenge government interference in their private life if they are unaware of being victims. Generally speaking, the lack of transparency regarding the application of laws governing covert surveillance can hinder meaningful democratic oversight of those laws.⁴⁹

On the other hand, the United Nations Office of the Special Rapporteur on Human Rights expressed its opinion in this regard:

Individuals should have the right to be notified that they have been subjected to surveillance of their communications or that their communications have been accessed by the State. By recognizing that prior or concurrent notification may jeopardize the effectiveness of the surveillance, individuals should in any event be notified once the surveillance has been completed and there is a possibility to seek appropriate redress for the use of communication surveillance measures.⁵⁰

49 "Necessary and Proportionate". International Principles on the application of Human Rights to communications surveillance. May version 2014. p 36

50 Report of the Special Rapporteur on the right to freedom of opinion and expression of the United Nations. April 17, 2013. A/HRC/23/40

The UN Special Rapporteur on Human Rights has emphasized that notification may not be carried out immediately as it could frustrate the success of an investigation, but should at least be made when an investigation is not at risk, there is no risk of flight, destruction of evidence or knowledge does not generate an imminent risk of danger to the life or integrity of any person. However, in Paraguay, the aforementioned legislation in force establishes that, in exceptional cases, judicial authorization may be requested for the interception of communications⁵¹, but there is no obligation to notify the person under investigation during this initial stage, except when an indictment is formalized and the alleged person responsible is identified.

In line with international human rights recommendations, ISPs have the responsibility to act in good faith to safeguard users' privacy. This includes notifying them of any interception of their communications, to the extent that such notification does not compromise the objectives of the criminal investigation. This practice also makes it easier for individuals to exercise their right to seek redress in the event that their rights have been improperly affected. In cases where the company's notification policy cannot be implemented, ISPs should judicially challenge legal impediments to notify affected users, at least after a reasonable time has passed so that the purpose of the surveillance measure is not frustrated. Another measure would be to carry out legislative or regulatory advocacy actions for the implementation of legal notification mechanisms.

In the context of requests for personal data, Internet providers take on an essential role in protecting the procedural safeguards of the users concerned. In other words, notification by the company enables the user to challenge unlawful requests: both unfounded court orders and requests by administrative authorities without competence or justification. In the current situation, users depend on the challenges made by the companies themselves against requests that they consider abusive. If users are notified, they obtain, as soon as possible, the ability to defend themselves against possible violations of their privacy.

With this in mind, it is important to encourage the practice of notifying users through the project "Who has your back?" (WDYD). In cases where data requests are not accompanied by the obligation of confidentiality, notification is permitted by Paraguayan law (given the absence of legal prescription to the contrary). The possibility of user notification 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 again put as a "premium", because notification is neither a legal obligation imposed on companies nor a generalized practice in Paraguay. It is a measure seen as innovative and to some extent expensive, as it requires staff dedicated to notifications. For these reasons, its adoption would reveal a special commitment to advancing the protection of users' rights. Notifying the user at the earliest legally possible opportunity, and preferably prior to disclosure of the data, collaborates with the principles of legal defense and fosters a culture of privacy protection.

51 Criminal Procedure Code (1998), Art. 200.

4. POLICIES FOR THE PROMOTION AND DEFENSE OF HUMAN RIGHTS

Public commitment and positions on public policies and national legislation affecting technology with a human rights perspective are decisive for the respect and protection of the human rights of users and for generating trust in the Internet ecosystem.

This parameter analyzes whether the ISP has a public institutional positioning in which it has recognized its responsibilities to respect and protect human rights, including the right to privacy. To this effect, it is analyzed if there is any positioning that complies with the characteristics indicated by Principle 16 of the Guiding Principles on Business and Human Rights approved by the Human Rights Council of the United Nations⁵² through resolution 17/4 of June 16, 2011, namely:

Political Commitment 16. In order to assume their responsibility to respect human rights, companies should express their commitment to this responsibility through a political statement that:

- a. Is approved at the highest management level of the company;
- b. Is based on internal and/or external expert advice;
- c. Sets out what the company expects, in relation to human rights, from its personnel, partners and other parties directly involved in its operations, products or services;
- d. Is made public and disseminated internally and externally to all personnel, partners and other stakeholders;
- e. Is reflected in operational policies and procedures necessary to instill the commitment made throughout the company.

In order to be considered, the policy position must be public and clearly reflect the company's commitment to respect human rights in the context of its business activities.

This criterion assesses whether the ISP has participated, either individually or collectively, in public legislative advocacy processes or before regulatory bodies, with the aim of defending the right to privacy. It is also analyzed whether it has carried out legal actions in defense of the privacy of its users.

It is also evaluated whether the company participates in any sectoral or multisectoral mechanism for the promotion, respect and protection of human rights within the scope of its business responsibilities, such as the Global Network Initiative⁵³ or the Telecommunications Industry Dialogue⁵⁴.

On the other hand, it is also considered that the ISP has policies for participation in local and international discussions on the Internet ecosystem; the Internet Governance Forums (IGF), where they openly discuss shared principles, norms, rules, decision-making processes and programs that shape the evolution and use of the Internet.

52 United Nations. (2011) Guiding Principles on Business and Human Rights > https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinessshr_sp.pdf

53 Global Network Initiative <https://globalnetworkinitiative.org>

54 Telecommunications Industry Dialogue www.telecomindustrydialogue.org

5. TRANSPARENCY

Principle 21 of the UN Guiding Principles on Business and Human Rights requires best practices from companies on transparency from a human rights perspective.

Transparency reports from the ICT sector regarding the impact on users' privacy have become more frequent in recent years⁵⁵. The publication of a transparency report on data access requests by security and justice authorities should provide sufficient information to assess the content and scope of surveillance measures by the authorities.

Transparency reports are statements issued by companies containing a variety of statistics related to data requests. Internet companies around the world have adopted the practice of publishing transparency reports to report how and when they cooperate with the government, generally because they are required to do so by law by disclosing information that can be used as evidence in civil and criminal cases. In itself this is already an established best practice among content companies such as Google, Facebook, X (formerly Twitter) and Microsoft and providers such as Vodafone, Verizon and Telefónica.

This criterion assesses the publication of statistics on how many requests for information have been received and fulfilled, as well as the inclusion of details on the type of requests, requesting institutions and the authorities' motivation and justification.

6. GUIDELINES FOR REQUESTING PERSONAL INFORMATION

IPs have guidelines, procedures or protocols oriented to law enforcement and other government agencies explaining how they should request personal information of clients, and what are the conditions for the delivery of such personal information.

This parameter differs from the publication of transparency reports, since the latter focuses on presenting statistical data on requests for information received and fulfilled. In contrast, the guidelines analyzed seek to evaluate how each company defines the procedures that law enforcement or investigative forces must follow to request information and what specifications they must comply with in this process. It is also examined whether the company, when establishing its rules for local authorities, considers the national context or adopts pre-defined guidelines of foreign origin. In the latter case, it is verified whether such procedures are stricter and better protect the privacy of its users. Some good examples

⁵⁵ The Implementation Guide for the UN Guiding Principles for the ICT (Information and Communication Technologies) Sector developed by the European Commission; the Implementation Guide of the Global Network Initiative; and the report 'Who has your back?' developed by the Electronic Frontier Foundation

are Telefónica⁵⁶, Entel⁵⁷, VTR⁵⁸ and Comcast⁵⁹ which have a list of requirements and global internal procedures for requests from local authorities.

ACCESSIBILITY

The accessibility of information available on the web, regardless of the disability or functional diversity of users, is essential to strengthen the commitment to transparency and guarantee respect for human rights. Article 9 of the Convention on the Rights of Persons with Disabilities⁶⁰ recognizes access to information and communication technologies, including the Web, as a basic human right.

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

The fact that ISPs in Paraguay have accessible data is part of broadening the commitment to transparency and respecting human rights. Designing websites and web tools that are accessible is crucial for Internet providers, as it enables more people to use and learn about their products and services in a skillful and satisfying way. Companies should 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 providers are evaluated by using the Accessibility⁶¹ principles guide of the Web Accessibility Initiative (WAI), part of the W3C (World Wide Web Consortium).

56 Telefónica 'defines the global internal procedure for requests from authorities according to each national legislation. The Principles governing the process are: Confidentiality, Exhaustiveness, Justification, Proportionality, Political Neutrality, Diligent Response, and Security' > <https://www.telefonica.com/wp-content/uploads/sites/7/2021/11/resumen-reglamento-peticiones-autoridades-competentes-19.pdf>

57 Entel, 2022 > <https://www.entel.cl/legales/centro-privacidad/public/pdf/guia%20solicitud%20judiciales.pdf?v=1592022.183832>

58 VTR, 2022 > <https://lla-cms-prod.directus.app/assets/683541ba-08f6-485f-8ae7-7fb0bdfa81e7.pdf>

59 According to its 2023 Transparency Report, Comcast warns that it is legally obligated to respond to requests for information made by government agencies, as long as they are legitimate. However, the company commits to protecting the privacy and rights of its customers by carefully reviewing each request. Before providing any information, Comcast states that it verifies that the request has a valid legal basis and is properly defined. If a request is legally questionable, unclear, inappropriate, or overly broad, Comcast will request clarification or reject it. Additionally, when a customer requests information about such government requests, Comcast generally tries to share that information, unless there are legal prohibitions, risks to ongoing investigations, individuals, or the safety and well-being of minors. See: Comcast. (2023). Transparency report. Retrieved from https://assets.xfinity.com/assets/dotcom/projects/cix-2605_irr-re-platform/2H2023%20Transparency%20Report.pdf; and, Comcast. (2022). *Guide for Law Enforcement*. Retrieved from https://assets.xfinity.com/assets/dotcom/projects/cix-4479_legal_documentation_sitecore_migration/Comcast%20Guide%20for%20Law%20Enforcement%20-%20August%202022.pdf

60 United Nations, Convention on the Rights of Persons with Disabilities > <https://www.un.org/esa/socdev/enable/documents/tcccon-vs.pdf>

61 Web Accessibility Principles Guide, Web Accessibility Initiative (WAI), part of W3C (World Wide Web Consortium) <https://www.w3.org/WAI/fundamentals/accessibility-principles/es>

REPORT FOR EACH ISP

CRITERION 1. Privacy and personal data protection policy





Does the evaluated ISP provide clear and complete information on the collection, use, storage, processing and protection of personal data of the user? Does it establish precisely what information about users and their communications is collected and stored, as well as the time period for which such data is stored?

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

Assessment criteria

- I. The ISP provides clear information and legal references on the collection of personal data, including what personal data is collected and in what situations the collection occurs;
- II. The ISP provides clear legal information and references on the use and/or processing of personal data, including the purposes for which it is used and how this process occurs;
- III. The ISP provides clear legal information and references on the storage of personal data, including how long the data is stored, as well as where it is stored and when it is deleted, if it is deleted;
- IV. The ISP provides clear legal information and references on personal data protection, including security practices observed in data retention procedures, whether there is a data anonymization policy, and who would have access to databases;
- V. The ISP provides clear legal information and references on the use of personal data by third parties, including information on the circumstances under which it would happen, and/or the need for customer authorization to do so;
- VI. This information is easily accessible on the ISP website.

Performance Standard:

Full star		The ISP complies with 5 to 6 criteria
Half a star		The ISP complies with 3 to 4 criteria
A quarter of a star		The ISP complies with 1 to 2 criteria
Empty star		The ISP does not comply with any of the criteria

REPORT - PRIVACY AND PERSONAL DATA PROTECTION POLICY



CLARO – AMX PARAGUAY S.A

Privacy and personal data protection policy		
	Yes	No
The ISP has a privacy policy	•	
The privacy policy clearly states which information about users and their communications is collected and stored	•	
The privacy policy specifies the duration for which the users' data is stored		•
The privacy policy outlines the reasons and procedures through which users' data are shared with third parties and authorities	•	
The ISP provides clear information and legal references regarding the use of personal data by third parties, including details on the circumstances and/or the need for client authorization to do so	•	
The privacy policy uses simple, non-technical language that is understandable for users. The policy is available on the company's website.	•	

Claro has a privacy policy accessible from its corporate website through a simple three-click process⁶². Significant progress has been evidenced in previous editions of WDYD. For example, in 2017 they did not have a privacy policy, limiting themselves only to a cookie policy. However, as of 2020, a privacy policy was added to their website. It is worth noting that for the 2022 report, there were no changes or updates in this regard. Unlike the 2022 edition, it was previously possible to consult the date of the last modification of the privacy policy. However, in the current revision this information is no longer available, even though the current policy expressly states that the date of the latest version will be provided.

The policy provides details on the types of data collected and ensures the non-manipulation of sensitive data. The data collected and stored includes personal identification, contact, reference, professional and/or property information. However, the policy does not specify how long the information will be stored. This gap may generate uncertainty among users, who could benefit from a clarification of the period during which their data will be retained by the company.

62 Claro. Privacy policies > <https://www.claro.com.py/personas/legal-y-regulatorio/politicas-de-privacidad>

In relation to the purposes of data use, the policy establishes both primary and secondary purposes. Regarding the latter, three reasons for their fulfillment are identified: marketing aimed at users; studies on consumption; and activities aimed at improving the services offered. The policy also highlights that users have the option to opt out of these secondary purposes, giving them the opportunity to contact the entity to request their removal.

The ISP explicitly mentions that it will share stored data with third parties for three specific reasons: user consent, external data processing and legal reasons. In addition, it states that information may be shared with companies outside Claro when it is necessary to comply with laws or to ensure compliance with obligations. The ISP establishes the obligation to notify its users before transferring personal information, although this notification will only be made in the context of mergers, acquisitions or sale of Claro's assets.

A noteworthy aspect is the inclusion of options to limit the disclosure of personal data, as well as the possibility to cancel or revoke consent for the processing of personal data. However, it is not clear whether these options only apply to the receipt of promotions from the company or cover other aspects related to the processing of users' data.

Finally, the privacy policy mentions that it fully complies with the laws related to the protection of personal data in the country, although it does not specify which laws specifically.

According to the established performance standard, Claro complies with 5 of the 6 criteria and therefore qualifies with one star.





COPACO S.A.

COPACO S.A. – COMPAÑIA PARAGUAYA DE COMUNICACIONES S.A.

Privacy and personal data protection policy		
	Yes	No
The ISP has a privacy policy		•
The privacy policy clearly states which information about users and their communications is collected and stored		•
The privacy policy specifies the duration for which the users' data is stored		•
The privacy policy outlines the reasons and procedures through which users' data are shared with third parties and authorities		•
The ISP provides clear information and legal references regarding the use of personal data by third parties, including details on the circumstances and/or the need for client authorization to do so		•
The privacy policy uses simple, non-technical language that is understandable for users. The policy is available on the company's website.		•

COPACO presents a privacy policy on its website that is limited exclusively to the use of its mobile applications⁶³. This observation has been noted since the previous editions, starting in 2020, and to date no significant adjustments or updates have been made to improve the privacy protection of users. Furthermore, compared to the previous edition, no obvious changes are identified in the previously analyzed privacy policy, nor is the date of its last update specified. Therefore, these general terms of use cannot be considered a comprehensive privacy policy that complies with the standards applicable to an ISP.

Regarding the second criterion referred to in the table, we note that the aforementioned privacy policy of this ISP does not specify which data will be collected by the official applications nor the duration of the storage of such information. This gap is consistent with the service provision contract available on the ISP's website⁶⁴. Although the confidential and private handling of users' personal data is mentioned in point 6.4, no additional details on the processing of this data are provided.

In relation to the transmission of data, COPACO expressly prohibits the transfer of data to third parties, except by court order. This clause states: "This company will not sell, assign or distribute the personal information that is collected without your consent, unless required by a judge with a court order." However, this restriction is limited to the use of official applications as specified at the beginning of the

63 General terms of use – Official APPs > <https://www.copaco.com.py/index.php/condiciones-apps.html>

64 COPACO. People and Home. Internet > <https://www.copaco.com.py/index.php/personas-y-hogares/internet/internet-adsl.html>

document: “This Privacy Policy establishes the terms in which Copaco S.A. uses and protects the information that is provided by its users and/or clients when using its official APPs”. Although the statement “This company will not sell” could be interpreted as a general prohibition of data transmission across the company, the scope of the policy is explicitly restricted to official apps, excluding information that could be obtained through other services such as telephony, Internet services and television.

In this context, the limited approach does not allow the assessment of the other privacy criteria set out in the performance standards and therefore an empty star is awarded because the ISP does not meet any of the criteria assessed.



PERSONAL - NÚCLEO S.A.

Privacy and personal data protection policy		
	Yes	No
The ISP has a privacy policy	•	
The privacy policy clearly states which information about users and their communications is collected and stored	•	
The privacy policy specifies the duration for which the users' data is stored		•
The privacy policy outlines the reasons and procedures through which users' data are shared with third parties and authorities	•	
The ISP provides clear information and legal references regarding the use of personal data by third parties, including details on the circumstances and/or the need for client authorization to do so	•	
The privacy policy uses simple, non-technical language that is understandable for users. The policy is available on the company's website.	•	

The company did not have privacy policies according to the 2017 and 2020 reports. This changed in 2022, although initially the policy was not available on its website. However, in the most recent edition of WDYD, it is highlighted that Personal now makes it easy to access its privacy policy with just one click, located at the bottom of its institutional website⁶⁵. The company mentions that this new version has been developed in accordance with Personal's global data protection policies and in strict compliance with applicable laws and regulations in Paraguay.

Regarding data collection and storage, the ISP details the types of data to be collected, stressing that they do not process information from individuals under 18 years of age. In addition, it provides information on the means through which the personal data of its users is obtained, mentioning available contact channels, the use of public sources and other technologies such as "cookies". A notable aspect is the reference to the consultation of credit information in companies or bureaus, with the granting of an irrevocable mandate for this purpose.

65 Personal. Data Privacy > <https://www.personal.com.py/institucional/privacidad-de-datos.html>

On the other hand, in the section on terms and conditions applicable to the ISP applications, such as Personal ID, Personal APP, Personal APP Store, My Personal WEB, My Personal Company Web, Personal Store - Ecommerce and Personal Wallet, the personal data that will be collected are more specifically detailed⁶⁶. This includes, in addition to those already mentioned, biometric data such as fingerprints, voice, facial image or others of a similar nature. In this section, the ISP clarifies that the collection of this sensitive data is done exclusively to validate identity in specific processes such as sales, after-sales or credit granting, with the aim of preventing illicit activities and allowing electronic authentication, if and when the user so chooses for certain products and services offered by Personal. Likewise, the ISP explicitly recognizes the rights of its users such as access, updating, rectification, deletion, opposition and portability of their data, among others. Detailed information is provided on how to exercise these rights, in accordance with the Privacy Notice and current legislation.

In relation to the third criterion, there is no information on the duration of data retention. Although it addresses the purposes of data processing, which include the provision of services, business objectives, compliance with legal requirements, improvement of services, determination of customer risk profiles, regulatory compliance, fraud and risk prevention, quality review, and improvement of application functionality, the retention period of such data is not specified.

In the fourth criterion, the ISP admits the possibility of delegating the custody and storage of data to third parties as well as sharing personal information of users with entities of its corporate group and third parties that provide services to it, especially in cases of merger, acquisition, sale of assets or transition of service. In addition, the ISP mentions that it may share data with jurisdictions that have data protection laws different from those of Paraguay, by court order or when permitted by law. The ISP also clarifies the power to provide debt information to credit information companies. Finally, it emphasizes that all communications and uses of personal data are protected against alteration, destruction or unauthorized access.

Regarding the fifth criterion, the ISP refers to Law 6534/2020 on “Protection of Personal Credit Data”, the current law on personal data protection in Paraguay. The ISP uses this law to support the rights of users to consult, access and rectify their personal data, oppose its use for advertising purposes, and other rights authorized by law. The ISP indicates that in case of conflicts, other laws in force in the country will be applicable for the interpretation, use, scope and termination of the privacy notice. Likewise, it mentions the Secretariat of Consumer and User Protection as the enforcement authority, in accordance with the provisions of Law 6534/2020.

It is worth highlighting the effort of this ISP in providing an accessible privacy notice unlike the previous edition of this research. Therefore, according to the established performance standard, Personal complies with 5 of the 6 criteria and therefore qualifies with one star.



66 Personal. Terms and Conditions of Personal Applications > <https://www.personal.com.py/institucional/terminos-y-condiciones-apps.html>



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

Privacy and personal data protection policy		
	Yes	No
The ISP has a privacy policy	•	
The privacy policy clearly states which information about users and their communications is collected and stored	•	
The privacy policy specifies the duration for which the users' data is stored		•
The privacy policy outlines the reasons and procedures through which users' data are shared with third parties and authorities	•	
The ISP provides clear information and legal references regarding the use of personal data by third parties, including details on the circumstances and/or the need for client authorization to do so	•	
The privacy policy uses simple, non-technical language that is understandable for users. The policy is available on the company's website.	•	

Tigo's privacy policy is easily accessible from the homepage of its website, located in the footer and just one click away⁶⁷. It is noteworthy that this ISP provides information on the dates of the updates of its policy, being the last update of this document on May 26, 2023.

This change is relevant because, according to reports in 2017, TIGO did not have a visible privacy policy on its website. What was available was found in the "Terms and conditions of use of the website", which applied exclusively to users browsing their portal. In contrast, for the 2020 edition, it was observed that TIGO already had a clearly accessible privacy policy, available even with a single click. In the 2022 edition, it was confirmed that this policy was still in force and corresponded to the version published on September 8, 2020.

⁶⁷ Tigo. Privacy Notice. Retrieved from <https://www.tigo.com.py/legales#terminos-y-condiciones-aviso-de-privacidad>

Regarding the second criterion, the privacy notice also states in detail the data to be collected, clarifying that they do not process information of individuals under 18 years of age. At this point it is important to note that Tigo offers a preview of its service provision contract on its website⁶⁸, updated as of May 25, 2023. This document addresses the issue of personal data collected in even more detail, including references to biometric data such as fingerprints, voice and facial recognition, although some parts use unclear terms.

It is relevant to remember that, being a standardized contract, the conditions are established unilaterally by the ISP, without giving users any margin to object in case they wish to use the service without providing sensitive data for processing. Therefore, it is important that the privacy notice be consistent with the personal data processing policy set forth in the contract. Although the ISP states that the notice will prevail over other terms and policies, including the contract, in case of conflict.

The reviewed privacy policy specifically details the means by which they collect information about their users, covering various contact channels, as well as mentioning the possibility of acquiring data automatically through the use of “cookies” or other technologies. However, it does not explicitly state the exact duration for which the personal data collected will be stored. Although the ISP mentions that it stores data “for the period of time that is necessary to fulfill the purpose for which it was collected, and as required by the local regulation in force,” it does not provide a clear specification regarding the specific time span.

In the 2017, 2020 and 2022 reports, it was highlighted that the data collection by the company was not clear, and the duration of data storage was not specified. While this practice partially complied with the E-Commerce Law by storing the information as required, it violated the regulations by sharing it for purposes not contemplated, such as criminal prosecutions. This shows a lack of significant progress in the implementation of proactive measures to protect the information and rights of users.

In relation to the fourth criterion, Tigo reports that it shares personal data with third parties for internal and external services, such as storage, collection and customer service. In addition, the company may share data with other Tigo entities or in situations such as mergers, acquisitions or sale of assets. It also mentions that it may transfer information to jurisdictions with protection laws different from Paraguay, under judicial authorization or in accordance with the law.

Regarding the fifth criterion, the ISP does not mention in the privacy notice the need for customer authorization to share data with third parties, however, it contemplates the possibility of revoking such authorization. However, it is necessary to mention that there is a discrepancy with the telecommunications services subscription contract. The latter document, in point 9.3. literal d), expressly states that users must authorize the provision of their personal data to third party service or product providers, business partners, affiliated entities and subsidiaries of the ISP, or companies of the same business group, both inside and outside Paraguay. In this regard, the ISP could facilitate a more transparent understanding of the terms related to the authorization of data to third parties.

68 Tigo. Telecommunications Service Subscription Agreement. Section 9. Retrieved from https://assets.tigocloud.net/j1bx-ozgharz5/3e69JpNDpIHw6aQGfNb2H/155811241e933df7960971d67e061f44/Contrato_De_Suscripci_n_De_Servicios_De_Telecomunicaciones.pdf?_ga=2.186110569.1774162512.1708956346-1194848194.1708361641&_gac=1.17007563.1708361669.CjwKCAiAlcyuBhBnEiwAOGZ2S8dv7pN2eQxjDb_7JnR2qXTMLfm_zEXJLR2kpqVL-JyZQDs8Nye-QBoCKUwQAvD_BwE

In the 2017 and 2020 editions, the criteria items were not as disaggregated and comparable as in the 2022 and current editions. However, it was noted that since 2022 there was no mention of the need for explicit authorization from the client to share data with third parties, although the possibility of revoking such authorization was contemplated. These points also show no substantial changes in relation to the current report.

Finally, although the privacy notice mentions legal references, this mention is generic. It establishes the applicability of Paraguayan laws to the use and interpretation of this, but does not specify which laws in particular. This same lack of precision had already been identified in the 2022 report, where the legal references were also general and limited to indicating the application of Paraguayan laws, without providing further details.

According to the analysis conducted for this edition, Tigo complies with 5 of the 6 criteria evaluated, which gives it a rating of one star. Although it is recognized that there has been some progress in certain aspects, the remaining challenges are still significant. The company must undertake substantial changes to ensure greater privacy protection and fully align itself with best practices in protecting the rights of its users.





VOX - HOLA PARAGUAY S.A.

Privacy and personal data protection policy		
	Yes	No
The ISP has a privacy policy		•
The privacy policy clearly states which information about users and their communications is collected and stored		•
The privacy policy specifies the duration for which the users' data is stored		•
The privacy policy outlines the reasons and procedures through which users' data are shared with third parties and authorities		•
The ISP provides clear information and legal references regarding the use of personal data by third parties, including details on the circumstances and/or the need for client authorization to do so		•
The privacy policy uses simple, non-technical language that is understandable for users. The policy is available on the company's website.		•

As in all previous editions of this research, this ISP lacks a privacy policy, which is neither available on its website nor could it be located through Internet search engines. Although it has a section called “My Data, My Security⁶⁹”, this is limited to providing basic recommendations on digital security.

Consequently, the ISP cannot be evaluated on the remaining criteria given the absence of relevant information on this aspect, and therefore scores zero stars.



69 Vox. Chembae. Retrieved from <https://www.vox.com.py/empresa/chembae>

CRITERION 2. Judicial authorization




Does the ISP commit to disclose customer information, metadata and communications content only in the presence of a court order?

This category assesses whether the ISP requires the authorities to present judicial authorization before disclosing data on the content of communications or their metadata. Whether the company, in its contract or any official document available to the public, clearly informs users about the circumstances under which judicial or administrative authorities may access their data.

Evaluation criteria

- I. The ISP commits to handing over data on the content of users’ communications to judicial authorities, subject to the existence of a prior court order;
- II. If it differentiates the delivery of data with respect to metadata and commits to do so whenever there is the existence of a prior court order.

Performance standard:

Full star		The ISP complies with all the criteria
Half a star		The ISP complies with one of the criterion
Empty star		The ISP does not comply with any of the criteria

REPORT - JUDICIAL AUTHORIZATION



CLARO - AMX PARAGUAY S.A.

Judicial authorization		
	Yes	No
The ISP commits to handing over data on the content of users' communications to judicial authorities, subject to the existence of a prior court order.		•
If it differentiates the delivery of data with respect to metadata and commits to do so whenever there is the existence of a prior court order.		•

Although Claro Paraguay mentions that it will share personal data for legal reasons, it does not clearly specify whether this is limited to court orders. For additional details on the service provided by this ISP and to evaluate this criterion, we reviewed the 2023 sustainability report provided by América Móvil⁷⁰, Claro Paraguay's parent company, which highlights its commitment to respect the privacy and security of users' communications, avoiding tapping, eavesdropping or monitoring.

In fact, in this 2023 sustainability report, the group states that before sharing information with authorities, it verifies that requests comply with legal requirements. It also reports that they received 810,956 requests, 97.26% were provided after verifying their compliance with legislation, and the remaining 2.74% were not processed due to non-compliance with regulations or other unspecified assumptions. It should also be noted that, in the aforementioned report, a link is provided to the Transparency in Communications Report⁷¹, which details the specific legislation on which América Móvil relies for the provision of data. In the case of Paraguay it is specified, among other issues, that the competent authorities for the delivery of data, blocking of telephone lines, geographic location and intervention in communications are the judges and the Public Prosecutor's Office indistinctly. However, the latter body lacks competence to issue judicial orders.

Regarding the first and second criteria, previous reports in 2017, 2020 and 2022 already evidenced practices similar to those observed in this 2024 period, reflecting a lack of significant progress in these critical areas. There continues to be a worrying lack of clarity in procedures related to the release of information under court order, particularly with regard to the handling of metadata.

70 América Móvil. Sustainability Report 2023. Pages 88-90. Retrieved from: <https://sustentabilidad.americamovil.com/portal/su/pdf/Informe-de-Sustentabilidad-2023.pdf>

71 América Móvil. Transparency in Communications Report 2023. Retrieved from: <https://sustentabilidad.americamovil.com/portal/su/pdf/2023-Informe-de-Transparencia-en-las-Comunicaciones.pdf>

Currently, this data is provided even at the request of the Public Prosecutor's Office, without adequate judicial oversight or a transparent process to ensure compliance with the principles of due process established in the Constitution. In fact, in the aforementioned Transparency Report, it can be observed that the ISP reported 4794 total requests per authority, out of which 4494 correspond to requests from the Prosecutor's offices and only 300 to the Judicial Branch. Likewise, they refer to have considered valid each and every one of these requirements⁷². This approach not only fails to comply with national standards, but also violates the provisions contained in judgments of the Inter-American Court of Human Rights, which are binding for our jurisdiction and require that any limitation to the right to privacy be duly grounded and supervised by the competent judicial authority.

The lack of alignment with these standards not only jeopardizes the fundamental rights of individuals, but also underscores the urgent need to implement structural changes in information management protocols. It is imperative to ensure that processes are clear, transparent and in line with international human rights principles and the country's legal obligations.

According to the established performance standard, Claro does not meet any of the established criteria as in the previous edition, so it does not have any star.



⁷² Ídem. Page 21



COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Judicial authorization		
	Yes	No
The ISP commits to handing over data on the content of users' communications to judicial authorities, subject to the existence of a prior court order.		•
If it differentiates the delivery of data with respect to metadata and commits to do so whenever there is the existence of a prior court order.		•

Although the ISP establishes an explicit commitment to hand over data on the content of a user's communications to the judicial authorities only when there is a prior court order, this commitment is expressed exclusively in the privacy policy that regulates the data collected and processed through its official applications. However, the privacy policy disclosed by COPACO does not specifically mention the telecommunications services it also provides, such as telephony and Internet. This does not necessarily imply that the same protection does not apply to the content of communications through these services, but the lack of an explicit reference in the online policy leaves this issue unclear.

As for the second criterion, under the conditions assessed, the ISP does not distinguish between the content of communications and metadata, so it has a negative rating.

The 2017, 2020 and 2022 reports already noted similar practices to those observed in 2024, reflecting a lack of progress. The lack of clarity in the delivery of information under court order persists, especially in the handling of metadata, which are delivered only at the request of the Public Prosecutor's Office, without adequate judicial supervision. This violates constitutional due process and the rulings of the Inter-American Court of Human Rights, which require transparency and judicial control. It is urgent to implement clear protocols aligned with international standards to protect fundamental rights.

According to the established performance standard, COPACO does not comply with any of the evaluated criteria, resulting in a rating with no star.



Personal

PERSONAL - NÚCLEO S.A.

Judicial authorization		
	Yes	No
The ISP commits to handing over data on the content of users' communications to judicial authorities, subject to the existence of a prior court order.		•
If it differentiates the delivery of data with respect to metadata and commits to do so whenever there is the existence of a prior court order.		•

The ISP reports that it may share a user's data by written order of a competent judicial authority or when permitted by law. However, it mentions other circumstances that indicate that a court order is not an exclusionary requirement for data disclosure.

In relation to the second criterion, the company does not make distinctions between the content of communications and metadata, i.e., it is not clear what type of data or content of communications is shared, resulting in non-compliance with both criteria.

The 2017, 2020 and 2022 reports already warned about the same practices identified in 2024, evidencing a lack of progress. The delivery of metadata is only done at the request of the Public Prosecutor's Office, without the required judicial oversight, in breach of constitutional due process and binding rulings of the Inter-American Court of Human Rights. It is necessary to adopt clear and transparent measures that respect international standards and guarantee the protection of fundamental rights.

On the other hand, it was identified that in the 2017 report, the Public Prosecutor's Office confirmed that a journalist of the ABC newspaper was subject to surveillance and evidence was found that the company Personal provided the data without due legal process⁷³. Although this case is specifically related to the telephony service and not to the company's Internet service, it is essential to highlight that the undue manipulation of metadata in telecommunications services violates our human rights and could be considered unconstitutional. In view of the seriousness of this fact, it is essential that Personal publicly issues a clear position on the matter.

According to the established performance standard, Personal does not comply with any of the established criteria, and therefore does not carry a star.



⁷³ Abc Color (2016). Government used its intelligence system to spy on journalist. <https://www.abc.com.py/edicion-impresa/notas/go-bierno-uso-su-sistema-de-inteligencia-para-espiar-periodista-1511976.html>



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

Judicial authorization		
	Yes	No
The ISP commits to handing over data on the content of users' communications to judicial authorities, subject to the existence of a prior court order.		•
If it differentiates the delivery of data with respect to metadata and commits to do so whenever there is the existence of a prior court order.		•

The ISP is committed to hand over data on the content of a user's communications to judicial authorities under various circumstances, not restricted only to a court order. This provision is reflected in the privacy notice, where Tigo refers that it can share personal data, presenting several options in a disjunctive manner and without requiring a court order as an exclusive requirement for the delivery of data in response to State requirements.

However, Millicom International Cellular SA, the parent company of Tigo Paraguay, highlights in its annual Law Enforcement Disclosure (LED) report that subsidiaries, including Tigo Paraguay, only hand over data on the content of communications under court order in Paraguay⁷⁴. It should be noted the difficulty in accessing this document, since it is not available on Tigo Paraguay's website, but only on Millicom's website.

On page 7 of the above-mentioned LED report, Millicom points out that in Paraguay, the authorities require direct access to the mobile network. The established procedures allow the company to verify the court order necessary to initiate the interception and to be aware of when it occurs. It notes that, in case of legal discrepancies, the company can file a complaint with the Supreme Court of Justice. However, according to this report, depending on the type of direct access, Tigo may not be notified in all cases of interception of customer communication. It also mentions that the actual written request received counts as one request in the data tables and one request may cover information on several persons or devices. Finally, the company states that it evaluates the legality of these requests before providing the requested information to the authorities.

In this document, three types of requests per authority are distinguished: interception of communications, Mobile Financial Services (financial services offered by the ISP, data on transactions and account activity) and metadata (IP addresses, message traffic, email, web browsing, location information). It is valuable that the parent company of Tigo Paraguay includes in its report information on the policy of

⁷⁴ Millicom International Cellular SA. 2023 Millicom Group Law Enforcement Disclosure (LED). Retrieved from: <https://www.millicom.com/media/5828/2023-led-report-20240402-2-2.pdf>

access to communications and establishes that the delivery of the content of the same is done exclusively by court order. However, it is imperative that such information be available in Spanish and accessible through the official website of the ISP in Paraguay, considering that this is the main channel of interaction with users in the national territory.

Transparency in this aspect is fundamental, since it involves an essential human right: protection against undue access to private communications by the authorities. For this reason, it is not possible to grant a positive evaluation in this criterion as long as Tigo Paraguay's privacy policy does not include an explicit and accessible statement that guarantees that access to the content of communications is only done under proper judicial authorization. This level of clarity and specificity is essential to comply with international human rights standards and to ensure user confidence in the company's handling of their data.

In response to the second criterion, the information provided by Millicom indicates that in Paraguay there are clear processes and specific requirements for judicial oversight of interception and requests for customer metadata. However, in the report, it is not clear who is granted access to this information, since, although it mentions who can request and issue interception orders, the distinction is not clear.

Regarding the first and second criteria, already in the previous editions of 2017, 2020 and 2022, the same practices identified in 2024 are observed. The lack of clarity in the delivery of information under court order persists, particularly with regard to metadata, which are provided only at the request of the Public Prosecutor's Office. This practice contravenes the standards of constitutional due process and the judgments of the Inter-American Court of Human Rights, which are binding for our jurisdiction. On the other hand, the company claims that most of the requests refer to the category of customer metadata, mainly to confirm the identity behind specific phone numbers. However, it is ambiguous whether such requests relate to tax requirements or court orders.

In summary, according to the established performance standard, Tigo does not comply with the established criteria and therefore does not obtain a star.





VOX - HOLA PARAGUAY S.A.

Judicial authorization		
	Yes	No
The ISP commits to handing over data on the content of users' communications to judicial authorities, subject to the existence of a prior court order.		•
If it differentiates the delivery of data with respect to metadata and commits to do so whenever there is the existence of a prior court order.		•

There is no accessible information available to determine whether the ISP hands over data, whether by court order or other method. Under the established performance standard, Vox does not meet any of the criteria, resulting in a no star rating.

As can be seen, the outcome of these companies' compliance with this criterion is troubling. Although Article 228 of the Code of Criminal Procedure grants the Public Prosecutor's Office the power to request reports from private entities, including ISPs, it is important to emphasize the primacy of specific regulations over general provisions in this analysis. In particular, Articles 198, 199 and 200 of the same code establish the need for a court order for any interception of communications. It is also essential to remember the exceptionality of such interventions, in accordance with the constitutional provisions that seek to safeguard the privacy of individuals. In addition, the Telecommunications Law and the judgments of the Inter-American Court of Human Rights (IACHR), which are of mandatory application thanks to the principle of conventionality, guarantee the protection of both the content and the existence of communications, including metadata.

The concern on this point, already expressed in previous editions, is reiterated. Contradictions and questionable jurisdictional practices in this area need improvement and should not be an excuse for ISPs to avoid rigorous scrutiny of requests for interception of communications.





CRITERION 3. Notification to users

To obtain a star in this category, companies must comply with at least one of the following actions: Have a policy that ensures notification to users affected by State surveillance measures as soon as permitted by law. Demonstrate that they have taken legal action to remove legal or regulatory impediments to such notifications. Demonstrate that they have promoted notification mechanisms before Congress or other regulatory bodies.

Evaluation Criteria

- I. The company is committed to notifying users before complying with requests for account information and connection records in cases not prohibited by legal confidentiality, or to issue a notification as soon as legally possible.

Performance Standard:

Full star		The ISP complies with the criterion
Empty star		The ISP does not comply with the criterion

REPORT - NOTIFICATION TO USERS



CLARO - AMX PARAGUAY S.A.

Notification to users		
	Yes	No
¿Does it notify users about the disclosure of personal data to third parties? The company is committed to notifying users before complying with requests for account information and connection records in cases not prohibited by legal confidentiality, or to issue a notification as soon as legally possible		•

Claro’s privacy policy does not state that the company is committed to notifying users before complying with data requests for account information and connection records, except in the case of a merger, acquisition or sale of assets. In the latter case, the ISP states that it will ensure confidentiality and notify affected users before the transfer of information or the implementation of a new privacy policy.

As we mentioned in the previous edition, the commitment to notify about the transfer of personal information is not sufficient, since the privacy policy allows transfers to third parties, both domestic and foreign, in various circumstances that go beyond the essential functions of the company. This includes transfers for the purposes of external processing, product or service promotion, and legal compliance, without detailing clear mechanisms for prior notification to users.

The lack of commitment to notify users about the use, request or sharing of their personal data has been a constant in all previous editions of this report. This omission reflects a gap in transparency and respect for the rights of users, evidencing the need to implement clear notification mechanisms that strengthen trust and comply with international standards.

According to the established performance standard, Claro does not meet the criterion and therefore does not obtain a star.





COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A

Notification to users		
	Yes	No
¿Does it notify users about the disclosure of personal data to third parties? The company is committed to notifying users before complying with requests for account information and connection records in cases not prohibited by legal confidentiality, or to issue a notification as soon as legally possible		•

The ISP in question does not refer to notifications to users and let's remember that the privacy conditions available on its website refer only to the use of the company's applications.

Since the first evaluations, it has been pointed out that there are no transparent policies or procedures in place to inform its users when their information is requested, used or shared, whether for legal requirements or for other reasons.

According to the established performance standard, COPACO also does not comply with the criterion and, therefore, does not obtain a star.



Personal

PERSONAL - NÚCLEO S.A.

Notification to users		
	Yes	No
¿Does it notify users about the disclosure of personal data to third parties? The company is committed to notifying users before complying with requests for account information and connection records in cases not prohibited by legal confidentiality, or to issue a notification as soon as legally possible		•

Personal does not comply with the criterion of notifying users of the disclosure of personal data to third parties. Although they have updated their privacy policy with respect to the previous edition of this research, it is still not observed that they refer to users' notification before complying with data requests for account information and connection records, as established by the performance standard.

In all previous editions of this report, the absence of a commitment from the company to inform users when their personal data is requested, used or shared has been highlighted. This lack of commitment is evidence of a lack of transparency that affects the trust of users and underscores the need to establish clear notification mechanisms aligned with international standards.

According to the established performance standard, this ISP does not obtain a star in this criterion.





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

Notification to users		
	Yes	No
¿Does it notify users about the disclosure of personal data to third parties? The company is committed to notifying users before complying with requests for account information and connection records in cases not prohibited by legal confidentiality, or to issue a notification as soon as legally possible		•

As observed in our previous edition, Tigo still does not address in its privacy notice the issue of notification to users before and/or after the release of personal data to third parties.

All previous editions of this report have highlighted the absence of clear measures to notify users about the handling of their personal data. This lack of transparency represents a key opportunity for the company, which could strengthen the trust of users by implementing notification processes aligned with international best practices.

According to the established performance standard, Tigo does not meet the criterion and therefore does not obtain a star.





VOX - HOLA PARAGUAY S.A.

Notification to users		
	Yes	No
¿Does it notify users about the disclosure of personal data to third parties? The company is committed to notifying users before complying with requests for account information and connection records in cases not prohibited by legal confidentiality, or to issue a notification as soon as legally possible		•

It is important to emphasize again that this ISP does not have data privacy policies, at least not publicly. Likewise, no other mention or reference is identified about notifications to users before complying with requests for account information and connection records in cases not prohibited by legal confidentiality.

Previous editions of this report have highlighted the company’s lack of commitment to notify users about the use or request of their personal data. This omission evidenced the need to adopt more transparent policies that reinforce user confidence and comply with international standards.

According to the established performance standard, Vox does not comply with the criterion and therefore does not obtain a star.



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

Has the ISP initiated a public position on the respect and promotion of human rights on the Internet, especially against mass surveillance or uncontrolled surveillance of communications?

This criterion analyzes whether the company has an institutional policy that recognizes 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 is also considered whether the company has intervened, individually or collectively, in public processes of legislative incidence or before regulatory entities to defend the right to privacy, as well as whether it has taken legal measures to protect the privacy of its users.

Likewise, it is evaluated whether the company carries out activities such as awareness campaigns, information days or advertising actions aimed at raising awareness of the importance of privacy and digital rights. This criterion seeks to measure the company's comprehensive commitment to privacy from different perspectives.

Evaluation criteria

- I. If the ISP promotes political or legal initiatives to protect the privacy of its users, for example, in Congress, through legislative bills or participation in hearings, or in the Courts;
- II. If the ISP carries out activities, conferences, advertisements or public reports in order to raise awareness in society about the right to privacy and/or the protection of personal data;
- III. If the company resists through judicial channels requests for information that are excessive and do not comply with legal requirements;
- IV. Participates in any sectoral or multi-sectoral mechanism for the promotion, respect and protection of human rights within the scope of its business responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).

Performance standard:

Full star		The ISP complies with 3 or all of the criteria
Half a star		The ISP complies with two of the criteria
A quarter of a star		The ISP complies with one criterion
Empty star		The ISP does not comply with any of the criteria

REPORT - POLICIES FOR THE PROMOTION AND DEFENSE OF HUMAN RIGHTS



CLARO - AMX PARAGUAY S.A.

Policies for the promotion and defense of human rights		
	Yes	No
If the ISP promotes political or legal initiatives to protect the privacy of its users, for example, in Congress, through legislative bills or participation in hearings, or in the Courts		•
If the ISP carries out activities, conferences, advertisements or public reports in order to raise awareness in society about the right to privacy and/or the protection of personal data.	•	
If the company resists through judicial channels requests for information that are excessive and do not comply with legal requirements.s.		•
Participates in any sectoral or multi-sectoral mechanism for the promotion, respect and protection of human rights within the scope of its business responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).	•	

On the first criterion, the ISP participated in the approval of the telecommunications user protection regulation with CONATEL, approved in 2016. Beyond this initiative, no other public political or legal actions seeking to protect the privacy of users have been identified within the legislative framework. There is also no indication that the company has judicially challenged requests for information that may be excessive or not in accordance with legal requirements.

Although the company has participated in consultations and public hearings related to personal data, harmful content on the Internet and cybersecurity, there has been no evidence of a defined public position on its impact on the drafting of these regulations.

The ISP does not present references to activities or contents that specifically address the protection of personal data on its website. However, in the code of ethics of América Móvil, to which the company adheres as a subsidiary and makes available on its website⁷⁵, it commits to protecting and respecting human rights, including awareness campaigns on these principles.

75 Claro. Code of Ethics > <https://landing.claro.com.ar/p/pdf/claro-codigo-etica.pdf>

Although no direct mentions were identified on the company's website, the sustainability report⁷⁶ also indicates that América Móvil provides certifications and training to its employees on issues related to the handling of personal data and digital security. Additionally, the subsidiary in Paraguay has launched a "Digital Security" campaign on its Instagram profile⁷⁷, presenting a Digital Security Guide for users, although the visibility of this information may be limited due to its availability on the social network. In that sense, we will consider the second criterion as complied, although we will recommend later on to improve certain specific aspects.

Regarding the last criterion, the ISP collaborates with other members of the sector and therefore scores positively. As part of GSMA (Groupe Speciale Mobile Association) initiatives, for example, it encourages telecommunications industry participants to report on emissions and set ambitious reduction targets. In addition, as part of its sustainability strategy, the company works with associations and organizations to achieve goals aligned with global initiatives such as the Sustainable Development Goals (SDGs), the Ten Principles of the Global Compact and the United Nations Business Ambition for 1.5 °C campaign. In Paraguay, it collaborates with various entities, including the Chamber of Mobile Operators of Paraguay (COMPy) and the Paraguayan Network of Inclusive Companies (RPEI).

According to the above, Claro meets two of the four criteria established, so it qualifies with half a star.



76 América Móvil. Sustainability Report 2023. Retrieved from <https://sustentabilidad.americamovil.com/portal/su/pdf/Informe-de-Sustentabilidad-2023.pdf>

77 Claro Paraguay. Retrieved from <https://www.instagram.com/claropy?igsh=MW0wcHM5a3RydXA4Nw==>



COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Policies for the promotion and defense of human rights		
	Yes	No
If the ISP promotes political or legal initiatives to protect the privacy of its users, for example, in Congress, through legislative bills or participation in hearings, or in the Courts		•
If the ISP carries out activities, conferences, advertisements or public reports in order to raise awareness in society about the right to privacy and/or the protection of personal data.	•	
If the company resists through judicial channels requests for information that are excessive and do not comply with legal requirements.s.		•
Participates in any sectoral or multi-sectoral mechanism for the promotion, respect and protection of human rights within the scope of its business responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).		•

COPACO has promoted initiatives on digital security issues on its website and social media under “Che mba’e: my data, my security”, providing educational content aimed at its users. In this context, criterion 2 is considered to be complied with.

However, there is no information that meets the other criteria. In the 2017 and 2020 editions, it was observed that COPACO actively participated in the Internet Governance Forums in its Paraguayan chapter. However, this participation ceased and no other actions related to governance or the defense of users’ rights were identified. Consequently, as it has 1 out of 4 criteria, it is rated with a quarter of a star.



PERSONAL - NÚCLEO S.A.

Policies for the promotion and defense of human rights		
	Yes	No
If the ISP promotes political or legal initiatives to protect the privacy of its users, for example, in Congress, through legislative bills or participation in hearings, or in the Courts		●
If the ISP carries out activities, conferences, advertisements or public reports in order to raise awareness in society about the right to privacy and/or the protection of personal data.	●	
If the company resists through judicial channels requests for information that are excessive and do not comply with legal requirements.s.		●
Participates in any sectoral or multi-sectoral mechanism for the promotion, respect and protection of human rights within the scope of its business responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).	●	

The company's website does not show a public commitment to the promotion and protection of human rights, a commitment that can be seen, for example, on the website of its international counterpart⁷⁸.

On the other hand, the ISP also collaborated in the approval process of the telecommunications user protection regulation with CONATEL in 2016. Beyond that initiative, no other public political or legal initiatives were found to protect the privacy of users before the Legislative Branch. Neither is it observed that the ISP refers to having resisted through the courts to excessive requests for information or that do not comply with legal requirements. Although it has participated in consultations and public hearings on regulations related to personal data, harmful content on the Internet and cybersecurity policies, no clear public positions in favor or against these regulations have been found. This lack of public positioning could be interpreted as a lack of active commitment to defend the privacy and digital rights of its users.

Likewise, there is evidence of efforts aimed at educating and training society on issues related to personal data protection and digital security⁷⁹. The company is also a participating member of the GSMA initiative⁸⁰. Thus, as in the previous edition, it complies with the second and fourth criteria, so it scores half a star.



78 TELECOM Argentina. Retrieved from <https://institucional.telecom.com.ar/sustentabilidad>

79 Personal. Blog. Retrieved from <https://blog.personal.com.py>

80 GSMA. Memberships. Retrieved from <https://www.gsma.com/get-involved/gsma-membership/our-members/>



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

Policies for the promotion and defense of human rights		
	Yes	No
If the ISP promotes political or legal initiatives to protect the privacy of its users, for example, in Congress, through legislative bills or participation in hearings, or in the Courts		•
If the ISP carries out activities, conferences, advertisements or public reports in order to raise awareness in society about the right to privacy and/or the protection of personal data.	•	
If the company resists through judicial channels requests for information that are excessive and do not comply with legal requirements.s.	•	
Participates in any sectoral or multi-sectoral mechanism for the promotion, respect and protection of human rights within the scope of its business responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).	•	

It is noteworthy that the company Tigo has had public participation in various legislative initiatives related to technology. According to the 2017 and 2020 reports, Tigo was part of legislative analysis groups focused on the “Protection of children and adolescents against harmful content on the Internet” law. Likewise, the company collaborated in working groups for the development of the National Cybersecurity Plan. In addition, Tigo is listed as one of the ISPs that actively participated in the approval process of the telecommunications user protection regulation in conjunction with CONATEL in 2016. Likewise, the ISP reports that, as part of its social commitments, it collaborates with CONATEL and the National Government to expand connectivity to all parts of the country⁸¹. However, no political or legal initiatives aimed at protecting the privacy of its users were identified before the Legislative Branch regarding 2023 and 2024.

Although Millicom⁸² highlighted its priority for 2024 to increase its involvement with the authorities of the different countries in which it operates to contribute to the definition of, for example, clear, transparent and effective surveillance laws with adequate guarantees, it remains to be assessed whether this priority was also reflected in the subsidiary Tigo Paraguay.

81 Tigo. Social Commitments > <https://www.tigo.com.py/conocenos/compromisos-sociales>

82 Millicom. Report LED Millicom 2023. page 15.

Regarding the second criterion, in the 2023 annual report⁸³ Millicom claims that both the group and its subsidiaries, following the principles of the United Nations and other international standards, actively promote human rights, including privacy and freedom of expression. This is also evidenced on Tigo Paraguay's website, in the corporate responsibility section⁸⁴. It is also noted in the 2020 and 2022 reports that it participates in the UN Global Compact, as well as the Telecommunications Industry Dialogue. In addition, it has specific initiatives, such as "Conectadas" and "Maestros conectados" aimed at training women entrepreneurs and teachers of the country in digital tools.

Regarding the third criterion, it is worth mentioning that in the aforementioned sustainability report 2023, Millicom reports that it implements measures to assess the legality of requests for information before providing it to the authorities and has mechanisms to file complaints before the Supreme Court of Justice in case it considers that the orders or interceptions do not comply with legal requirements.

As for the fourth criterion, the ISP is also involved in the GSMA⁸⁵, a global organization that drives innovation in the mobile ecosystem to foster positive business environments and social change.

In the 2022 report, Millicom's presence as a member of the Global Network Initiative (GNI) was highlighted; however, as of 2023, this company decided to withdraw and focus only on the GSMA.

In sum, it is observed that this ISP meets three of the four criteria established in the performance standard, which merits a one-star rating.



83 Millicom. Annual Report 2023. Retrieved from: <https://www.millicom.com/media/5769/ar-2023-w-mic-sa.pdf>

84 Tigo. Corporate Responsibility. Retrieved from <https://www.tigo.com.py/conocenos/responsabilidad-corporativa>

85 GSMA. Memberships. Retrieved from <https://www.gsma.com/get-involved/gsma-membership/our-members/>



VOX - HOLA PARAGUAY S.A.

Policies for the promotion and defense of human rights		
	Yes	No
If the ISP promotes political or legal initiatives to protect the privacy of its users, for example, in Congress, through legislative bills or participation in hearings, or in the Courts		•
If the ISP carries out activities, conferences, advertisements or public reports in order to raise awareness in society about the right to privacy and/or the protection of personal data.		•
If the company resists through judicial channels requests for information that are excessive and do not comply with legal requirements.s.		•
Participates in any sectoral or multi-sectoral mechanism for the promotion, respect and protection of human rights within the scope of its business responsibilities. (Examples: Global Network Initiative, Telecommunications Industry Dialogue, Global Compact).	•	

Vox only meets the last of the three criteria observed as it participates in the GSMA initiative⁸⁶, complying with one of the four criteria. The previous editions of this research were also analyzed and there was no evidence of participation or public actions in defense of the rights of users. Consequently, it qualifies with a quarter of a star.



⁸⁶ GSMA. Memberships. Retrieved from <https://www.gsma.com/get-involved/gsma-membership/our-members/>

CRITERION 5. Transparency




Does the ISP publish transparency reports that contain 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 for blocking or removing of content from the Internet - including child pornography, copyright infringement, compliance with their own policies, etc. While ISPs in Paraguay are under no obligation to produce active transparency reports, this could be a window of opportunity to show that they are concerned about building trust in their relationships with customers, based on transparency.

Evaluation criteria

- I. The ISP publishes transparency reports so that the user can learn about collaboration with government authorities on the data provided;
- II. The ISP publishes transparency reports informing about collaboration with government authorities, indicating:
 - a. the number of requests and disclosures classified by type of data - whether it is account information or connection of records;
 - b. the number of requests and disclosures categorized by the government authority that made the request;
 - c. the number of requests and disclosures classified by the motivation alleged by the government authority - presentation of evidence in civil, criminal, or administrative cases, etc.

Performance standard:

Full star		The ISP complies with both criteria
Half a star		The ISP complies with one of the criteria
Empty star		The ISP does not comply with any of the criteria

REPORT - TRANSPARENCY



CLARO - AMX PARAGUAY S.A.

Transparency		
	Yes	No
The ISP publishes transparency reports so that the user can learn about collaboration with government authorities on the data provided.	•	
The ISP publishes transparency reports informing about collaboration with government authorities, indicating: a) the number of requests and disclosures classified by type of data - whether it is account information or connection of records; b) the number of requests and disclosures categorized by the government authority that made the request; c) the number of requests and disclosures classified by the motivation alleged by the government authority - presentation of evidence in civil, criminal, or administrative cases, etc.		•

Just like in the previous edition, Claro Paraguay continues to lack specific reports on its collaboration with government authorities. On the other hand, it is worth noting that there is an agreement in 2018 with the Supreme Court of Justice⁸⁷, establishing technological mechanisms for access to information generated by AMX Paraguay, this information is not on the ISP website, and there are no details on the validity of the agreement.

The main difficulty lies in the fact that the relevant information can only be obtained through the Sustainability Report available on the América Móvil website, which requires consulting the parent company's website, as it is not accessible on the subsidiary's website. Despite this limitation, this report is the only source of information available to evaluate the ISP in this criterion, so we will consider what is presented therein.

In its Transparency in Communications Report 2023⁸⁸, cited above, América Móvil reports that its subsidiary in Paraguay is obliged to cooperate with national security and law enforcement authorities by virtue of constitutional provisions and other laws and regulations. Additionally, unlike previous years, the parent company indicated that the subsidiaries received 810,956 requests in its subsidiaries, including a breakdown of the information by country. In this sense, the first criterion is considered fulfilled.

87 Judicial Branch. News. March 12, 2018 > <https://www.pj.gov.py/notas/15105-convenio-entre-amx-paraguay-y-la-corte-suprema-de-justicia>

88 América Móvil. Transparency Report on Communications 2023. Retrieved from <https://sustentabilidad.americamovil.com/portal/su/pdf/2023-Informe-de-Transparencia-en-las-Comunicaciones.pdf>

A significant progress of this company is evident when comparing the first editions of WDYD with the most recent ones. In the first and second editions, relevant information was not included, not even on the parent company. However, starting with the 2022 reports, América Móvil began to publish transparency reports on its subsidiaries in Latin America. These publications are presented in regional blocks, and as of 2023, the number of requests by country is also detailed.

The company does not comply with the second criterion either, since the only report found does not detail the cooperation with the government. Considering this performance, the ISP should be rated with half a star, as it meets one of the evaluated criteria.





COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Transparency		
	Yes	No
The ISP publishes transparency reports so that the user can learn about collaboration with government authorities on the data provided.		•
The ISP publishes transparency reports informing about collaboration with government authorities, indicating: a) the number of requests and disclosures classified by type of data - whether it is account information or connection of records; b) the number of requests and disclosures categorized by the government authority that made the request; c) the number of requests and disclosures classified by the motivation alleged by the government authority - presentation of evidence in civil, criminal, or administrative cases, etc.		•

The ISP does not comply with any of the established criteria. It does not publish transparency reports detailing collaboration with government authorities, classification by type of data, the requesting authority and the alleged motivation.

COPACO provides on its website a list of governmental entities with which it has entered into agreements until 2022⁸⁹, including the Supreme Court of Justice, the Judicial Branch and the Public Prosecutor's Office. However, it is not possible to access further details on the scope of these agreements, making it impossible to consider this information to evaluate criterion number one. Additionally, in the news section of its website and through Google searches, there is recent information about agreements with government entities such as the National Electricity Administration (ANDE)⁹⁰ and the National Directorate of Migration⁹¹, but these seem to focus more on improving connectivity than on the exchange of information or personal data of its users. Nor do the previous editions of WDYD show that this company has ever complied with this criterion.

In conclusion, COPACO does not meet any of the established criteria, so it does not receive a star for the transparency criterion.



89 COPACO. Institutional. Transparency. Law 5282/14. Retrieved from <https://www.copaco.com.py/index.php/institucional/transparencia/ley-5282-14.html>

90 COPACO. News. Retrieved from <https://www.copaco.com.py/index.php/cooperacion-interinstitucional.html>

91 General Directorate of Migrations. News. Retrieved from <https://www.migraciones.gov.py/index.php/noticias/migraciones-y-copaco-dan-continuidad-al-acuerdo-para-provision-de-servicios-de-comunicacion-de-datos>

PERSONAL - NÚCLEO S.A.

Transparency		
	Yes	No
The ISP publishes transparency reports so that the user can learn about collaboration with government authorities on the data provided.		•
The ISP publishes transparency reports informing about collaboration with government authorities, indicating: a) the number of requests and disclosures classified by type of data - whether it is account information or connection of records; b) the number of requests and disclosures categorized by the government authority that made the request; c) the number of requests and disclosures classified by the motivation alleged by the government authority - presentation of evidence in civil, criminal, or administrative cases, etc.		•

Personal has no reports on its collaboration with the government on its website and no relevant reports are identified in Internet search tools. This lack of documentation was identified in previous editions of WDYD corresponding to 2017, 2020 and 2022, making it difficult to assess its performance in terms of privacy protection and collaboration with government authorities, which justifies the conclusion that the iSP does not meet the criteria set out in the performance standard. In this regard, Personal does not qualify in the transparency criterion.





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

Transparency		
	Yes	No
The ISP publishes transparency reports so that the user can learn about collaboration with government authorities on the data provided.	•	
The ISP publishes transparency reports informing about collaboration with government authorities, indicating: a) the number of requests and disclosures classified by type of data - whether it is account information or connection of records; b) the number of requests and disclosures categorized by the government authority that made the request; c) the number of requests and disclosures classified by the motivation alleged by the government authority - presentation of evidence in civil, criminal, or administrative cases, etc.		•

In relation to the first criterion, it is relevant to note that this ISP again scores because its parent company provides a report on collaboration with government authorities in the Millicom LED 2023 Report mentioned above.

The report indicates that South America, including Bolivia, Colombia and Paraguay, received 414 wire-tap orders, 475 requests for information on mobile payment services (MFS) data and 45,277 requests for information on user metadata in 2023⁹². While it is noteworthy that the report provides information on requests for interception of communications, access to metadata and MFS data, the main challenge remains in the lack of differentiation by country. Therefore, it is not possible to know with certainty the numbers of requests that correspond to Paraguay.

This access difficulty had already been identified in previous reports, although with some variations. In 2017 the report was published exclusively in English from Millicom's parent company and contained limited information omitting key data such as volumes, origin, reasons and scope of the requests. In the 2020 and 2022 reports some additional data was introduced, however, this was not broken down by country but only by region. This practice has been maintained by presenting data grouped in a general way which results in a persistent lack of specific and detailed information by country. This limits transparency and hinders a complete understanding of operations at the local level. In relation to the second criterion, despite the information provided, it cannot be considered as compliant, as no detailed breakdown is presented that meets the specific requirements of this criterion.

Therefore, Tigo complies with one of the two criteria observed, and therefore qualifies with half a star.



92 Millicom. LED Millicom 2023 Report. Page 7.



VOX - HOLA PARAGUAY S.A.

Transparency		
	Yes	No
The ISP publishes transparency reports so that the user can learn about collaboration with government authorities on the data provided.		•
The ISP publishes transparency reports informing about collaboration with government authorities, indicating: a) the number of requests and disclosures classified by type of data - whether it is account information or connection of records; b) the number of requests and disclosures categorized by the government authority that made the request; c) the number of requests and disclosures classified by the motivation alleged by the government authority - presentation of evidence in civil, criminal, or administrative cases, etc.		•

As in previous editions, Vox does not present reports on its website that address its collaboration with the government. Due to the absence of documentation that meets the criteria established in the performance standard, the ISP does not comply with any of the criteria evaluated.



CRITERION 6. Guidelines for requesting personal information





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

It will be evaluated whether the ISP has guidelines, procedures and protocols that define how each company cooperates with the State, either by providing information to the criminal prosecution system or other types of investigation and, if so, what specifications must be met for this purpose. It is also evaluated whether the company, when establishing its own rules for local authorities, takes into account the national context or if the pre-established guidelines respond to foreign procedures. In the latter case, it will be verified whether these procedures are more rigorous in favor of protecting the privacy of its users.

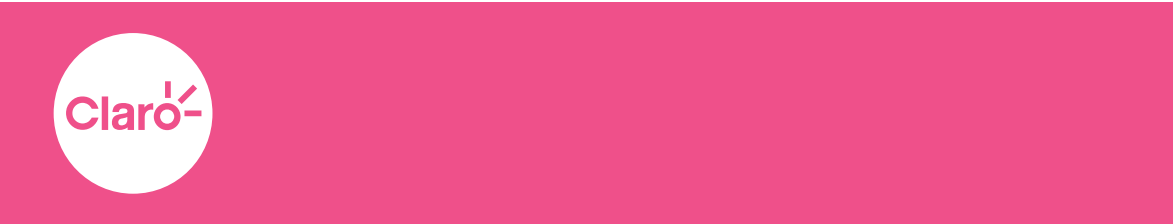
Evaluation criteria

- I. If the ISP has guidelines, procedures or protocols that determine how they will receive requests for information about their clients;
- II. If the guidelines, procedures or protocols are publicly available;
- III. If such guidelines, procedures or protocols explain in detail the steps to be followed upon request and the procedure for providing the data to the requesting authority.

Performance standard:

Full star		The ISP complies with all of the criteria
Half a star		The ISP complies with two of the criteria
A quarter of a star		The ISP complies with one criterion
Empty star		The ISP does not comply with any of the criteria

REPORT - GUIDELINES FOR REQUESTING PERSONAL INFORMATION



CLARO - AMX PARAGUAY S.A.

Guidelines for requesting personal information		
	Yes	No
If the ISP has guidelines, procedures or protocols that determine how they will receive requests for information about their clients.	•	
If the guidelines, procedures or protocols are publicly available.	•	
If such guidelines, procedures or protocols explain in detail the steps to be followed upon request and the procedure for providing the data to the requesting authority.	•	

Similar to the circumstance mentioned in our previous edition, Claro still does not provide relevant information to assess this criterion on its website. The protocols for handling data requests are available on the website of the parent company, América Móvil.

These protocols, detailed in the Transparency in Communications Report⁹³, address legal policies and obligations applicable in the countries where it operates, including Paraguay. América Móvil also has a privacy policy that establishes the rights of data subjects and provides general guidelines for governmental requirements. It is concluded that the ISP meets the criteria related to data handling protocols and its public availability through its parent company. However, it would be desirable for this information to be accessible directly from Claro’s website.

In sum, Claro complies with the three criteria considered here, and therefore qualifies with one star.



93 América Móvil. Transparency in Communications Report 2023. Retrieved from <https://sustentabilidad.americamovil.com/portal/su/pdf/2023-Informe-de-Transparencia-en-las-Comunicaciones.pdf>



COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Guidelines for requesting personal information		
	Yes	No
If the ISP has guidelines, procedures or protocols that determine how they will receive requests for information about their clients.		•
If the guidelines, procedures or protocols are publicly available.		•
If such guidelines, procedures or protocols explain in detail the steps to be followed upon request and the procedure for providing the data to the requesting authority.		•

The ISP does not provide guidelines, procedures or protocols that determine how they will receive requests for information on its clients. Although it has a detailed protocol for requesting public information under Law No. 5282/2014, on Free Citizen Access to Public Information and Government Transparency, this is not aimed at specific guidelines for security forces or government agencies. Since COPACO does not comply with any of the points evaluated, it does not qualify for the criterion of requesting personal information.



Personal

PERSONAL - NÚCLEO S.A.

Guidelines for requesting personal information		
	Yes	No
If the ISP has guidelines, procedures or protocols that determine how they will receive requests for information about their clients.		•
If the guidelines, procedures or protocols are publicly available.		•
If such guidelines, procedures or protocols explain in detail the steps to be followed upon request and the procedure for providing the data to the requesting authority.		•

The ISP does not provide clear and complete information on guidelines, procedures or protocols aimed at law enforcement and other government agencies for requesting personal information from clients.

However, it is worth mentioning that through a Google search, a news item was found regarding an agreement between the Supreme Court of Justice (CSJ, its Spanish acronym) and Núcleo SA signed in 2022 that will last for five years⁹⁴. According to the information available, the purpose of the agreement is to establish technological mechanisms for the CSJ to access data generated by the ISP. The agreement highlights the use of electronic orders instead of written documents. Furthermore, specific requirements are set for the electronic orders sent to the ISP, including attention to current regulatory deadlines. It also emphasizes that the responsibility for the information provided rests exclusively with the requesting official, exempting the ISP from any legal responsibility for incorrect handling of the information.

Given the limited information provided and the lack of specific details, especially the absence of the agreement documentation and its unavailability on the ISP website, it is difficult to fully assess the points established for this criterion. According to the performance standard, the ISP scores no points.



⁹⁴ Judicial Branch. Notes. December 19, 2022. Retrieved from <https://www.pj.gov.py/notas/23325-corte-suprema-y-nucleo-sa-suscribieron-convenio-a-fin-de-fortalecer-el-oficio-electronico>



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

Guidelines for requesting personal information		
	Yes	No
If the ISP has guidelines, procedures or protocols that determine how they will receive requests for information about their clients.	•	
If the guidelines, procedures or protocols are publicly available.	•	
If such guidelines, procedures or protocols explain in detail the steps to be followed upon request and the procedure for providing the data to the requesting authority.	•	

According to the information available on the ISP website, there are no specific guidelines for handling requests for personal data from security forces or government agencies.

However, we can observe relevant information in the Millicom LED Report 2023. The document details general guidelines and protocols on how to manage information requests from authorities, although these protocols are only available in the English version⁹⁵. Although the language barrier could make it difficult to fully understand the documents, we will adopt a flexible position in recognizing the existence of the language barrier, which allows us to give a positive rating for the second and third evaluation criteria. According to the established performance standard, Tigo complies with the three evaluated criteria and therefore qualifies with one star.



⁹⁵ Millicom. Compliance and Business Ethics. Policies and Guiding Principles. Law Enforcement and Major Events Guidelines. Recovered from <https://www.millicom.com/media/3613/law-enforcement-assistance-and-major-events-guidelines.pdf>



VOX - HOLA PARAGUAY S.A.

Guidelines for requesting personal information		
	Yes	No
If the ISP has guidelines, procedures or protocols that determine how they will receive requests for information about their clients.		•
If the guidelines, procedures or protocols are publicly available.		•
If such guidelines, procedures or protocols explain in detail the steps to be followed upon request and the procedure for providing the data to the requesting authority.		•

Vox does not meet this criterion either, as it does not provide clear and complete information on guidelines, procedures or protocols oriented to security forces and other government agencies, nor does it detail the conditions for the delivery of personal information of clients.

Considering the scoring standard, the ISP does not receive any rating in this aspect.



CRITERION 7. Accessibility





Does the ISP have a website with an interface that provides perceptible and understandable information, functional navigation, and operability regarding privacy policies, terms, and conditions of its products and services?

It is evaluated whether the ISP has perceptible information and equivalent alternatives to display content, if it has a navigable and functional interface, with understandable information and compatible with user tools in relation to the content on privacy policies and terms and conditions of its products and services.

Evaluation Criteria

- I. The ISP has a website interface that provides perceptible information and equivalent alternatives to display content, purpose or function;
- II. The ISP has a website interface that is navigable, functional, and has keyboard support;
- III. The ISP has a website with understandable information, which appears and operates in a predictable manner;
- IV. The content on the ISP website is compatible with the user’s current tools (different browsers, assistive technologies, and other user agents).

Performance standard:

Full star		The ISP complies with all of the criteria
Half a star		The ISP complies with two of the criteria
A quarter of a star		The ISP complies with one criterion
Empty star		The ISP does not comply with any of the criteria

REPORT - ACCESSIBILITY



CLARO - AMX PARAGUAY S.A.

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

In terms of accessibility, the ISP failed to improve its compliance standard since the last evaluation. It is true that Claro provides “Terms and Conditions of Use” and “Privacy Policies” documents for various services, which are available through a link at the bottom of the home page⁹⁶. However, accessing these documents requires navigating through several pages or using filters, which can be complicated, especially for screen reader users. When trying to access the documents, a very extensive tabulation is observed and keyboard navigation is difficult.

Although each document displays good contrast and text resizing, which meets the first accessibility criterion, navigation in general lacks predictability and complete accessibility, failing to meet criteria two and three.

Claro offers the option to provide invoices in Braille to users who require it⁹⁷, but the overall accessibility of the website is limited and it is necessary to scroll six times to access the information on the procedure for requesting this type of invoice. Likewise, it should be remembered that much of the information relevant to this research is not directly available on the ISP's website, having had to resort to the parent company's website.

⁹⁶ Claro. Legal and Regulatory. Retrieved from <https://www.claro.com.py/personas/legal-y-regulatorio>

⁹⁷ Claro. Legal and Regulatory. Other. Braille Invoice. Retrieved from <https://www.claro.com.py/personas/legal-y-regulatorio/factura-braille>

Evaluation of the website using tools such as WAVE⁹⁸ and TAW⁹⁹ reveal several other accessibility problems. To name a few, while the tab structure follows a logical order, concerns were identified such as the lack of tabs on forms which can complicate understanding and navigation for screen reader users. The presence of empty buttons affects the information provided to those using assistive technologies. In general, contrast problems were also found that could affect the legibility of the text, especially for users with low vision.

The presence of underlined text was also identified, which can cause confusion, as it is commonly associated with links. In addition, redundant text was detected in certain attributes which could affect the clarity and comprehension of the content. The lack of “aria-label” or “aria-labelledby” attributes in certain elements and problems with language designation could also be improved. Considering this, although different browsers and device diversity are contemplated, the website is not suitable for the use of assistive technologies such as screen readers, thus failing to meet the fourth criterion.

In summary, the website faces significant accessibility challenges that could impair the experience of users, especially those with disabilities. Therefore, by complying with only one of the criteria evaluated, Claro qualifies with a quarter star.



98 Web Accessibility Tool. Retrieved from <https://wave.webaim.org>

99 TAW. Retrieved from <https://www.tawdis.net/resumen>



COPACO S.A.

COPACO - LA COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A.

Accesibility		
	Yes	No
The ISP has a website interface that provides perceptible information and equivalent alternatives to display content, purpose or function.	•	
The ISP has a website interface that is navigable, functional, and has keyboard support.		•
The ISP has a website with understandable information, which appears and operates in a predictable manner.	•	
The content on the ISP website is compatible with the user's current tools (different browsers, assistive technologies, and other user agents).		•

Firstly, it should be noted that COPACO does not guarantee access to reliable information through the inclusion of clear terms and conditions on its web page, as well as a complete privacy notice covering all the services it offers.

Regarding the company's website and considering the first evaluated criterion, it should be noted that although suggestions for improvement were found according to the accessibility tools used such as WAVE¹⁰⁰ and TAW¹⁰¹, the general information of the website is perceptible and the different components of the user interface can be accessed. In addition, the background and foreground colors have a sufficient contrast ratio and it has normal text sizes. Therefore it is considered, in general terms, that this criterion is met.

In relation to the second aspect evaluated, keyboard navigation is possible, however, there are deficiencies that affect functionality, such as the lack of a clear hierarchy in the headings and the absence of descriptive labels that hinder navigation and understanding of the content. Likewise, some links do not provide clear information on their function or destination. Therefore, this criterion is not met.

On the third criterion, although some warnings related to the lack of alternative texts were found, the information on the website is understandable and operates in a predictable manner for users. Although some warnings related to the lack of alternative texts were found, the content is readable and the site operates in a coherent manner. Therefore, this criterion is considered complied with.

100 WAVE. Report > <https://wave.webaim.org/report#/https://www.copaco.com.py>

101 TAW. Summary of inquiry > <https://www.tawdis.net/resumen>

However, significant issues were identified in terms of the website’s navigability, particularly concerning links lacking text that clearly identifies their purpose and the lack of alternative texts in images. These problems indicate that the website design does not adequately address the diversity of tools and user agents, which may negatively affect people who rely on assistive technologies. Therefore, this criterion is not considered to be met.

Considering the above, COPACO complies with two of the four criteria analyzed, and therefore qualifies with half a star.



PERSONAL - NÚCLEO S.A.

Accesibility		
	Yes	No
The ISP has a website interface that provides perceptible information and equivalent alternatives to display content, purpose or function.	•	
The ISP has a website interface that is navigable, functional, and has keyboard support.		•
The ISP has a website with understandable information, which appears and operates in a predictable manner.	•	
The content on the ISP website is compatible with the user's current tools (different browsers, assistive technologies, and other user agents).		•

Taking into consideration the reports from the WAVE¹⁰² and TAW¹⁰³ accessibility tools, as well as the manual verification of the ISP's website, it is considered that this criterion is met since the website presents a scalable interface with adequate text sizes and a correct language identification, thus facilitating the perception of information. However, it is important to mention that several problems were found that require attention, such as the absence of alternative texts in images and other non-textual content, which prevents users of assistive technologies from fully accessing the content.

Regarding the second criterion, although the site allows keyboard navigation, obstacles affecting functionality were identified, such as the absence of a clear structure of headings and labels, which makes sequential navigation and content comprehension difficult. Additionally, some links lack clear contextual descriptions, which may confuse users as to their function or destination. Given these deficiencies, this criterion is not considered to be met.

The third criterion evaluated is also considered complied with, since the content appears predictable, with legible and understandable text, and the main language identified as Spanish. However, we suggest attention to this area because some difficulties were observed related to the lack of specific assistance for users, such as clear instructions or contextual help, which may affect the experience of users with cognitive disabilities or those unfamiliar with the interface.

¹⁰² WAVE > <https://wave.webaim.org/report#/https://www.personal.com.py/index.html>

¹⁰³ Taw > <https://www.tawdis.net/resumen>

Finally, problems affecting compatibility with assistive technologies were detected. In this context, an inadequate hierarchy of headings was identified, which makes navigation difficult through screen readers, as well as multiple low contrast alerts, which may prevent people with visual impairments from reading the text. These problems indicate that the site is not fully designed considering the diversity of support tools and browsers, which is suggested as a relevant area for improvement.

The ISP complies with two of the four criteria evaluated and therefore qualifies with half a star.





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

Accesibility		
	Yes	No
The ISP has a website interface that provides perceptible information and equivalent alternatives to display content, purpose or function.	•	
The ISP has a website interface that is navigable, functional, and has keyboard support.	•	
The ISP has a website with understandable information, which appears and operates in a predictable manner.	•	
The content on the ISP website is compatible with the user's current tools (different browsers, assistive technologies, and other user agents).	•	

The company complies with the first accessibility criterion since its website has easy access to documents from the page, such as: terms and conditions, privacy notice and even the telecommunications services subscription contract. The first two documents mentioned have texts that can be resized and adapted, ensuring a good perception of the information and complying with the principle of equivalence of content.

In relation to the second criterion, the ISP complies with accessibility for keyboard navigation. The front page of the website functions correctly and allows scrolling and zooming with the keyboard without inconveniences. Although some areas for improvement are identified in the structuring of headings and tab order, the carousel is also keyboard navigable, ensuring a functional experience for users with accessibility needs.

The ISP also meets the third criterion as the website text is readable and understandable and the content appears and operates in a predictable manner. This ensures a good user experience and facilitates understanding of the information presented on the site.

As for the fourth criterion, it is determined that the company complies with it since its website is designed considering a diversity of tools and user agents. Screen reader tests were carried out and textual alternatives were found in most of the multimedia content. Although the accessibility tools used to

evaluate the ISP website, such as WAVE¹⁰⁴ and TAW¹⁰⁵ identified some errors related to contrast and the definition of alternative texts in certain icons, these errors do not exceed four, and the website complies with accessibility standards.

Tigo meets all four accessibility criteria, ensuring a positive experience for all users, including those with special information access needs. Therefore, it qualifies with one star.



104 WAVE > <https://wave.webaim.org/report#/https://www.tigo.com.py>

105 TAW. Summary > <https://www.tawdis.net/resumen>



VOX - HOLA PARAGUAY S.A.

Accesibility		
	Yes	No
The ISP has a website interface that provides perceptible information and equivalent alternatives to display content, purpose or function.		•
The ISP has a website interface that is navigable, functional, and has keyboard support.		•
The ISP has a website with understandable information, which appears and operates in a predictable manner.		•
The content on the ISP website is compatible with the user's current tools (different browsers, assistive technologies, and other user agents).		•

The company does not meet the first accessibility criterion as its website presents significant problems related to the perceptibility of information and user interface components. On the other hand, the website does not have relevant information available on terms and conditions or privacy policy, points that were already noticed in the previous edition of this research.

The ISP does not meet the second criterion either. While it has keyboard support, the website has several navigational issues that affect functionality and usability for users who rely on keyboard or assistive tools such as the lack of several headers and tabs. Although the interface is functional overall, the issues identified negatively impact the user experience.

Regarding the third criterion, improvements have been made in identifying the language of the page, as validates by the TAW¹⁰⁶ report. However, there are still problems such as the lack of definitions for uncommon or Guaraní words used. In addition, no assistance is provided to users for some non-standard drop-down elements, nor for preventing and correcting errors. It is noted that some pages are still not finalized despite being linked in the main menu of the site, a problem that persists from the previous edition of this research¹⁰⁷. Although the content of the website is legible and understandable in general terms, navigability problems and even the absence of numerous alternative texts¹⁰⁸ make it difficult to operate the site in a predictable manner, and may generate confusion in the user's experience when interacting with the content.

106 TAW. Summary > <https://www.tawdis.net/resumen>

107 Just like reported in 2022, attempting to access the "TELEFONOS" page (sic) from the main menu leads to a "under construction" page. Retrieved from <https://www.vox.com.py/telefonos>

108 WAVE. Retrieved from <https://wave.webaim.org/report#/https://www.vox.com.py>

Finally, the ISP does not meet the fourth criterion either, since navigability, adaptability and contrast problems affect the accessibility of the site in different browsers, assistive technologies and user agents. The diversity of tools is not adequately contemplated in the design of the site, negatively affecting the user experience.

In sum, Vox does not meet any of the established criteria and therefore does not receive any stars.



CONCLUSION

Since the first editions, a substantial difference has been observed between national Internet providers and those operating as subsidiaries of foreign companies. Companies such as Claro, Personal and Tigo have maintained better scores since the beginning of the evaluation in 2017. Although they have shown improvements in some aspects and criteria up to 2024, their progress remains slow and faces major challenges. In contrast, domestic providers such as COPACO and VOX have shown minimal progress since 2017, which is worrisome due to its impact on service quality and local market competitiveness. This lack of progress limits the protection of the rights of its users.

Privacy and personal data protection policy

An analysis of data privacy practices among ISPs reveals a mixed picture, with some providers showing positive steps while others lag far behind. Although companies such as Claro, Personal and Tigo have facilitated access to their privacy policies and provide relatively detailed information on data collection and processing practices, there are still doubts about the completeness and clarity of the information they provide. As an example, none of the three companies clearly describe data retention periods, a crucial aspect of data protection. This lack of transparency could raise concerns that data could be stored indefinitely, contradicting the principles of data minimization and purpose limitation.

Copaco, despite having a privacy policy, limits its scope to data collected through its applications, neglecting to address data processing practices for other services such as Internet and telephony. This limited scope creates a troubling transparency gap in relation to the company's overall approach to data privacy. Tigo, despite having a seemingly comprehensive privacy policy, shows inconsistencies between the policy and its service subscription contract, particularly regarding the need for user consent to share data with third parties. These discrepancies could cause confusion for users.

The most worrying case is that of Vox, which completely lacks a publicly available privacy policy. This absence demonstrates their lack of concern for transparency and user rights, underscoring the need for immediate action to address this critical deficiency.

Judicial Authorization

With regard to judicial authorization, the results of this edition do not differ significantly from those obtained in previous WDYD analyses. All ISPs require a court order before releasing user information. However, this due process does not include communication metadata, despite the fact that international human rights standards on surveillance, as established in the judgments of the Inter-American Court of Human Rights in the cases *Escher v. Brazil* (2009) and *CAJAR v. Colombia* (2023), which state that such data should also be protected. These rulings are binding for Paraguayan jurisprudence and reinforce the need for a strict legal framework in this area.

The analysis of this criterion underlines the importance of specific regulations over general legislation, particularly in the context of communication surveillance. Articles 198, 199 and 200 of the Paraguayan Code of Criminal Procedure clearly and explicitly state that any intervention in communications requires a court order. This principle reinforces the exceptional nature of these measures, seeking to balance the needs of criminal investigations with the protection of fundamental rights. In addition, constitutional provisions and the Telecommunications Law complement this framework by protecting not only

the content of communications, but also their existence, including metadata. This comprehensive approach seeks to ensure that any communication intervention is carried out under strict legality and with full respect for fundamental guarantees. A critical point identified in this criterion is the lack of clarity and uniformity in company policies regarding privacy and due process. For example, Claro mentions in its policy that it shares data for “legal reasons”, but does not clarify whether this is conditional on a court order. According to the *Sustainability Report 2023* of América Móvil, its parent company, they are committed to avoiding illegal interventions and respecting users’ privacy. However, the report also mentions the Public Prosecutor’s Office as a competent authority to request data, including geolocation and interception of communications, despite the fact that it has no powers to issue court orders. This raises serious concerns about possible violations of due process and the right to privacy.

On the other hand, Personal states that it shares user data only with a written order from a competent judicial authority, but also points out that this is not an exclusive requirement. Also, like COPACO, it does not make a clear distinction between content and metadata, which further weakens the protection of users’ privacy. In the case of Tigo, its privacy notice indicates that it may share data in a variety of circumstances without specifying that a court order is a prerequisite. However, its parent company, Millicom, assures in its 2023 Disclosure to Authorities Report that subsidiaries, including Tigo Paraguay, only hand over communications content with a court order. This discrepancy between Tigo’s local policy and its parent company’s claims raises doubts about the company’s actual practices.

Finally, Vox does not provide public information on whether and under what circumstances it discloses user data. This lack of transparency makes it impossible to assess its commitment to judicial authorization for data disclosure, which represents a critical gap in terms of privacy protection.

Although companies show general compliance in terms of requiring court orders for access to communications content, serious concerns persist regarding metadata protection, clarity in privacy policies and transparency in processes. These aspects are essential to ensure respect for the right to privacy and due process in Paraguay.

Notification to users

Regarding the third criterion, the analysis reveals that none of the five ISPs has a policy for notifying users when their data is requested by the authorities. This lack of transparency, already identified in all previous editions of WDYD, raises significant concerns about users’ rights and due process protections in Paraguay.

Policies for the promotion and defense of human rights

In terms of this criterion the ISPs analyzed mostly do not demonstrate a strong public commitment to human rights, especially with regard to seeking regulations on privacy and personal data protection. However, subsidiaries such as CLARO and TIGO take positive actions because they come mainly from the policies of the parent companies, rather than from the direct commitment of the local ones. It should be noted that CLARO, Personal, Tigo and VOX participate in the GMSA, a global organization that promotes a positive business environment and social change in the mobile ecosystem. Tigo and Claro are also the companies with the most safety campaigns for their users, identified throughout the editions of WDYD.

Transparency

Regarding this criterion, only Claro and Tigo provide some level of transparency, and these reports are only accessible on the websites of their parent companies. These regional transparency reports do not always provide detailed country-level breakdowns, making it difficult to assess the specific practices and compliance rates of their national subsidiaries. In addition, these available transparency reports focus primarily on interception orders and metadata requests, providing limited information on other forms of user data sharing with government entities. For example, it would be relevant to include details on requests for data such as names, addresses or billing information, which might be required by authorities to identify individuals during investigations, as well as to clarify whether these companies participate in continuous monitoring programs or other systematic surveillance practices.

Accessibility

On the last criterion related to accessibility, the analysis reveals a marked disparity in the accessibility of ISP websites. Throughout the four editions of the WDYD, interesting advances were observed in this criterion. For example, Tigo stands out as the undisputed leader, demonstrating a strong commitment to inclusion by meeting all four accessibility criteria evaluated. In contrast, Claro, Copaco, Personal and Vox present deficiencies to varying degrees, with Vox showing the most significant barriers in terms of accessibility.

RECOMMENDATIONS

The analysis of the present research underscores the need for improvements in all areas. All ISPs in Paraguay should prioritize the development of clear, comprehensive and easily accessible privacy policies covering all their services. They should explicitly address data retention periods, include specific legal references, and ensure consistency among the various documents related to data processing practices.

The failure of ISPs to notify users is a critical problem that requires immediate attention. By failing to notify individuals about data requests, these companies prevent clients from exercising their right to challenge potential unlawful surveillance and protect their privacy. Addressing this deficiency is crucial to fostering a data protection environment that respects users' rights and promotes greater transparency and accountability.

While Claro and Tigo's parent companies have taken initial steps toward greater disclosure, the lack of independent reporting at the local level and the limited scope of information provided hinder meaningful accountability. All five ISPs must prioritize transparency by publishing comprehensive and detailed reports that allow users to understand and scrutinize how their data is handled in response to government requests. This increased transparency is essential to build trust and ensure the protection of users' privacy and due process rights in Paraguay.

In addition, it is essential to take proactive steps that go beyond basic policy statements. The ISPs should participate in industry initiatives that promote data privacy and human rights, invest in user education and awareness programs, and proactively engage in legal recourse against excessive or illegal data requests. By taking these steps, ISPs can foster greater trust with their users and contribute to a stronger data protection environment in Paraguay.



“Who has your back?”

qddt.tedic.org

2024

This work is licensed under
a Creative Commons Attribution-ShareAlike 4.0
International License.

