Telefónica

Report on Transparency in Communications 2023

Contents

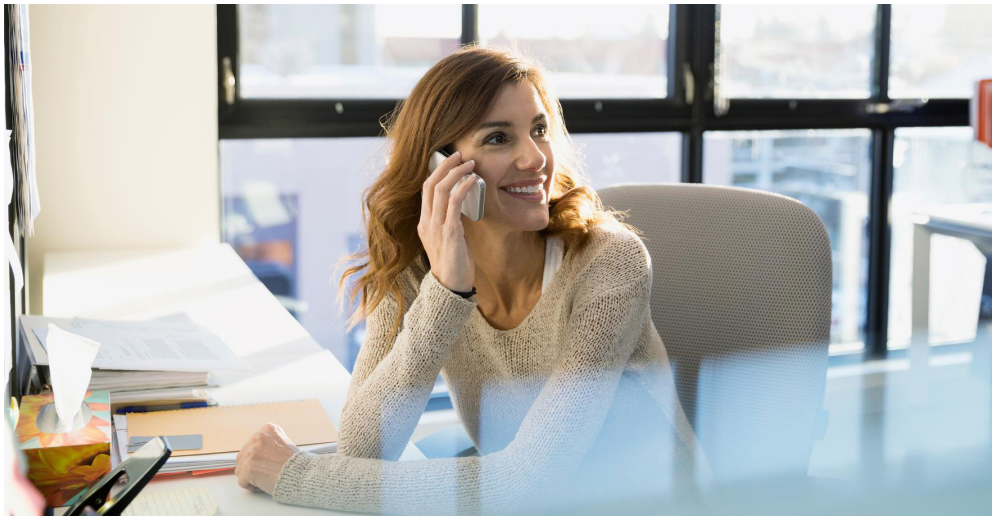
3 Introduction and scope of the report
4 Our human rights due diligence
6 Our governance
8 Applicable policies and processes
13 Indicators in this report

15 Report by country in which operate

16 Argentina
19 Brazil
22 Chile
25 Colombia
30 Ecuador
32 Germany
35 Mexico
38 Peru
41 Spain
45 Uruguay
48 Venezuela

50 Glossary

Introduction and scope of the report



Companies which operate in the telecommunications sector are required by law in the jurisdictions in which they operate to collaborate and respond to requests for information issued by competent authorities, including state security forces and bodies, government agencies, and/or courts (hereinafter, "competent authorities": see definition in glossary).

Such requests relate to our customers´ or users´ communications, requests to block access to certain websites and contents and to filter contents, and/or to temporarily suspend the service in certain areas or with regard to certain accounts.

As part of its commitment to the protection of human rights and especially the right to privacy and freedom of expression, Telefónica publishes its Telecommunications Transparency Report (this is the ninth edition of the report). In this way, we demonstrate compliance with the legal obligations in the different countries in which Telefónica operates, as well as with related digital rights.

This report, which corresponds to the annual period from 1 January 2023 to 31 December 2023, shows*:

- A description of our human rights due diligence process;
- Our governance in terms of human rights in general and privacy and freedom of expression in particular;
- The commitments, policies and processes we follow when responding to requests from competent authorities;
- Information on the legal context that provides the competent authorities with the legal basis to make these kinds of requests[1];
- The competent authorities that are empowered under the local legislation to request information for each of the indicators we report on;
- The total number of requests we received during the stated annual period in each of the countries we operate in, unless the country's legislation prohibits us from doing so or a government or another public body already discloses that information;
- Whenever technically possible, the number of requests that we reject, the accesses that are affected by each indicator and the URLs and/or IPs affected in the event of any blocking or restrictions on content.

1.The specific legal framework of each country also sets out limitations to the information on the requests that Telefónica receives.

*The data included in this report are not audited.

Our human rights due diligence

Human rights have been an integral part of our Business Principles, which constitute our code of conduct, since 2006.

The UN Guiding Principles on Business and Human Rights have served as a fundamental guide to foster the guarantee of and respect for people´s fundamental rights and, specifically, with regard to privacy and freedom of expression.

Likewise, we have several internal policies aligned with our Responsible Business Principles.

Groups of impacts identified and priority areas in the area of human rights

Conflict minerals	Labour conditions	Diversity and non-discrimination	Privacy	Digital inclusion	Protection of children
Health and safety	Freedom of expression and information	Responsible use of new technologies	Environment	Land rights	Corruption and bribery
Cybersecurity	Circular economy	Biodiversity	Water resources	Fiscal responsibility	Competitive behaviour

Priority areas for Telefónica regarding human rights

The 18 groups of impacts we have described in the table above are encompassed within the following broad areas:


Digital rights


Responsible use of new technologies


Digital inclusion


Protection of children


Social and environmental standards in the supply chain

In accordance with our Global Human Rights Policy, we have a Due Diligence process in place to identify, prevent, mitigate and remedy the (potential and actual) impacts of our business on human rights. Regarding management, the starting point of our Due Diligence consists of the Global Human Rights Impact Assessments; these are conducted every three/four years at global level with the help of external human rights experts and in close collaboration with our stakeholders. The goal of these impact assessments is to find out how our activities/business relationships and products/services impact on all existing human rights and, on this basis, identify the human rights issues that are most salient to our business activity.

Based on the global assessments and the material issues identified in them, we also conduct more detailed analyses:

- Biannual risk assessments in all our markets;
- Local impact assessments, in cases where it is important to have a more accurate picture of the national situation in order to identify risks in a specific context;
- Thematic impact assessments, when we need to have a more detailed view of an issue because we have identified a particular risk or concern.

We also have a complaint and remedy mechanism, our Whistleblowing and queries Channel, which allows stakeholders to confidentially and anonymously make complaints and queries based on the principles of respect, confidentiality, substantiation and completeness (in several languages) concerning any aspect related to the Business Principles and human rights in general, as well as privacy and/or freedom of expression in particular. The publicly available Queries Channel Management Regulation and Internal Regulation System Management Policy are both accessible on Telefónica's corporate website and regulate the procedure to be followed to resolve queries and complaints.

The digital rights discussed in this report are continually reflected and assessed as part of our due diligence process to ensure respect for privacy and freedom of expression rights through responsible, comprehensive and contemporary management.

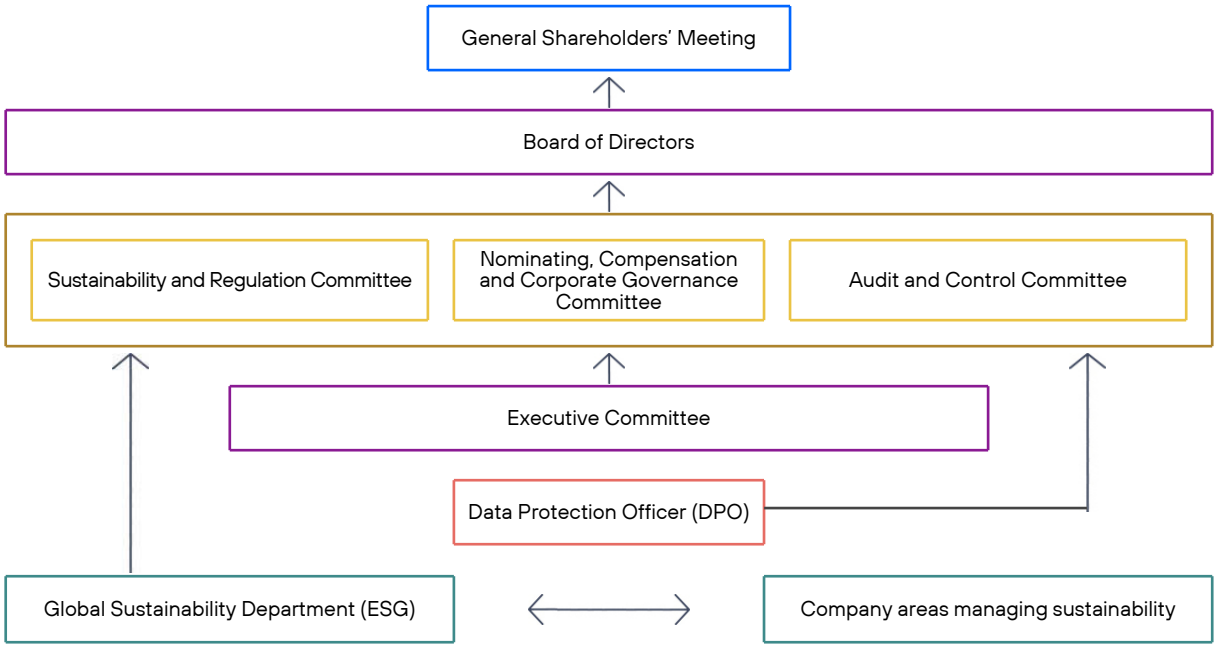
Our governance

We have established a governance model with clear responsibilities for the protection of human rights in general and privacy and freedom of expression in particular.

Our human rights activities, including issues related to privacy and freedom of expression, are defined and implemented by means of the **Responsible Business Plan.** This plan sets out the Company's sustainability strategy and objectives and is **approved and monitored by the Board of Directors and its Sustainability and Regulation Committee** (created under its new configuration on 13 December 2023)

The aim of this governance model, headed by the Board of Directors, is to ensure that our commitment to human rights is incorporated into all activities and levels of the Company.

Main bodies within the sustainability governance model

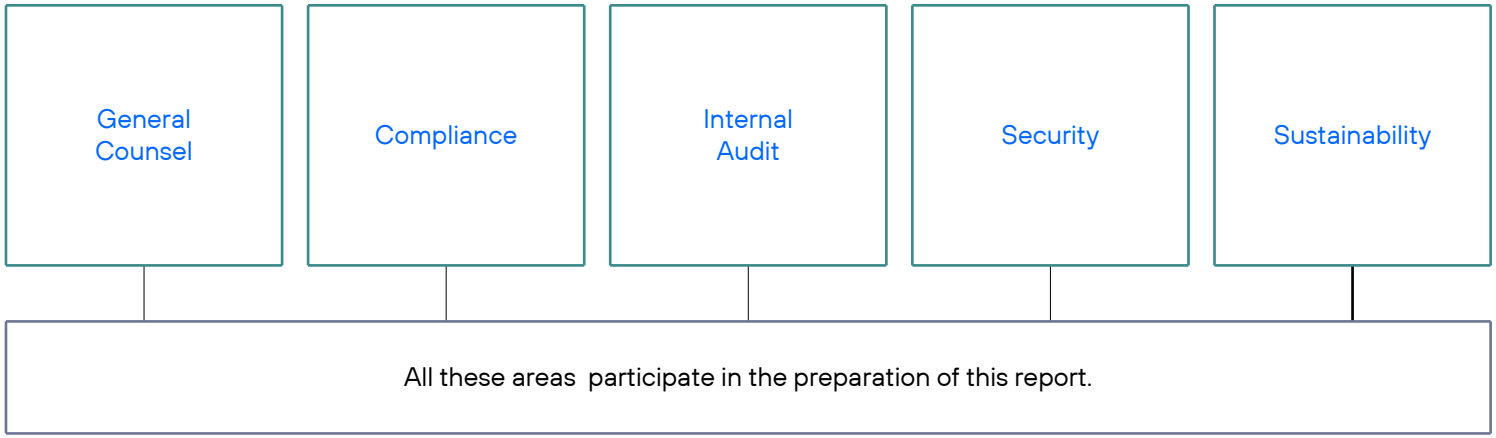


The **DPO (Data Protection Officer)** is the person within the Group who is responsible for coordinating the personal data protection initiatives and reports directly to the Board of Directors via the Audit and Control Committee (one of the Board's permanent committees). The DPO coordinates the Steering Committee, a committee which involves all relevant corporate areas for specific matters relating to privacy and freedom of expression.

Furthermore, the **General Counsel, Compliance, Internal Audit, Security** and **Sustainability** areas are involved in the governance and management of this report, which covers the requirements of the competent authorities and their relationship with the rights of privacy and freedom of expression.

To produce this report, a high-level analytical review of the locally reported data is carried out. Participating areas may make any comments they consider pertinent, either generally or specifically, in relation to the information provided by the operators. The aim is to ensure the quality of the information at all times, in compliance with the regulations in force, as well as to protect the fundamental rights of individuals, on the basis of the procedures carried out.

Any requests which need to be analysed due to their characteristics and exceptional nature are analysed by the heads of the respective business units by means of the appropriate weighting of all the interests potentially involved, including human rights, fundamental freedoms and any other interests that may be applicable. They may also be analysed, should the circumstances arise, by the bodies within each company whose functions include assessing and managing situations which could eventually lead to a crisis.



In the event of a crisis, the procedure established in the Global Crisis Management System is applied. The taxonomy in this system explicitly includes critical incidents that may have an impact on freedom of expression and privacy due to:

- certain requests by authorities
- certain legislations

The Global Crisis Management System stipulates that, in the event of a crisis relating to privacy and/or freedom of expression issues, the Chair of the Crisis Committee may convene the Human Rights Panel (made up of the relevant departments) in order to analyse the situation, design and apply a response strategy, report to the Executive Committee and conduct further analysis in order to prevent such risks in the future.

Applicable policies and processes

To ensure the protection of the rights to privacy and freedom of expression, access to information and non-discrimination, we have promoted and reviewed different policies and procedures. Below, we highlight the most important internal policies/processes concerning privacy and freedom of expression that have been adapted as a result of the latest impact assessments.

Policies

- **Global Human Rights Policy:**

This policy formalises our commitment to human rights included, in general terms, in Telefónica's Business Principles and contained in greater detail in a set of policies and rules that seek to ensure respect for and application of internationally recognised social, economic and cultural human rights.

- **Global Privacy Policy:**

This policy forms part of Telefonica's strategy to design a digital experience based on trust.

Aware of the importance of deserving the trust of our customers and/or users and, generally speaking, of our stakeholders, this policy guarantees the lawfulness of and respect for privacy in the processing of their data by Telefónica.

It stipulates mandatory common standards of behaviour for all entities in the Group and establishes a framework for a culture of privacy based on the principles of legality, transparency, commitment to the rights of the data subject, security and limitation of the storage period.

Under the principle of transparency, we guarantee that data subjects are provided with easily accessible and intelligible information about the personal data we collect (e.g., their name, surname/s , address, bank account, personal preferences, etc.), how we collect them and the purpose (service provision, etc.).

- **Governance Model Rule on Personal Data Protection:**

The objective of this regulation is to address the most important aspects to be taken into account for the proper management and protection of personal data.

It establishes an organisational and relationship model in which the person with the highest level of responsibility for the protection of personal data function is the Data Protection Officer (DPO), who reports directly to the Board of Directors of Telefónica, S.A. In addition, it establishes the following relationship and governance structure:

- **Global DPO Office:** This office is responsible for supervising compliance with the Telefónica Group's data protection regulations. It is responsible for carrying out and/or coordinating the functions derived from Article 39 of the GDPR, as well as the Telefónica Group's Data Protection Governance Model. It supports the Telefónica Group (as data controller or data processor) in data protection matters, coordinating, from its global role, the supervision of compliance with current regulations.
- **Privacy Committee:** This committee meets every six months under the coordination of the Global DPO, with the attendance of a representative of the global Security, General Counsel, Regulation, Technology, Data Office, Compliance, Sustainability and Internal Audit areas and the Business Areas. The Privacy Committee reviews issues related to the data protection function, coordinating the perspectives from the different roles involved in it in compliance with the Telefónica´s Privacy Governance model and identifying cross-cutting issues that, in terms of privacy, affect or may affect the business areas.

- **Global Rule on Requests made by Competent Authorities:**

This rule was approved in 2019 to strengthen the existing procedure in place since 2016, with the aim of aligning it with the other policies in force and our commitment to respect human rights and fundamental freedoms. It defines the principles and common minimum standards to be taken into account in the internal procedures of each of the Group's companies/business units/OB in order to fulfil their duty of collaboration with the competent authorities in accordance with the applicable national legislation of each country and with the fundamental rights of those involved in this type of procedures.

The principles governing the procedure are confidentiality, completeness, justification, proportionality, political neutrality, diligent response and security.

We are committed to ensuring participation in the process by legal areas or similar areas with legal competence in the handling of these requests. In our relationship with the competent authorities, there are permanent representatives who act as the single point of contact, so we reject any requests that do not come through these official channels.

- Global Security Policy:

Updated in 2023 and inspired by the principles of integrity, commitment and transparency, this policy is governed by the relevant domestic and international standards and regulations and establishes the guiding principles regarding security that are applicable to all the companies that form part of the Telefónica Group.

Security activities are governed by the following principles:

- **Legality:** Necessary compliance with domestic and international laws and regulations with regard to security.
- **Efficiency:** This highlights the anticipatory and preventive nature of such actions with regard to any potential risks and/or threats, with the aim of anticipating and preventing any potential harmful effect and/or mitigating any damage that might be caused.
- **Co-responsibility:** The duty of users to preserve the security of the assets that Telefónica places at their disposal.
- **Cooperation and coordination:** Cooperation and coordination between all business units and employees are prioritised in order to achieve the appropriate levels of efficiency.

As a result of this policy, we have developed regulations for compliance, which are reviewed and updated as a result of a continuous improvement process. Regular measurements and audits on security activities, changes in context and new risks are taken into consideration in this review.

- Responsible Communications Policy:

Its aim is to establish guidelines for Telefónica's actions with regard to our communication and content generation channels. It is based on the principles of legality, integrity and transparency, neutrality and protection of minors.

With regard to the principle of neutrality, we undertake to avoid positioning ourselves politically as a company and promote the right to freedom of expression within the regulatory frameworks to which we are subject. In our communication to customers and through advertising we prohibit certain conduct that is contrary to our Business Principles. Thus, in our messages and our sponsorship we do not tolerate any abuse of the consumer's good faith; violations of people's dignity; the promotion of alcohol, tobacco, drugs, eating disorders or terrorism; incitement to hatred, violence or discrimination; the execution of unlawful behaviour; or taking advantage of children's naivety.

- Artificial Intelligence Principles:

Approved by the Executive Committee in October 2018, we are committed to designing, developing and using Artificial Intelligence (AI) with integrity and transparency. Our AI principles put people at the centre and ensure respect for human rights in any context and process in which Artificial Intelligence is used. The principles emphasise equality and impartiality, transparency, clarity, privacy and security. These principles are applied in all of the markets in which we operate and are extended to our entire value chain through our partners and suppliers.

In 2022, Telefónica launched an ethical and responsible AI governance pilot programme, testing new roles such as the AI "Ethics Expert Group", the "RAI Champions" (those responsible for AI in the various departments), the AI coordination role and an "AI Office". In addition, testing was carried out on the methodology for evaluating products and services and training and awareness-raising on ethical AI for the various roles began. The monitoring mechanisms necessary for the implementation of AI governance were put into practice during the pilot.

Drawing on the experience gained over the years, on 1 December 2023, Telefónica approved its AI governance model, which binds the Group's companies and employees, harnessing the best practices and lessons learned from the implementation of Telefónica's ethical principles, our participation in European reflection processes and our experience in privacy governance.

This governance is based on the following principles:

- Strong penetration of governance in the business areas, which assume responsibility for documenting and implementing requirements for the AI systems they develop, acquire, use or market.
- Robust coordination mechanisms at both functional and group level.

- Clear focus on risks, their identification and mitigation.
- Scaled decision making, incorporating experts in ethics for those issues that require this.
- Management and supervision of AI governance by the Telefónica Group's compliance areas.

This governance model, together with the corporate inventory and risk management applications and AI requirements that have been developed internally, allows Telefónica to meet its ethical commitments in terms of responsible technology and, additionally, to fulfil its obligations concerning the international collaboration frameworks in which it participates, such as the one led by UNESCO, and the regulation of AI that is being incorporated into the legal systems of the different countries in which Telefónica operates.

Initiatives and processes

- **Human rights training:**

In 2023, we continued our general human rights training, assigning all new employees to attend the Responsible Business Principles Course.

- **Integration of human rights into Enterprise Risk Management:**

Risks related to human rights impacts are included in the Telefónica Group's Enterprise Risk Management as a specific item that has to be evaluated on a biannual basis by each operation/country.

The objective is to identify any risks of direct or indirect impact on the operations of the Telefónica Group in relation to possible infringements of human rights, be it as a consequence of the Company's own activity or the activity carried out by our suppliers or other commercial relations. This analysis contemplates any change in legislation or activity that may have an impact on human rights.

This risk assessment makes it easier to define the action needed in directly affected business units with the aim of mitigating and/or avoiding these risks and prioritising the actions to be taken by Internal Audit, with regard to its schedule of supervision of internal control structures.

- **Human Rights by Design:**

We assess potential human rights impacts of new products and services through a "human rights by design" approach, i.e., at the outset of designing and/or marketing products and services. To be more precise, product managers have to perform a self-assessment of new products and services using an online tool in the design phase in order to identify and address potential human rights impacts while in the design phase. The human rights addressed in this questionnaire include privacy, freedom of expression, non-discrimination, artificial intelligence and impact on vulnerable groups such as children. If human rights risks are identified after completion of the self-assessment, the product/service in question is subjected to an exhaustive and more detailed analysis with the help of human rights experts in the Company in order to minimise potential adverse human rights impacts in the development of the product/service.

- **Transparency initiatives:**

One of the challenges and key elements of privacy is guaranteeing transparency. At Telefónica we have opted to put this aspect into practice by including transparency as one of the guiding principles of the Global Privacy Policy and developing different initiatives bringing this principle to life.

> Global Transparency Center: The Global Privacy Centre is a public reference point for our policy and processes relating to privacy and security at a global level. Available at www.telefonica.com, our stakeholders can find all the information they need easily and in a reader-friendly format by means of visual and graphic resources. Our objective during 2023 was to continue improving on this centralised channel, including linking all of the Group's Transparency Centres to present all the relevant information in a centralised manner.

> Operator/Local Transparency Centres: The purpose of these centres is to enable both our customers and any stakeholders to obtain information, in a simple, digital and understandable way, with regard to the processing of their personal data by the operators and other relevant information on privacy and security aspects. The information available includes data on channels and avenues to exercise rights, security and confidentiality measures adopted for data processing, privacy terms and conditions applicable to our products and services, transparency reports and our Artificial Intelligence principles, as well as the child security and protection issues that apply in digital environments.
The local Transparency Centres are currently available on the websites of all the operators. They are updated regularly in accordance with regulations and stakeholder analysis.

In addition, the Transparency Center was launched for our content platform, Movistar+. The service is available through the Mi Movistar section and allows customers to control their data.

> Customer empowerment: As part of the principle of transparency, Telefónica provides customers with access to the data they generate during the use of our products and services, data that are collected in the so-called "Personal Data Space" of Kernel and which are accessible through different channels.

The Transparency Center, which offers all customers access to their privacy preferences and management of the data collected in the "Personal Data Space", is currently available to a group of users through the Mi Movistar app (in the Security and Privacy section of the User Profile) and has been available through the television channel in Spain since 2022.

In the Transparency Centre, through the Privacy Permissions section customers can manage the legitimising grounds relating to the use of their data for certain purposes. In addition, the Access and Download section includes useful views of different types of data, with a user-friendly experience, in compliance with privacy criteria; there is also the option of downloading a more detailed document.

The Transparency Centre experience has been designed to give users confidence, using clear language and explaining the purpose for which their data is processed and its nature within Telefónica.

Through the Transparency Centre we fulfil our promise to empower our customers, by means of features for them to control and ensure the transparency of their data, in accordance with applicable regulations on privacy. For example, in Europe this processing is fully aligned with the GDPR.

- **Effective application of policies and processes:**

In accordance with our Policy for the Elaboration and Organisation of the Regulatory Framework, the Compliance Department is responsible for coordinating the Telefónica Group's Regulatory Framework by supervising the process of defining the internal policies and, in turn, promoting actions to encourage their updating and communication. In addition, it detects the needs and opportunities for the improvement, modification and updating of the existing internal policies, proposing lines of action to the people responsible for the internal policies and providing support and advice for the person responsible in relation to their wording and implementation.

Observance and compliance with the regulations (e.g., the above-mentioned privacy and security policies, etc.) are subject to review and supervision by those responsible for the internal policies, who lead the proposal, creation, dissemination and implementation of these and carry out the pertinent monitoring, evaluation and updating. They are also empowered to carry out supervision, on a sampling basis, of the controls whenever they deem appropriate.

Additionally, in line with the provisions of the National Securities Market Commission (CNMV) and the provisions of Article 22 of the Regulations of the Board of Directors of Telefónica, S.A., one of the powers of the Audit and Control Committee of the Board is to supervise the effectiveness of the Company's internal control, internal audit and risk management systems.

RDR (Ranking Digital Rights) and B-Tech

We maintained our leadership, for the third consecutive year, of all the telecommunications companies evaluated by the **Ranking Digital Rights** initiative. This organisation evaluates the commitments, policies and practices of companies in matters that affect customers´ freedom of expression and privacy, including governance and oversight.

In 2023, Telefónica continued its membership of **B-Tech,** an initiative from the United Nations that seeks to promote human rights in the digital sector and offer a platform for multi-stakeholder engagement to promote knowledge sharing on human rights.

Indicators in this report

In the following sections we report the number of requests we receive from the competent authorities in the countries in which we operate.

Any request received from a competent national authority must comply with the judicial and/or legal processes that correspond to the country in question. At Telefónica we only respond to requests from competent authorities as laid down in our Global Rule on Requests made by Competent Authorities. At Telefónica **we do not respond to private requests; we only process requests from competent authorities**.

In order to proactively fight against online child sexual abuse content and images, at Telefónica we proceed to proactively to block these materials in accordance with the guidelines and lists provided by the Internet Watch Foundation.

The indicators we offer in this report are:

Lawful interceptions

Requests made by competent authorities within the framework of criminal and, where appropriate, civil investigations with the aim of intercepting communications or accessing traffic data in real time.

We have incorporated the breakdown of interceptions, whenever technically and/or legally possible, in the following way:

- **Registrations:** Requests for a new interception.
- **Extensions:** Requests to extend an existing interception.
- **Cancellations:** Requests to disconnect an existing interception.

Access to metadata

Requests made by competent authorities that seek to obtain historical data referring to:

- registered users' name and address (subscriber information);
- data identifying the source and destination of a specific communication (e.g., telephone numbers, Internet service user names, etc.);
- communication dates, times and duration;
- type of communication;
- computer equipment identities (including IMSI or IMEI);
- the geolocation of the user's device.

Content blocking and restriction

Requests made by competent authorities to block access to specific websites or any given content. These involve requests to block access to websites or contents, but not requests to delete user content. To give an example, blocking requests are issued because websites or contents infringe local laws (usually in relation to child sexual abuse, online betting games, copyright, libel, the illegal sale of medicine, weapons, registered trademarks). We have incorporated the breakdown by blocking type when the tools and legislation so permit.

Geographical or temporary suspension of the service

Requests from the competent authorities to temporarily and/or geographically limit the provision of a service. These requirements are usually related to situations of force majeure such as natural catastrophes, acts of terrorism, etc. Individual access restrictions are also accounted for.

In addition, for each indicator we also report the following sub-indicators:

Requests rejected or partially dealt with

The number of times that we have rejected a request or only provided partial information or no information in response to a request for one of the following reasons:

- Because it does not comply with local legislation for that type of requirement;
- Because it does not contain all the necessary elements to enable the execution (necessary signatures, competent authority, technical description of the requirement, etc.);
- Because it is technically impossible to execute the request.

Accesses affected

Number of accesses affected by each request. We count the affected URLs for the blocking and restriction of contents.

There may here may be notable variations in data for each of the indicators with respect to previous years or between countries, which are usually due to technical, methodological or legislative reasons. In addition, it should be noted that these are not audited data.

There may also be variations compared to previous years due to requests with a potential impact on the rights to freedom of expression and privacy; we identify such requests as "major events".

In this respect, we must highlight the situation of Venezuela, in which Telefónica must prioritise compliance with current legislation, the maintenance of connectivity in the country and the well-being of our employees.

Lastly, we would like to mention the international conflicts that are taking place in the world, such as those in Ukraine and Israel. Although we do not have a presence as an operator in these regions, we have a firm commitment and responsibility to consider the possible impacts that our activity could have on human rights in general and privacy and freedom of expression more specifically.

Report by country

Argentina
Brazil
Chile
Colombia
Ecuador
Germany
Mexico
Peru
Spain
Uruguay
Venezuela

Argentina

www.telefonica.com.ar

21,966
Total accesses

Accesses

2,239
Fixed telephony

17,841
Mobile telephony

1433
Fixed broadband

414
Pay TV

Accesses close of 2023 (data in thousands).

Telefónica has been present in Argentina since the privatisation of telephone services in 1990. Over these years, the company has developed into a leading group of companies specialising in integrated telecommunications.

Representing the first significant investment of Spanish capital, Telefónica Argentina contributed to the development of communications through infrastructure investments and a wide range of fixed and mobile telephony and Internet services.

Telefónica Argentina managed more than 21.9 million accesses at the end of December 2023.

With regard to the financial figures, Telefónica's revenue in Argentina stood at 1,237 million euros and OIBDA was 56 million euros.

Data at the end of 2023

Lawful interceptions

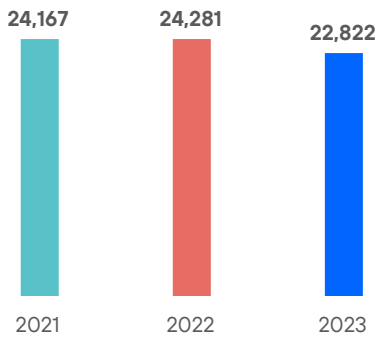
Legal framework

- National Constitution of Argentina, Article 18.
- Law 19,798, Inviolability of Communications, Articles 18 and 19.
- Law 27,078, Inviolability of Communications, Article 5.

Competent authorities

- Judges are the only ones authorised to request judicial intervention on access; prosecutors are the only ones in the case of an ongoing crime of extortive kidnapping, in which case they may request the intervention, which must be ratified by a judge within a maximum of 24 hours. In terms of procedure, the courts request the intervention of the so-called Directorate of Legal Assistance in Complex Crimes (DAJDECO), an agency of the National Supreme Court, which then formalises and follows up on the request for intervention from the service providers.

Requests



Breakdown of Interceptions (2023)

Access to metadata

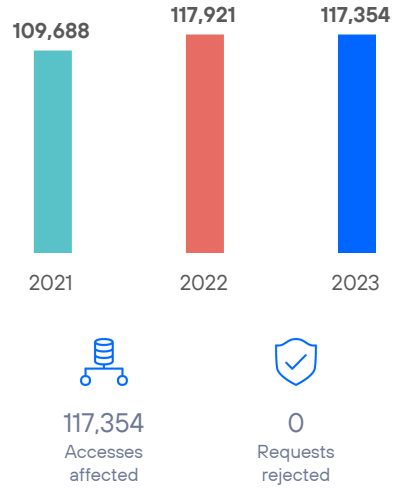
Legal framework

- National Constitution of Argentina, Article 18.
- Law 19,798, Inviolability of Communications, Articles 18 and 19.
- Law 27,078, Inviolability of Communications, Article 5.

Competent authorities

- Judges, prosecutors and the State security corps and bodies to which the investigation has been delegated.

Requests



Blocking and filtering of certain contents

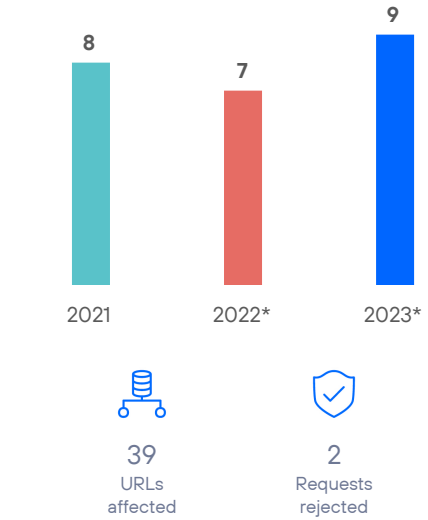
Legal framework

- Law 27,078, Inviolability of Communications, Article 5.

Competent authorities

- Judges, prosecutors and the State security corps and bodies to which the investigation has been delegated.

Requests



*Several sites were blocked by court order due to complaints of phishing, unauthorised online gambling, etc.

Geographical or temporary suspension of the service

Legal framework

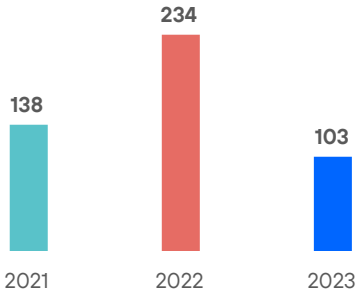
Although there is no specific rule governing this, it may be interpreted as part of what is established in Article 57 of Law 27,078, which stipulates:

Net neutrality. Prohibitions. ICT Service Providers may not: block, interfere with, discriminate against, hinder, degrade or restrict the use, sending, receiving, offering or accessing of any content, application, service or protocol except by court order or at the express request of the user.

Competent authorities

- In the absence of a specific rule, the only body competent for passing a measure to suspend the service in a given area is a judge with federal jurisdiction.

Requests



103* Accesses affected

0 Requests rejected

* Individual data blocking.

Brazil

www.telefonica.com.br

113,102
Total accesses

Accesses

6,458
Fixed telephony

99,070
Mobile telephony

6,655
Fixed broadband

845
Pay TV

Accesses close of 2023 (data in thousands).

Telefónica entered the Brazilian market in 1998, when the restructuring and privatisation of Telebrás was taking place.

Later, in 2002, Telefónica and Portugal Telecom created a joint venture to operate in the Brazilian mobile market and they began their commercial operations under the name Vivo in April 2003.

In 2015, Telefónica Brazil closed the acquisition of GVT, becoming the leading Brazilian integrated operator.

Telefónica Brazil managed more than 113 million accesses in Brazil at December 2023.

With regard to the financial figures, Telefónica's revenue in Brazil reached 9,650 million euros and OIBDA stood at 4,128 million euros.

Data at the end of 2023

Lawful interceptions

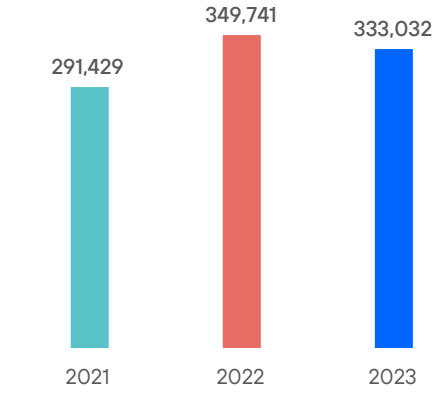
Legal framework

- Constitution of the Federal Republic of Brazil, Article 5.
- Law No. 9,296, 24/07/1996.
- Resolution 73/1998, under the terms of resolution 738/2020 of 12/21/2020.

Competent authorities

- In accordance with Article 3 of Brazilian Federal Law No. 9,296/1996 (Law on Interceptions), only the Judge (in the criminal sphere) can determine the interceptions (both telephonic and telematic), at the request of the Public Prosecutor or the Police Commissioner (Police Authority).

Requests



Breakdown of Interceptions (2023)

255,752
Registrations

ND
Extensions

6,886
Cancellations

262,638
Accesses affected

70,394
Requests rejected

Access to Metadata

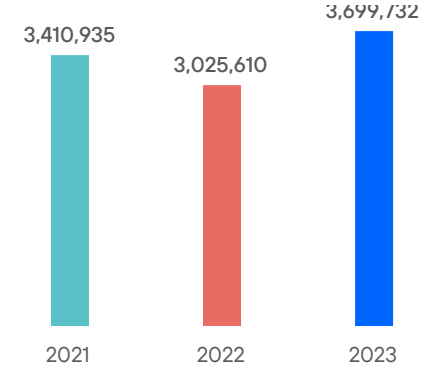
Legal framework

- Law No. 9,296, 24/07/1996.
- Law No. 9,472, Article 3, 16/07/1997.
- Law No. 12,683, Article 17 B, 09/07/2012.
- Law No. 12,830, Article 2, 20/07/2013.
- Law No. 12,850, Article 15, 20/08/2013.
- Law No. 12,965, Articles 7, 10 and 19, 23/04/2014.
- Decree No. 8,771, Article 1, 11/05/2016.
- Law No. 13,344, Article 11, 10/2016.
- Law No. 13,812, Article 10, 05/2019.
- Resolution No. 73 of 25 November 1998 / Regulation of Telecommunications Service - Article 65 - K .
- Resolution No. 632 of 7 March 2014 / General Regulation of Consumer Rights of Telecommunications Services - RGC - Article 3, V.

Competent authorities

- Public Prosecutor's Office, Police Commissioners and Judges in any sphere as well as the Chairs of the Parliamentary Investigatory Committees: the name and address of the registered user (subscriber data), as well as the identity of the communication equipment (including IMSI or IMEI).
- Judges in any sphere: data to identify the origin and destination of a communication (e.g., telephone numbers, internet service user names), date, time and duration of a communication and the location of the device.

Requests



Breakdown of Interceptions (2023)

3,567,796
Accesses affected

131,936
Requests rejected

Blocking and filtering of certain contents

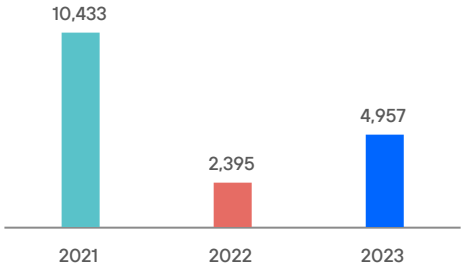
Legal framework

- Law No. 12,965, Articles 7 and 19, 23/04/2014.

Competent authorities

- Exclusively Judges.

Requests



4,863
Accesses affected

79
Requests rejected

68
Image copyrights

2,946
Copyright infringement

137
No reason declared

1,727
Copyright infringement - Piracy

Geographical or temporary suspension of the service

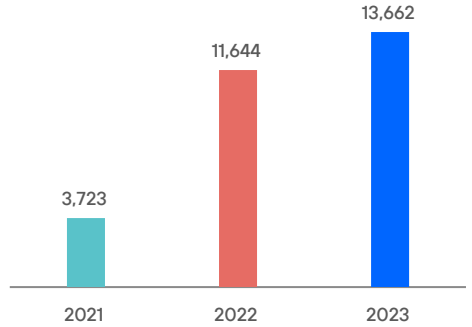
Legal framework

- Resolution No.73 of 25 November 1998 / Regulation of Telecommunications Service - Article 65-K

Competent authorities

Exclusively Judges.

Requests



12,727
Accesses affected

935
Requests rejected

Chile

www.telefonicachile.cl

11,599
Total accesses

Accesses

651
Fixed telephony

8,857
Mobile telephony

1,441
Fixed broadband

649
Pay TV

Accesses close of 2023 (data in thousands).

The Telefónica Group in Chile is a provider of telecommunications services (broadband, digital TV and voice) and, after reorganising its corporate structure, it completed the commercial brand unification process under the Movistar name in October 2009.

At the end of December 2023, Telefónica Chile managed more than 11.5 million accesses. With regard to the financial figures,

Telefónica's revenue in Chile stood at 1,946 million euros and OIBDA was 412 million euros.

Data at the end of 2023

Lawful interceptions

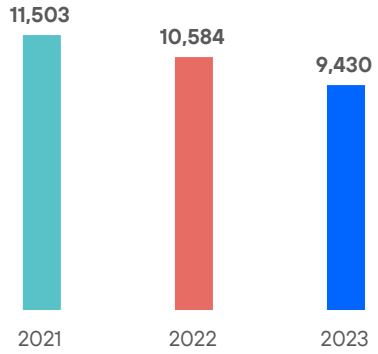
Legal framework

- No. 5 of Article 19 of the Political Constitution. Inviolability of Communications.
- Criminal Procedure Code, Articles 9, 219, 222, 223 and 224.
- Law 20,000. Traffic and control of narcotics, Article 24.
- Law 19,913 on money laundering.
- Law 18,314 that determines terrorist conduct. No.3, Article 14.
- Decree Law 211, Article 39 letter n).
- Law 19,974. National Intelligence System Law. Letters a), b), c) and d) of Article 24, in relation to Articles 23 and 28 of the same legal body.
- Criminal Procedure Code, Articles 177, 113 bis and 113 ter.
- Decree 142 of 2005 of the Ministry of Transport and Telecommunications, Regulation on the interception and recording of telephone communications and other forms of telecommunication.

Competent authorities

- Public Prosecutor's Office, by virtue of a prior judicial authorisation.
- State Intelligence Agencies, through the National Intelligence System with the authorisation of the Appeal Court Minister.
- The Police, by means of authorisation from the Examining Judge of the Crime (Inquisitorial Criminal Procedure).
- National Economic Public Prosecutor's Office, with the prior authorisation of the Court of Defence of Free Competition, approved by the respective Appeal Court Minister.

Requests



Breakdown of Interceptions (2023)

9,284 Registrations

542 Extensions

660 Cancellations

4,427 Accesses affected

146 Requests rejected*

*For technical reasons, rejected applications are not considered in the breakdown of registrations, extensions and cancellations.

Access to Metadata

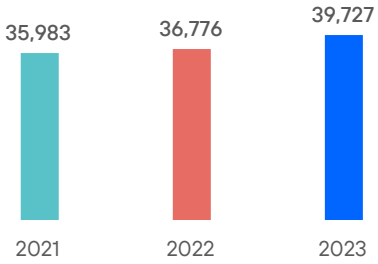
Legal framework

- No. 4 of Article 19 of the Political Constitution of the Republic of Chile, in accordance with the provisions of the sole article of Law 21,096: protection of your personal data. The processing and protection of this data will be carried out in the form and under the conditions determined by law.
- Article 218 bis and 218 ter in relation to Article 180 of the same legal text, under penalty of contempt of court, Article 240 of the Civil Procedure Code.
- Inquisitorial Criminal Procedure: Articles 120 bis and 171 of the Criminal Procedure Code.

Competent authorities

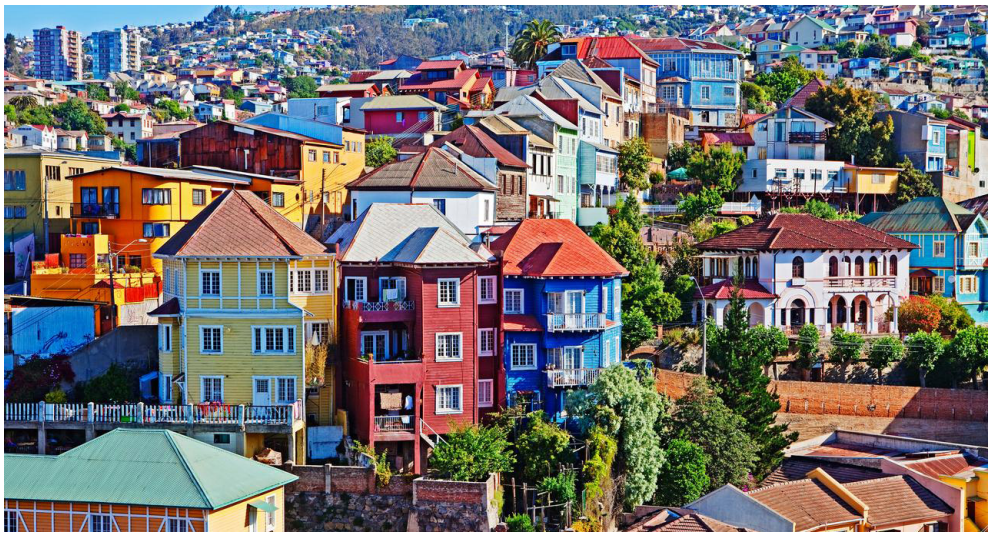
- Public Criminal Prosecutor: the Public Prosecutor's Office, by means of an order to investigate only personal data which are not covered by Constitutional Guarantees of Privacy and the Inviolability of Communications.
- Police with authorisation from the Public Prosecutor's Office and an order to investigate.
- Summary Judge in the Inquisitorial Criminal Procedure (Criminal Procedure Code).
- State Intelligence Agencies with prior legal authorisation.

Requests



29,605
Accesses affected

1,526
Requests rejected



Blocking and filtering of certain contents

Legal framework

- Law 17,336, on Intellectual Property. Article 85 Q, in relation to the provisions of article 85 R, letters a) and b), of the same legal text.
- Civil Procedure Code: Unnamed precautionary or interim measures.
- Criminal Procedure Code: Unnamed precautionary or interim measures.

Competent authorities

- Ordinary and special courts organisationally accountable to the Judicial Authority.
- Court of Defence of Free Competition, subject to the managerial, correctional and economic superintendence of the Supreme Court, with the knowledge of an adversarial process.

Requests

Geographical or temporary suspension of the service

Legal framework

There are no laws in the regulatory framework that allow for geographical or temporary service suspensions.

Competent authorities

Not applicable.

Requests

N/A	N/A	N/A
2021	2022	2023

0
Accesses affected

0
Requests rejected

Colombia

www.telefonica.co

25,129
Total accesses

Accesses

1,381
Fixed telephony

21,431
Mobile telephony

1,478
Fixed broadband

828
Pay TV

Accesses close of 2023 (data in thousands).

Telefónica has been present in Colombia since 2004. It began its activities in the mobile market, following the acquisition of Bellsouth's cellular operation in the country. Subsequently, in 2006, Telefónica acquired the control and management of Colombia Telecomunicaciones. Today, Telefónica provides voice, broadband and pay-television services in the country.

At December 2023,Telefónica Colombia managed 25 million accesses.

Telefónica's revenue in Colombia reached 1,497 million euros and OIBDA stood at 359 million euros.

Data at the end of 2023

Lawful interceptions

Legal framework

- Colombian Constitution, Articles 15 and 250.
- Law 599 of 2000 (Criminal Code) and Law 906 of 2004 (Criminal Procedure Code) (Article 200 amended by Article 49 of Law 1142 of 2007 and Article 235 amended by Article 52 of Law 1453 of 2011).
- Law 1621 of 2013. Intelligence and Counter Intelligence Law, Article 44.
- Decree 1704 of 2012, Articles 1-8, implementing Article 52 of Law 1453 of 2011, repealing Decree 075 of 2006 and laying down other provisions.
- Decree 2044 of 2013, Article 3, implementing Articles 12 and 68 of Law 1341 of 2009.
- Law 1273 of 2009, amending the Criminal Code, creating a new protected legal right - known as "data protection"- and integrally preserving the systems which use information and communication technology, among other provisions (Article 269C).

Competent authorities

- In Colombia, the sole competent authority for performing interception of communications is the Attorney General's Office, through its Judicial Police group.

Requests*

N/A	N/A	N/A
2021	2022	2023

N/A
Accesses affected

N/A
Requests rejected

*The Attorney General's Office in Colombia, as the competent authority in accordance with the Constitution and the Law, performs direct interceptions of mobile lines.

Access to metadata

Legal framework

- Colombian Constitution, Article 250.
- Law 599 of 2000 (Criminal Code) and Law 906 of 2004 (Criminal Procedure Code) (Article 200, amended).
- Law 1621 of 2013 (Intelligence and Counter Intelligence Law), Article 44.
- Decree 1704 of 2012, Articles 1-8, implementing Article 52 of Law 1453 of 2011, repealing Decree 075 of 2006 and laying down other provisions.
- Constitutional Court Ruling C-336 of 2007.
- Law 1273 of 2009 (Article 269F), amending the Criminal Code, creating a new protected legal right - known as "data protection"- and integrally preserving the systems which use information and communication technology, among other provisions.

Competent authorities

The applicable law currently in force is Law 906 of 2004 (Criminal Procedure Code).

Investigative bodies

a) Bodies, Article 200, amended by Law 1142 of 2007

The Attorney General's Office is responsible for making inquiries into and investigating acts constituting criminal offences which are brought to its notice through a complaint, lawsuit, special petition or any other suitable means.

b) Permanent judicial police bodies (Article 201, Criminal Procedure Code)

The functions of the judicial police are permanently exercised by the public servants vested with that function, belonging to the Technical Investigation Corps of the Office of the Attorney General and to the Nation and the National Police, through their specialized units.

In places in the national territory where there are no members of the judicial police of the National Police, these functions may be performed by the National Police.

c) Bodies which permanently perform special judicial police duties within their authority (Article 202, Criminal Procedure Code)

The following bodies perform specialised judicial police functions as part of criminal proceedings and within the scope of their authority:

1. Inspector General of the Nation.

2.Comptroller General of the Republic.

3. Transit authorities.

4. Public entities that perform oversight and control functions.

5. National and regional directors of the INPEC (National Penitentiary and Prison Institute), directors of prison establishments and custodial and surveillance personnel, in accordance with the Penitentiary and Prison Code.

6. Mayors.

7. Police inspectors.

In coordination with the Attorney General's Office, the directors of these entities will designate the public servants in their remit who will be part of the corresponding units.

d) Bodies that temporarily perform judicial police functions (Article 203, Criminal Procedure Code)

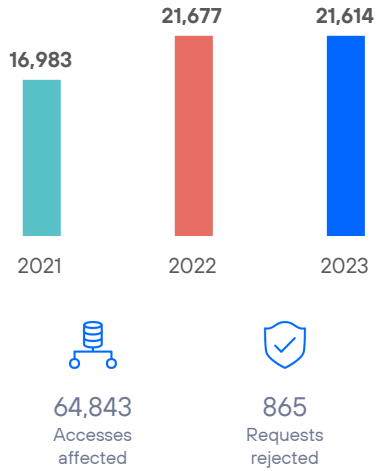
Judicial police functions are performed on a temporary basis by the public bodies authorised to do so by decision of the Attorney General's Office. These public bodies must act in accordance with the authorisation granted to them and in the matters which have been specified in the aforementioned decision.

e) Technical scientific body (Article 204, Criminal Procedure Code)

The National Institute of Legal Medicine and Forensic Science, in accordance with the law and the provisions of the Organic Statute of the Attorney General's Office of Colombia, will provide technical and scientific help and support in investigations carried out by the Attorney General's Office and bodies with judicial police functions. It will also do this with the defendant or their counsel, when they request it.

The Attorney General's Office, defendant or defendant's counsel will have recourse, when necessary, to Colombian or foreign private laboratories or laboratories of public or private universities, whether Colombian or foreign.

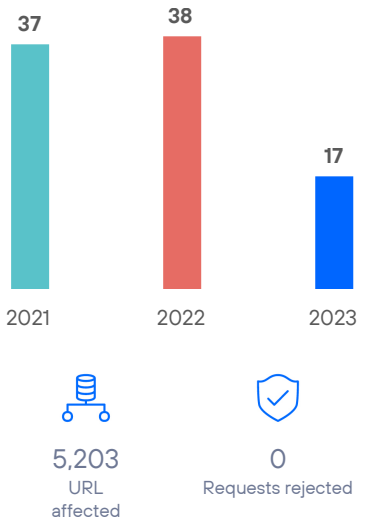
Requests*



*The values indicated are estimates based on technically available data.

Blocking and filtering of certain content

Requests*



*In September 2016, the WOLF Control de Contenidos platform became operational. This platform specialises in filtering all illegal content categorised by local authorities as such; e.g., child pornography.
The list continues to be updated and published on a regular basis through the web page of the Ministry of Information and Communication Technology (MinTIC).
The procedure for URL validation is:
1. Check information posted on the MinTEC portal on a regular basis, to determine if there are any new URLs which have been given a blocking order.
2. Analyse URLs posted. If there are new URLs, these are identified and uploaded to the DPI (Deep Packet Inspection) platform.
3. Analyse, block and unblock URLs. If it is necessary to block or unblock any URLs due to updates to the list, a work order is generated to be executed by the technical area.
4. Perform verification consultation. Once the work order has been executed, it is checked that the URLs which have blocking orders are currently blocked.
MinTIC is responsible for recording on a platform the list containing the blocking orders for both child abuse material and online gambling. Each operator is responsible for accessing the platform, validating whether there are any new orders and carrying out the corresponding blocks.

Child sexual abuse material

Legal framework

- Law 1098 of 2006 (Code on Children and Adolescents) and Law 1453 of 2011 reforming the Code on Children and Adolescents.
- Law 679 of 2001, which issued legislation to prevent and counter child exploitation, child pornography and child sexual tourism, pursuant to Article 44 of the Constitution (Articles 7 and 8).
- Decree 1524 of 2002, implementing Article 5 of Law 679 of 2001, in order to establish the technical and administrative measures intended to prevent access by children to any type of pornographic information on the Internet or on the different types of computer networks which can be accessed through global information networks (Articles 5 and 6).
- Law 1450 of 2011, which issued the 2010-2014 National Development Plan, Article 56.
- Law 1273 of 2009, amending the Criminal Code, creating a new protected legal right - known as "data protection" - and integrally preserving the systems which use information and communication technology, among

other provisions, Article 269G, Article 269F.

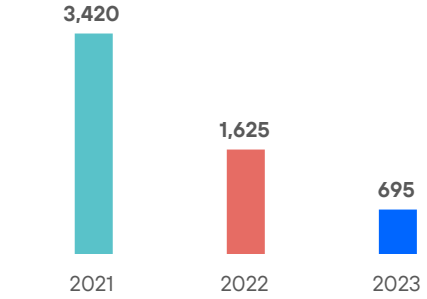
- CRC (Communications Regulatory Commission) Ruling 3502 of 2011.

Competent authorities

- Judicial police with a court order from a supervisory judge.
- Supervisory judge.
- Judicial authorities, with intelligence and counter intelligence units (National Police; military forces; UIAF - Information and Financial Analysis Unit).

The National Police sends the Ministry of Information and Communication Technology a list of the URLs issued with blocking orders so that the Ministry can publish it on its website and it can be consulted by Internet Service Providers (ISPs). To access this list, the ISPs must have a username and password, provided in advance by the Ministry, so as to prevent anyone from browsing the URLs issued with a blocking order due to containing child pornography material.

No. of URLs*



* Number of URLs added to the list published by MinTIC during the year.

Illegal gambling

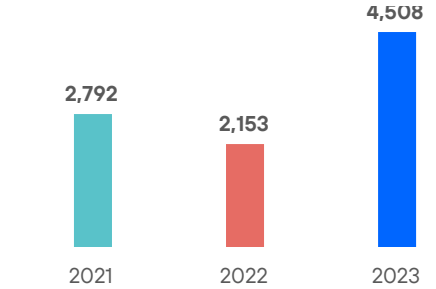
Legal framework

- Law 1753 of 2015, amending the Criminal Code, creating a new protected legal right - known as "data protection"- and integrally preserving the systems which use information and communication technology, among other provisions (Article 93, paragraph 3).
- Law 1450 of 2011, Article 56.
- CRC (Communications Regulatory Commission) Ruling 3502 of 2011.

Competent authorities

Coljuegos, a state-owned industrial and commercial company in charge of the administration of the state monopoly on games of chance and gambling, in conjunction with the National Police, identifies web portals which commercialise unauthorised games of chance and gambling and requests the Ministry of Information and Communication Technology to inform the ISPs of the list of URLs that they must block.

No. of URLs*



* Number of URLs added to the list published by MinTIC during the year.

Court order

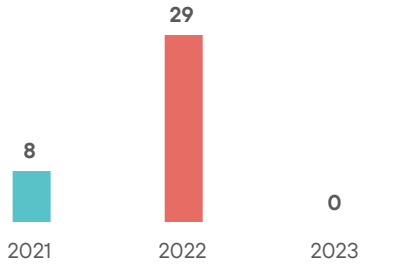
Legal framework

- Law 599 of 2000 (Criminal Code) and Law 906 of 2004 (Criminal Procedure Code)
- Constitutional Court Ruling C-897 of 2005
- Constitutional Court Ruling C-600 of 2019
- Constitutional Court Ruling C-243 of 1996

Competent authorities

The Attorney General's Office and the Superintendence of Industry and Commerce, as part of the investigations they carry out, request the Ministry of Information and Communication Technology to inform the ISPs of the URLs that they must block.

No. of URLs*



* Number of URLs added to the list published by MinTIC during the year.

Geographical or temporary suspension of the service

Legal framework

- Law 1341 of 2009, Article 8. Cases of emergency, upheaval, disaster and prevention.
- Decree 2434 of 2015, CRC (Communications Regulatory Commission) Ruling 4972 of 2016 - this makes it obligatory to prioritise calls between authorities to deal with emergencies.
- This prioritisation means terminating calls by users who are not on the list of numbers.

Competent authorities

Priority will be given to the authorities in the transmission of free and timely communications in order to prevent disasters, when such communications are considered essential.

Requests

0
Accesses affected

0
Requests rejected

Ecuador

www.telefonica.com.ec

5,501
Total accesses

Accesses

2
Fixed telephony

5,486
Mobile telephony

7
Fixed broadband

0
Pay TV

Accesses close of 2023 (data in thousands).

In Ecuador, Telefónica began its operations in 2004, with the acquisition of BellSouth's mobile operation in the country (which, at that time, was the second largest operator in Ecuador, with 816,000 customers and a market share of 35%).

Telefónica managed more than 5.5 million accesses in Telefonica Ecuador at the end of 2023.

Telefónica's revenue in Ecuador stood at 461 million euros and OIBDA was 186 million euros.

Data at the end of 2023

Lawful interceptions

Legal framework

- Organic Integral Penal Code, Articles 476 and 477.
- Concession Contract signed between OTECEL S.A. and the Ecuadorian State.

Competent authorities

- Competent prosecutor within an investigation.

Requests*

*The Attorney General's Office of Ecuador, as the competent authority in accordance with the law, carries out the interceptions directly.

Access to metadata

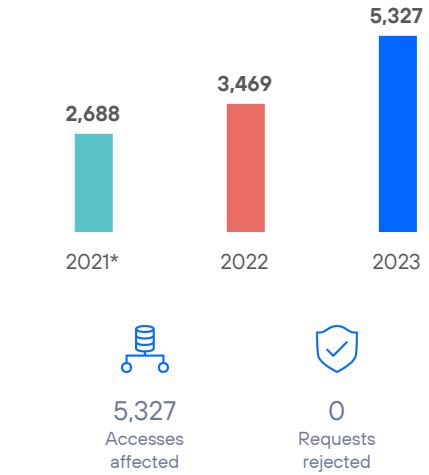
Legal framework

- Organic Integral Penal Code, Article 499.

Competent authorities

- Judges of Criminal Guarantees.

Requests



* Most of the 2021 requests were delayed files from 2020 due to Covid. The judicial and prosecution authority suffered outbreaks of the Covid pandemic (especially in Quito and Guayaquil).

Blocking and filtering of certain contents

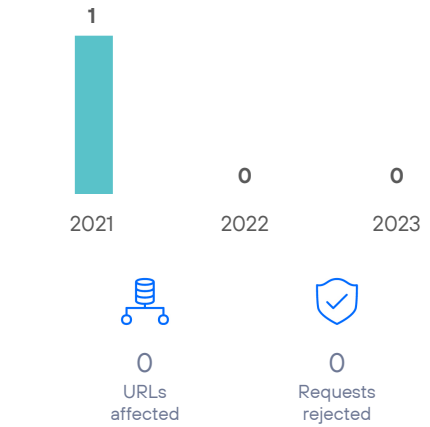
Legal framework

- Organic Integral Penal Code, Article 583.
- Organic Code of the Social Knowledge Economy, Articles 563 and 565.

Competent authorities

- The Prosecutor can, in a well-founded manner, request authorisation from the Judge of Criminal Guarantees to proceed.
- The SENADI (National Intellectual Rights Service) may order precautionary measures.

Requests



Geographical or temporary suspension of the service

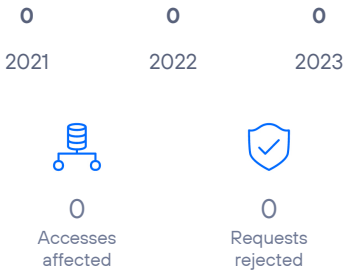
Legal framework

Constitution of Ecuador, Articles 164 and 165.

Competent authorities

Those that the President of the Republic delegates on behalf of the President, in accordance with the circumstances reflected by the Law.

Requests



Germany

www.telefonica.de

49,832
Total accesses

Accesses

2,300
Fixed telephony

45,072
Mobile telephony

2,384
Fixed broadband

0,0
Pay TV

Accesses close of 2023 (data in thousands).

Telefónica has been in the country for many years and operates under the commercial brand O2.

Telefónica Germany offers its private and business customers post-paid and prepaid mobile telecom products as well as innovative mobile data services based on the GPRS and LTE technologies. In addition, the integrated communications provider also offers ADSL, VDSL fixed network telephony and high-speed Internet. Telefónica manages 49.8 million accesses in Germany.

Telefónica's revenue in Germany reached 8,614 million euros and OIBDA was 2,640 million euros.

Data at the end of 2023

Lawful interceptions

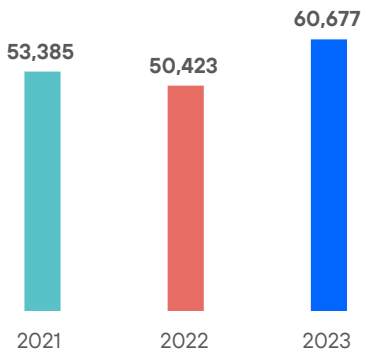
Legal framework

- Telecommunications Act, Section 170 (*Telekommunikationsgesetz* - TKG).
- StPO. The German Code of Criminal Procedure.
- Law G10, Section 100, Article 10 (Gesetz - G10).
- Customs Investigation Services Act (ZFDG).
- Federal Criminal Police Office Act (BKAG).
- Police Acts of the federal states (*Landespolizeigesetze*).

Competent authorities

- Law Enforcement Agencies (LEAs), e.g., Police Authorities (national and federal), Intelligence Agencies and Customs Investigations Services (national and federal).
- Measures corresponding to Sec. 100a German Code of Criminal Procedure (StPO) require a prior court order. In case of exigent circumstances, the public prosecutor's office can issue an order as well, which must be confirmed by the court within three working days in order to be effective.

Requests



Breakdown of Interceptions (2023)

34,634 Registrations

9,985 Extensions

16,058 Cancellations

60,677 Accesses affected

0* Requests rejected

* This result is due to the fact that the Authorities are challenged to correct incomplete requests.

Access to metadata

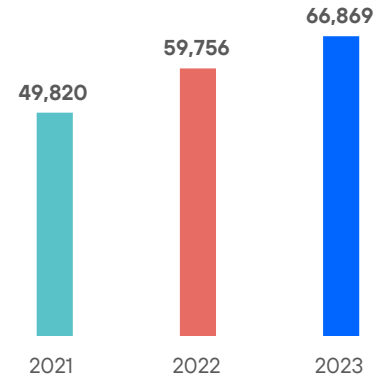
Legal framework

- Sections 9 and 12 of the German Telecommunications and Telemedia Data Protection Act, and Section 176 of the Telecommunications Act.
- Sec. 100g German Code of Criminal Procedure (*Strafprozessordnung* - StPO).
- Police Acts of the federal states *(Landespolizeigesetze).*

Competent authorities

- Law Enforcement Agencies (LEAs), e.g., Police Authorities (national and federal), Intelligence Agencies and Customs Investigations Services (national and federal).
- Measures corresponding to Sec.100a German Code of Criminal Procedure (StPO) require a prior court order. In case of exigent circumstances, the public prosecutor's office can issue an order as well, which must be confirmed by the court within three working days in order to be effective.

Requests



509,928 Accesses affected

0* Requests rejected

* This result is due to the fact that the authorities are asked to correct incomplete requests.

Blocking and filtering of certain contents

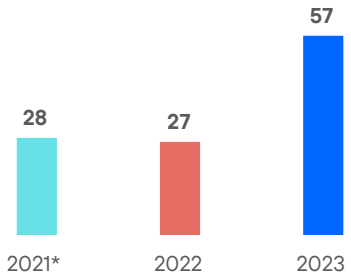
Legal framework

There are no laws in the regulatory framework that allow blocking and filtering.*

Competent authorities

Not applicable.

Requests



237** URLs affected

0*** Requests rejected

* In 2021, the CUII sector agreement was implemented to perform blocking due to content piracy.

** Typology: 158: Intellectual property; 28: European Regulation (EU) 2022/350; 10: Telefónica internal; 1: Regulation of the Bavarian New Media Authority; 1:Federal Office for Information Security.

***This result is due to the fact that the authorities are asked to correct incomplete requests.

Geographical or temporary suspension of the service

Legal framework

There are no laws in the regulatory framework that allow geographical or temporary suspensions of the service.

Competent authorities

Not applicable.

Requests

N/A	N/A	N/A
2021	2022	2023

N/A Accesses affected

N/A Requests rejected

Mexico

www.telefonica.com.mx

24,121
Total accesses

Accesses

344	23,774	3	0
Fixed telephony	Mobile telephony	Fixed broadband	Pay TV

Accesses close of 2023 (data in thousands).

Telefónica Mexico has participated and competed in the mobile telecommunications market since 2001 and promotes the development of telecommunications in the country. It currently has the best national coverage, with over 114,666 locations and 14,886 km.

The commercial offers are available in 299 Customer Service Centres (CAC), and more than 3,600 indirect points of sale throughout the country.

Telefónica in Mexico managed more than 24.1 million accesses in December 2023.

With regard to the financial figures, Telefónica's revenue in Mexico stood at 1,318 million euros and OIBDA was 129 million euros.

Data at the end of 2023

Lawful interceptions

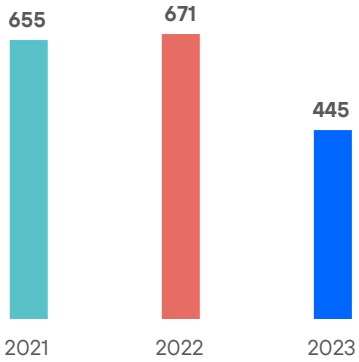
Legal framework

- Political Constitution of the United Mexican States, Article 16, paragraph 12.
- National Criminal Procedure Code, Article 291.
- Federal Law Against Organised Crime, Article 16.

Competent authorities

- The federal judicial authority determines whether the request of the investigating authority concerning intervention of communications is appropriate, ordering the concession holder to establish the measure for a certain period of time.

Requests



Breakdown of Interceptions (2023)

443 Registrations

9 Extensions

332 Cancellations

875 Accesses affected

2 Requests rejected

Access to metadata

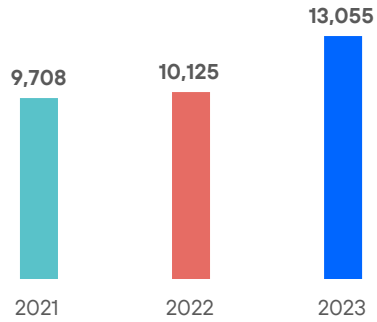
Legal framework

- Federal Law on Telecommunications and Broadcasting, Article 190.
- National Criminal Procedure Code, Article 303.
- Law on General Channels of Communications, Article 122.

Competent authorities

- The heads of the security and justice procurement authorities shall designate the public servants responsible for managing the requests made to the concession holders and receiving the corresponding information, by means of agreements published in the Official Gazette of the Federation.

Requests



24,155 Accesses affected

611 Requests rejected

Blocking and filtering of certain content

Legal framework

- There are no laws in the regulatory framework that allow blocking and filtering of certain content.

Competent authorities

- Not applicable.

Requests

2021	2022	2023
N/A	N/A	N/A

0	0
URLs affected	Requests rejected

Geographical or temporary suspension of the service

Legal framework

There are no laws in the regulatory framework that allow for geographical or temporary service suspensions.

Competent authorities

Not applicable.

Requests

2021	2022	2023
N/A	N/A	N/A

0	0
Accesses affected	Requests rejected

Peru

www.telefonica.com.pe

14,052
Total accesses

Telefónica began to operate in the Peruvian market in the mid-1990s.The company managed more than 14 million accesses at the end of December 2023.

Regarding financial figures, Telefónica's revenue in Peru stood at 1,591 million euros and the OIBDA was 301 million euros.

Accesses

964
Fixed telephony

10,454
Mobile telephony

1,661
Fixed broadband

949
Pay TV

Accesses close of 2023 (data in thousands).

Data at the end of 2023

Lawful interceptions

Legal framework

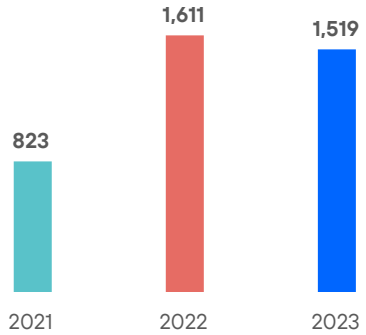
- Political Constitution of Peru, Article 2, paragraph 10.
- Telecommunications Law (Supreme Decree No. 013-93-TCC - Article 4) and its Regulations (Supreme Decree No. 020- 2007-MTC - Article 13).
- Law No. 27697: Law that grants power to the prosecutor for the intervention and control of communications and private documents in exceptional cases.

In all the concession contracts there is a clause related to the secrecy of telecommunications and the protection of personal data which establishes that the company will safeguard them and maintain the confidentiality of the personal information related to their customers, unless there is a specific court order.

Competent authorities

- Judges (Judicial Authority).
- Public Prosecutor's Office of the Nation, Criminal Prosecutors and Public Prosecutors, with the authorisation of the Judge.

Requests



Breakdown of Interceptions (2022)

1,433	74	0
Registrations	Extensions	Cancellations

9,658	12
Accesses affected	Requests rejected*

*For technical reasons, rejected requests are not considered in the breakdown of registrations, extensions and cancellations.

Access to metadata

Legal framework

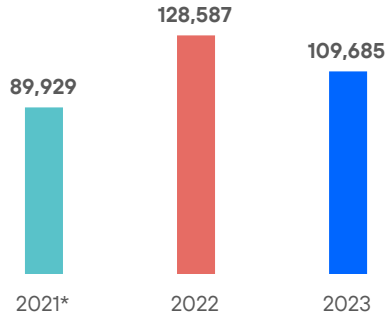
- Political Constitution of Peru, Article 2, paragraph 10.
- Telecommunications Law (Supreme Decree No. 013-93-TCC - Article 4) and its Regulations (Supreme Decree No. 020- 2007-MTC - Article 13).
- Law No. 27697: Law that grants power to the prosecutor for the intervention and control of communications and private documents in exceptional cases.
- Law No. 31284: IMEI Geolocation information.
- Legislative Decree No. 1182 which regulates the use of telecommunications for the identification, location and geolocation of communication equipment in the fight against delinquency and organised crime.

In all the concession contracts there is a clause related to the secrecy of telecommunications and the protection of personal data which establishes that the company will safeguard them and maintain the confidentiality of the personal information related to their customers, unless there is a specific court order.

Competent authorities

The heads of the judicial authorities, Public Prosecutor's Office and National Police will designate the public servants responsible for managing the requests made to the operators and receiving the corresponding information.

Requests



99,797	1,111
Accesses affected	Requests rejected

*This number includes geolocation and call reports.

Blocking and filtering of certain contents

Legal framework

- Copyright Law.

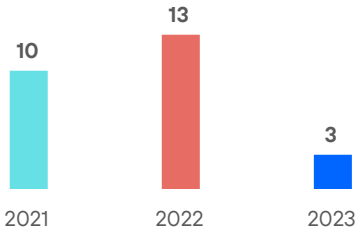
Competent authorities

- INDECOPI (National Institute for the Defence of Competition and Intellectual Property).

Strictly speaking, there has been no legislative change; there is no authority that can block web content, except the Judicial Authority. However, there is an exception in the case of INDECOPI. Under Article 169 of the Copyright Law, the Copyright Commission of INDECOPI (National Institute for the Defence of Competition and Intellectual Property) has the power to issue preventive or precautionary measures and to sanction ex officio, at the request of a party, infringements or violations to national copyright law, and related rights, and is able to warn, seize, confiscate, and order the temporary or definitive closure of the establishments where the offence is committed.

For INDECOPI, to the extent that through the websites acts would be performed that violate the right to public communication by complainant companies, the administration can order the blocking, in Peruvian territory, of access to the offending website, through blocking based on DNS or URLs.

Requests*



380
URLs affected

0
Requests rejected

*INDECOPI requests (precautionary measures due to intellectual property cases).

Geographical or temporary suspension of the service

Legal framework

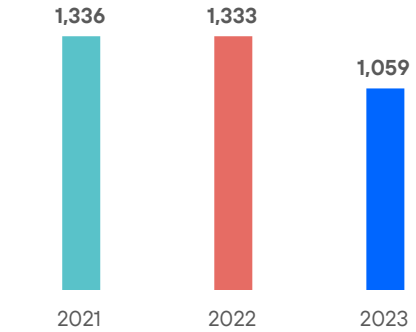
Telecommunications Law Regulations (D.S. No. 020-2007-MTC - Articles 18 and 19).

The concession contracts establish that, in the event of an emergency, crisis or a threat to national security, the concession holder will provide telecommunication services, prioritising actions to support the State and following the instructions of the Ministry of Transport and Communications (MTC).

Competent authorities

- Ministry of Transport and Communications (MTC).
- National and Civil Defence System.

Requests



1,059
Accesses affected

0
Requests rejected

Spain

www.telefonica.es

40,992
Total accesses

Accesses

7,948
Fixed telephony

20,115
Mobile telephony

5,918
Fixed broadband

3,426
Pay TV

Accesses close of 2023 (data in thousands).

Telefónica operates in Spain mainly in the fixed and mobile telephony sector, using broadband as the key tool for developing both businesses, along with IT and solutions services.

Telefónica Spain is the leading provider of telecommunication services in Spain by number of accesses, including voice, data, television and internet access. Additionally, it offers its customers the most innovative services and cutting edge technology to achieve its aim of becoming the top digital telco.

Telefónica Spain handled almost 41 million accesses at the end of December 2023.

Revenue from operations amounted to 12,654 million euros and OIBDA reached 3,229 million euros in 2023.

Data at the end of 2023

Lawful interceptions

Legal framework

- Spanish Constitution, Article 18.
- Criminal Procedure Code, Article 588.
- Law 11/2022, General Telecommunications, Article 59. In addition, this law includes what is established in Royal Decree Law 14/2019, of 31 October, by which urgent measures are adopted for reasons of public security in the field of digital administration, public sector procurement and telecommunications. Thus, there is new wording of Article 4(6) and Article 111(1).
  - Article 4(6): "The Government may, exceptionally and temporarily, agree to the direct management or intervention by the General State Administration of electronic communications networks and services in certain exceptional cases which could affect public order, public safety and national security. In particular, this exceptional and transitional power of direct management or intervention may affect any infrastructure, associated resource or element or level of the network or service that is necessary to preserve or restore public order, public safety and national security.

    Likewise, in the event of non-compliance with the public service obligations referred to in Title III of this Law, the Government, following a mandatory report from the National Commission for Markets and Competition, and also on an exceptional and transitory basis, may grant the General State Administration direct management or intervention of the corresponding services or operation of the corresponding networks.

    The agreements to take over the direct management of the service and the intervention or those to intervene in or operate the networks referred to in the preceding paragraphs shall be adopted by the Government on its own initiative or at the request of any competent public administration.

    In the latter case, it will be necessary that the public administration has jurisdiction as regards security issues or for the provision of the public services affected by the abnormal functioning of the service or the network of electronic communications. In the event that the procedure is initiated at the request of an administration other than that of the State, the latter shall be deemed an interested party and may prepare a report prior to the final resolution."
  - Article 81(1): "Prior to the beginning of the sanctioning procedure, the cessation of the alleged infringing activity may be ordered by the competent body of the Ministry of Economy and Enterprise, by resolution without prior hearing, where there are reasons of overriding urgency based on any of the following assumptions:

    a) Where there is an immediate and serious threat to public order, public safety or national security.

    b) Where there is an immediate and serious threat to public health.
    c) When the alleged infringing activity may result in serious damage to the operating of public law enforcement, civil protection and emergency services.

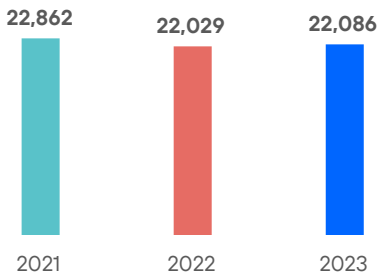
    d) Where there is serious interference with other electronic communications services or networks.

    e) When it creates serious economic or operational problems for other suppliers or users of electronic communications networks or services or other users of the radio spectrum."

Competent authorities

- Judges of the Examining Magistrates' Courts.
- Exceptional cases (emergencies, armed groups): the Minister of the Interior or the Secretary of State for Security. In 24 hours the judge shall ratify or revoke the request.
- The Government, on an exceptional basis, may agree to the assumption by the General State Administration of the direct management or intervention of networks and electronic communications services in certain exceptional cases that may affect public order, public safety and national security.

Requests



Breakdown of Interceptions (2022)

9,697 Registrations

8,646 Extensions

3,743 Cancellations

8,871 Accesses affected

2,653 Requests rejected

Access to metadata

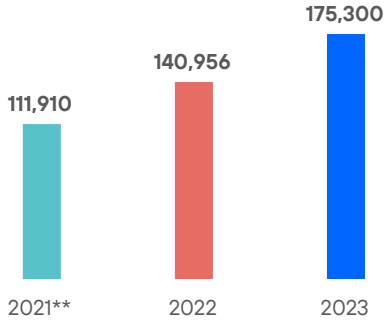
Legal framework

- Law 25/2007, Law on Data Conservation, Articles 1-10.
- Law 11/2022, General Telecommunications Law, Article 61.

Competent authorities

- Courts.
- Judicial Police and Public Prosecutor's Office (Organic Law 13/2015 amending the Criminal Procedure Code).

Requests



N/D* Accesses affected

7,829 Requests rejected

* The nature of certain requests and the configuration of the tools mean that it is not possible to provide this information.

**The new system for sending orders from the competent authorities has been extended and generalized in 2022. Under this system, requests are counted individually, unlike the previous system in which one order could contain several requests.

Blocking and filtering of certain contents

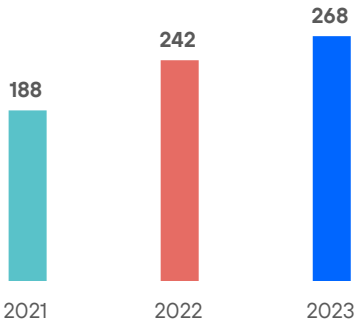
Legal framework

- Royal Decree 1889/2011, Articles 22 and 23 which regulate the operation of the Intellectual Property Commission, 30/12/2011
- Revised Text of the Intellectual Property Law, Article 138, approved by Royal Legislative Decree 1/1996, 12/04/1996.
- Law 34/2002, Article 8, on information society services and electronic commerce, 11/07/2002.

Competent authorities

- Mercantile/Civil/Cont. Administrative/ Criminal Courts.
- National Intellectual Property Commission.
- General Gambling Directorate.
- Spanish Agency for Medication and Healthcare Products.

Requests



Intellectual property

No. of requests 2022	2023	No. of URLs affected 2022	2023
190	221	7,485	10,704

Crimes

No. of requests 2022	2023	No. of URLs affected 2022	2023
36	28	147	36

Medication

No. of requests 2022	2023	No. of URLs affected 2022	2023
5	7	24	55

Illegal gambling

No. of requests 2022	2023	No. of URLs affected 2022	2023
11	11	1,934	3,323

13,972
URLs affected

3
Requests rejected

*Of the total requests, four are continuous throughout the reporting period. The execution of dynamic blocking processes is authorised, by sending lists (three weekly lists and one monthly list):
1) Two by Judgments of the Mercantile Courts 6 and 9 of Barcelona. The first for TAD-Movistar Plus+ and the second jointly relating to LaLiga and TAD-Movistar Plus+, which authorise the weekly sending of lists with domains to block;
2) Protocol, at the initiative of the Ministry of Culture, which develops what was agreed in judgments and judicial orders, enabling the weekly sending of a list with domains to block;
3) Judgment unifying others from the Mercantile Courts of Barcelona, which authorizes the sending of a monthly list with domains to block from MPA (Motion Picture Association) members. All enable a list of URLs/domains to be prepared and sent, weekly and monthly, which Telecommunications Operators/Internet Access Providers in Spain must block.

Geographical or temporary suspension of the service

Legal framework

There are no laws in the regulatory framework that allow for geographical or temporary service suspensions.

Competent authorities

Not applicable.

Requests

N/A	N/A	N/A
2021	2022	2023

N/A
Accesses affected

N/A
Requests rejected

Uruguay

www.telefonica.com.uy

1,567
Total accesses

Accesses

0	1,567	0	0
Fixed telephony	Mobile telephony	Fixed broadband	Pay TV

Accesses close of 2023 (data in thousands).

Telefónica has been present in Uruguay since 2005.

The company managed more than 1.5 million accesses at the end of December 2023. Telefónica's revenue in Uruguay reached 223 million euros and OIBDA was 110 million euros.

Data at the end of 2023

Lawful interceptions

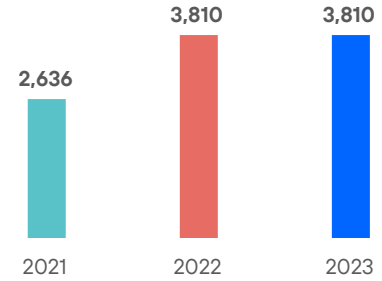
Legal framework

- Constitution of the Republic, Article 28.
- Law 19574, Article 62
- Decree I/1113 of 13 March 2014.
- Decree 359/021 of 26 October 2021

Competent authorities

- Criminal judges in charge of an investigation, at the request of the Public Prosecutor's Office and through the UNATEC (agency of the Ministry of the Interior responsible for centralising such requests).

Requests



Breakdown of Interceptions (2022)

2,121 Registrations

1,232 Extensions

457 Cancellations

2,119 Accesses affected

2 Requests rejected*

*The two rejected requests are already included as applications in the Registrations.

Access to Metadata

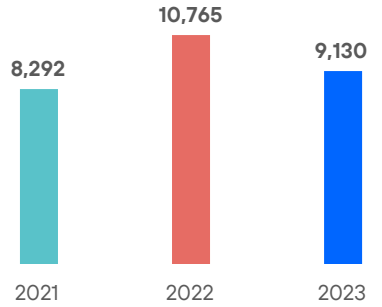
Legal framework

- Constitution of the Republic, Article 28.
- Law 19574, Article 62.
- Decree I/1113 of 13 March 2014
- Decree 359/021 of 26 October 2021

Competent authorities

- Judges, by means of a written and well-founded request.

Requests



9,130 Accesses affected

3 Requests rejected

Blocking and filtering of certain contents

Legal framework

- Law 19,535 of 25 September 2017, Articles 244 and 245.
- Decree 366/2017 regulated the provisions of Articles 244 and 245 of Law 19,535, 21/12/2017.
- Law 19,924 article 712.- Decree 345/2022

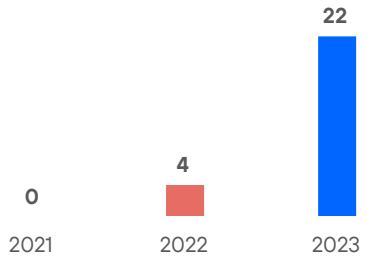
Competent authorities

The Executive Branch is empowered to take the necessary preventive and punitive measures to prevent the proliferation of Internet gaming marketing activities, in particular the blocking of access to websites.

The dissemination of television services for subscribers through the Internet or similar network, for commercial purposes, by a natural or legal person who is not authorized to offer said signals, in violation of the provisions of Laws No. 9,739, of 17 December 1937 (Copyright Law) and No. 17,616, of 10 January 2003, and its amendments, may be administratively sanctioned.

For these purposes, the Communications Services Regulatory Unit (URSEC) is empowered to adopt sanctioning and preventive measures in accordance with the provisions below and the regulations issued from time to time by the Executive Branch (Article 712 – Law 19,924).

Requests*



177
URLs affected

0
Requests rejected

*Online gambling and sports betting.

Geographical or temporary suspension of the service

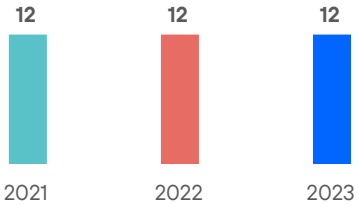
Legal framework

Law 19,355, Article 166: this enables the Ministry of the Interior to block the entry of calls from telephone services to the 911 Emergency Service when there are duly documented records accrediting the irregular use of such communications on a repeated basis (more than three communications in the month or six in the year).

Competent authorities

Ministry of the Interior (Executive Branch).

Requests*



1,083
Accesses affected

0
Requests rejected

*Suspension notifications by the authority. Temporary suspension for a period of 3 to 6 months.
*The values indicated are estimates based on technically available data.

Venezuela

www.telefonica.com.ve

8,640
Total accesses

Accesses

98	8,536	2	0
Fixed telephony	Mobile telephony	Fixed broadband	Pay TV

Accesses close of 2023 (data in thousands).

The Telefónica Group has operated mobile telephony services in Venezuela since 2005.

The company has a comprehensive range of services in Venezuela, with products in mobile internet, digital television and mobile and landline telephony.

In 2023, Telefónica's revenue in Venezuela was 112 million euros.

Data at the end of 2023

Lawful interceptions

Legal framework

- Organic Criminal Procedure Code, Articles 205 and 206.
- Decree with Rank, Value and Force of the Organic Law of the Police Investigation Service, the Scientific, Penal and Criminal Investigations Corps and the National Service of Medicine and Forensic Science, Article 42.

Competent authorities

- The Public Prosecutor's Office, through its prosecutors.
- The Scientific and Criminal Investigation Service Corps (CICPC).
- The Bolivarian National Intelligence Service (upon the request of the Public Prosecutor and the authorisation of the corresponding judge).
- The police corps duly empowered to exercise powers in criminal investigations.
- National Experimental University of Security; other special criminal investigation entities and bodies.

Access to Metadata

Legal framework

- Administrative Ruling No. 171. Rules concerning the collection or capture of personal data from applicants for mobile and fixed telephony services via wireless networks or non-geographic number with nomadic voice service.
- Law against Kidnapping and Extortion, Article 29.

Competent authorities

- The Public Prosecutor's Office.
- The Scientific, Penal and Criminal Investigation Service Corps (CICPC).
- The components of the Bolivarian National Armed Forces, within the limits of their competence.
- The police intelligence authorities.
- The National Police Corps, within the limits of its auxiliary criminal investigation duties.
- Any other auxiliary criminal investigation body whose intervention is required by the Public Prosecutor's Office.

Blocking and filtering of certain contents

Legal framework

- Organic Law on Telecommunications, Article 5.
- Law on Social Responsibility in Radio, Television and Electronic Media, Article 27.

Competent authorities

- National Telecommunications Commission (CONATEL).

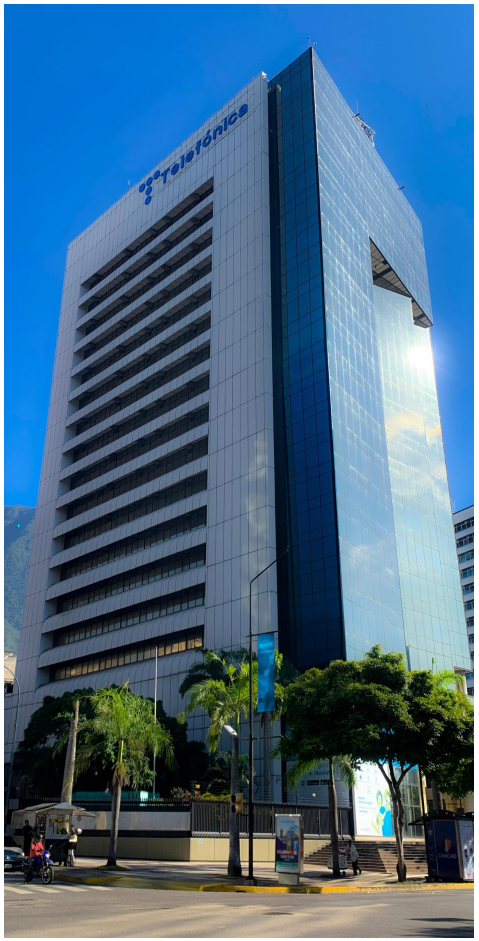
Geographical or temporary suspension of the service

Legal framework

Organic Law on Telecommunications, Article 5.

Competent authorities

- Ministry of Transport and Communications (MTC).
- National and Civil Defence System.



Glossary

Concept	Explanation
Competent Authority	Judges and courts, state security forces and bodies and other administrations or governmental bodies that are empowered by the law to make the requests relevant to this report. The Competent Authorities may vary according to the type of request and the applicable legislation in each of the countries.
Personal Data	Personal data means any information which refers to an identified or identifiable person, such as his or her name and address, the recipients of his or her communications, the location, the content of the communications, the traffic data (days, time, recipients of the communications, etc.).
Location Data	The location data may refer to the latitude, longitude and altitude of the user's terminal equipment, the direction of travel, the level of accuracy of the location information, the identification of the network cell in which the terminal equipment is located at a certain moment or the time at which the location information has been recorded.
Traffic Data	Any data processed for the purposes of conducting communication through an electronic communications network or for invoicing purposes.
DPI	These initials stand for Deep Packet Inspection. DPI identifies situations involving noncompliance with technical protocols, viruses, spam or invasions, but it can also use pre defined criteria different from those annotated to decide whether a packet can pass through or whether it needs to be routed to a different destination or given another priority or bandwidth allocation, to collect information for statistical purposes or simply to eliminate it.

Concept	Explanation
IMEI	These initials stand for International Mobile Equipment Identity. It has a serial number which physically identifies the terminal. The IMEI enables the operator to identify terminals which are valid and, therefore, can connect to the network.
IMSI	These are the initials which stand for International Mobile Subscriber Identity. It is the identifier of the line or service. This number is used to route calls and to obtain the country or network to which it belongs.
IOCCO	These are the initials which stand for Interception Of Communications Commissioner's Office in the UK. It is responsible for keeping under review the interception of communications and the acquisition and circulation of communications data by intelligence agencies, police forces and other public authorities. It submits biannual reports to the Prime Minister regarding the execution of the functions of the Communications Interception Commissioner.
MAJOR EVENTS	There are certain situations of force majeure which may lead to the following actions: **1. Service restriction or denial** (including SMS, voice, email, voicemail, internet and other services) entailing limitation of freedom of expression. Examples: • Restricting or denying services on a national scale. • Restriction or denial of access to a website/ websites for political reasons (such as Facebook pages, news websites such as bbc.co.uk, the opposition party's websites prior to elections or human rights groups' websites). • Specific shutdown of any kind of telecommunications services, resulting from political causes (e.g., concerning a small number of cells).

Concept	Explanation
***MAJOR EVENTS* (cont.)**	• Denying certain clients access to specific services or networks in order to limit said individuals' legitimate freedom of expression. **2. Network shutdown/access control.** Examples: • Total shutdown of a national network. • Access control involving a specific area or region, motivated by political reasons. **3. Legally unfounded interceptions.** • Situations in which the authorities intercept communications without any legal grounds for reasons of *force majeure*. **4. Communications imposed by the authorities.** Examples: • Sending politically motivated messages/communications to our customers on behalf of governments or government agencies. **5. Substantial operational changes.** Examples: • Substantial operational or technical changes or change proposals concerning surveillance services (such as data access, retention or interception) aimed at reducing the operator's control in terms of supervising such activities (e.g., procedural changes allowing direct access on the part of a governmental agency/ government). • A procedural change to establish widespread surveillance. **6. Substantial legal changes.** (substantial changes, or proposed changes, to laws providing governmental authorities with more power to impose requests on operators). Example: • Changes in the communication interception laws.
PSI	The PSI or Portal de Servicio Interno (Internal Service Portal) is an inquiry application, allowing members of the Colombian National Police, as internal clients of the organisation, to find all the information on internal procedures on a website with high levels of security.

Concept	Explanation
Request	A Petition is a requirement related to the provision of a service, in the exercise of the duty of cooperation with the Competent Authorities. A Petition may contain one or more individualised requests, called Requests. Types of Requests: • Lawful interception of communications. • Access to metadata. • Blocking and filtering of certain contents. • Geographical or temporary suspension of the service.
URL	These initials stand for Uniform Resource Locator, which is used to name internet resources. This denomination has a standard format and its purpose is to assign a single address to each of the resources available on the Internet, such as pages, images and videos.

Telefónica