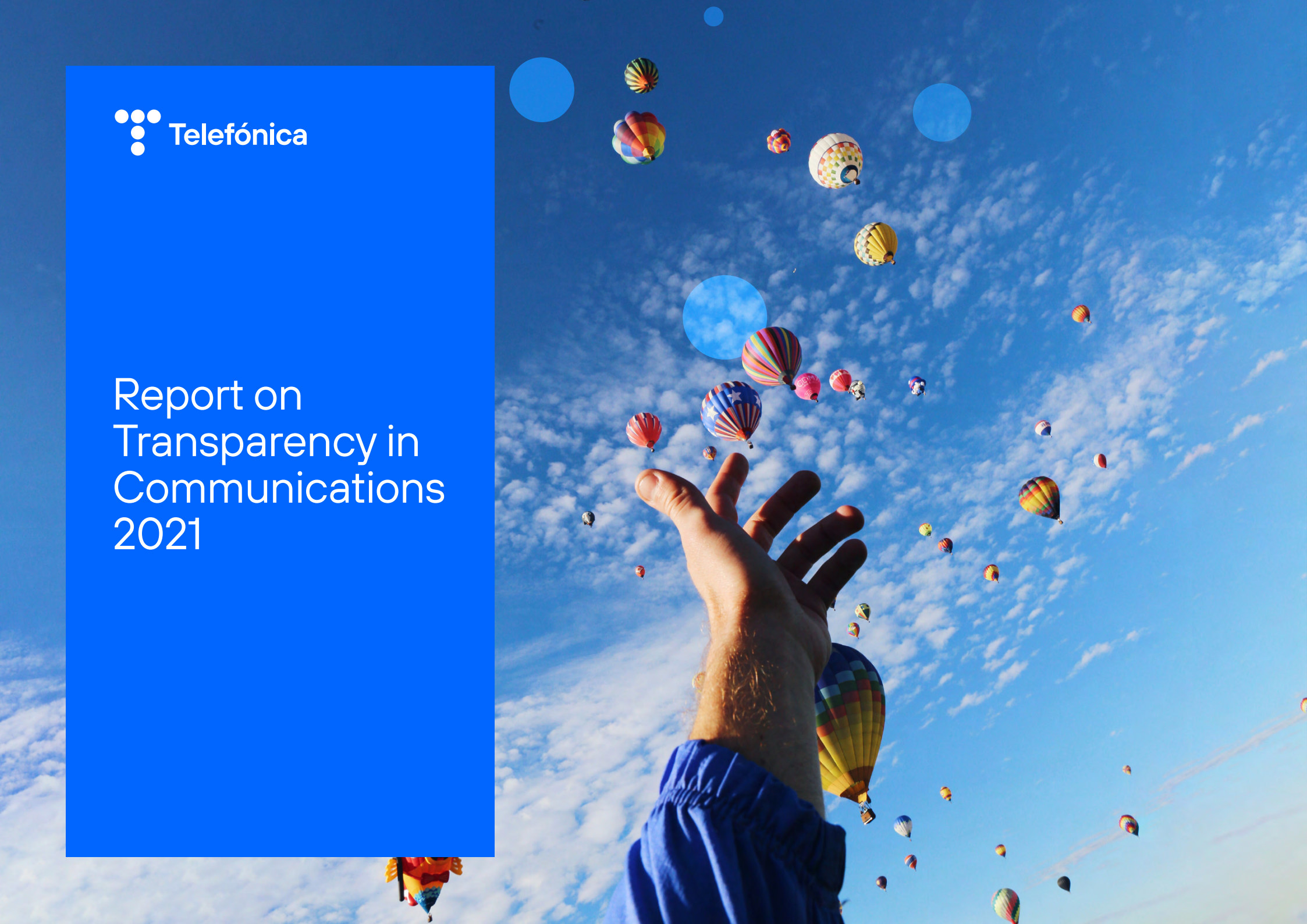
Telefónica

Report on Transparency in Communications 2021



Contents

Introduction and scope of the report

At Telefónica, we are firmly committed to human rights in general and to the right to privacy and freedom of expression in particular. We work to ensure compliance with these rights and promote total transparency in our actions through the publication of the Report on Transparency in Communications (7th edition).

Like other companies in our sector, at Telefónica we receive **requests for information** (view definition in glossary) concerning the communications of our customers and users, requests to block access to certain websites and contents and to filter contents, and requests whose purpose is to temporarily suspend the service in certain areas or certain accounts. Such requests are made by state security forces and bodies, governmental bodies and/or judges (hereafter, the "competent authorities", view definition in glossary).

Transparency is key in this regard, even more so in a world in which there is a shared responsibility to preserve and guarantee people's rights. It is also in this context that we have developed Transparency Centres, both at Group level and in the different countries where we operate, so that our stakeholders can find all the relevant information on privacy, security and freedom of expression in a simple, digital and understandable way.

This report, which corresponds to the period from 1 January 2021 to 31 December 2021, states:

i. our human rights due diligence;

ii. our governance in terms of human rights in general and privacy and freedom of expression in particular;

iii. the commitments, policies and processes we follow when responding to requests from competent authorities;

iv. information on the legal context that provides the competent authorities with the legal basis to make these kinds of requests;

v. the competent authorities that are empowered under the local legislation to request information on the indicators we report on;

vi. the total number of requests we received last year 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;

vii. 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.

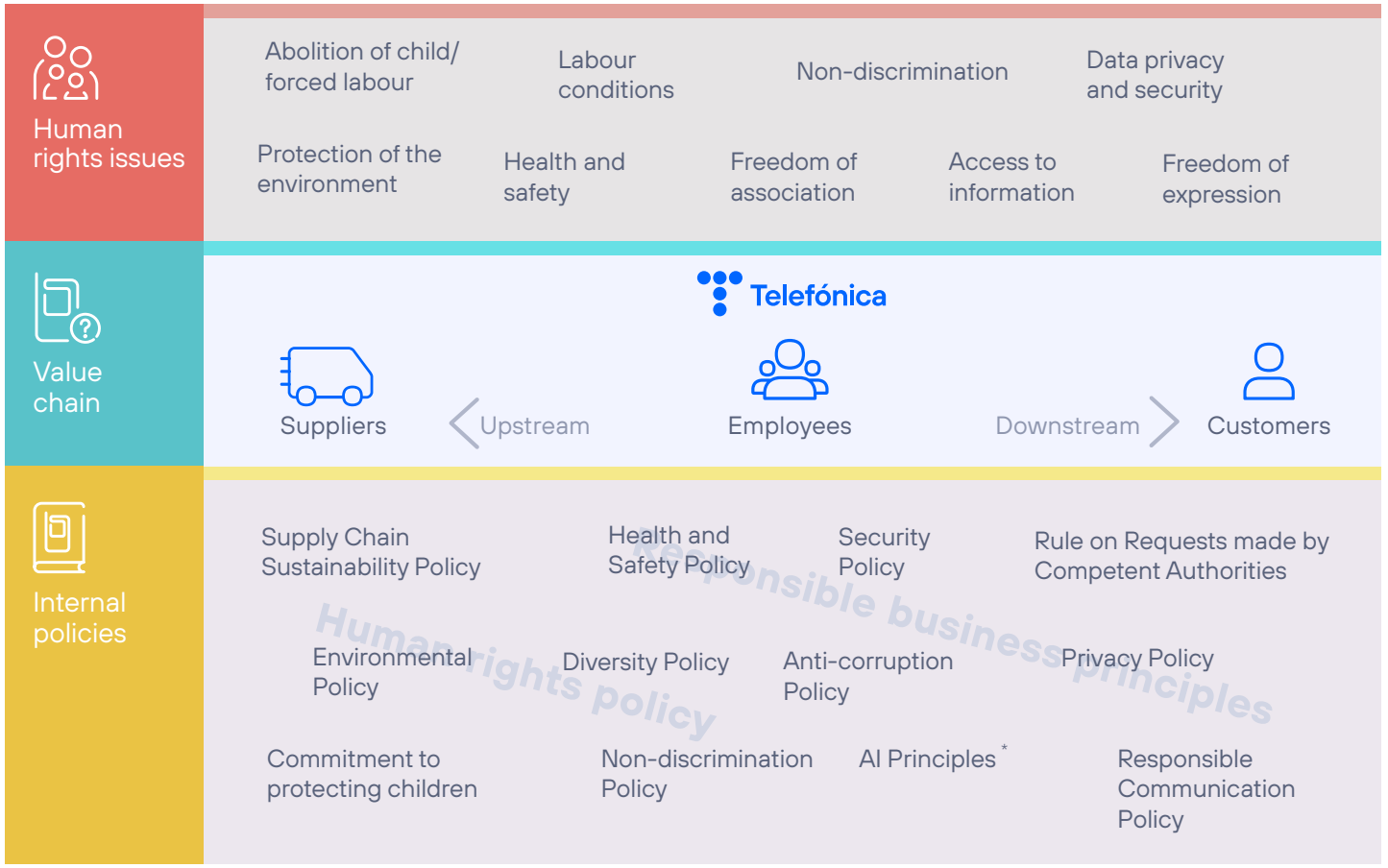
1. The specific legal framework of each country, whenever relevant, also points out limitations in terms of how much information on the requests that Telefónica receives can be provided. When we do not provide data, we explain why we cannot do so.

Our human rights due diligence

Since 2006, human rights have been an integral part of our Business Principles.

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.

Our human rights approach



* AI: Artificial intelligence

In accordance with our Global Human Rights Policy, we have a human rights **due diligence** process in place to identify, prevent, mitigate and remedy (potential and actual) the impacts of our business on human rights. The starting point of our human rights due diligence process are our 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 consultation 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 (see human rights issues analyzed in impact assessments in figure above).

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

- Annual 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 Concern and Whistleblowing Channel, which allows stakeholders to confidentially and anonymously make complaints and queries (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 operation and management of this channel is described in the Regulation about the Management of the Business Principles Channel and in the Policy on Whistleblowing Channel Management which are both publicly available and guarantee the proper management of the channel.

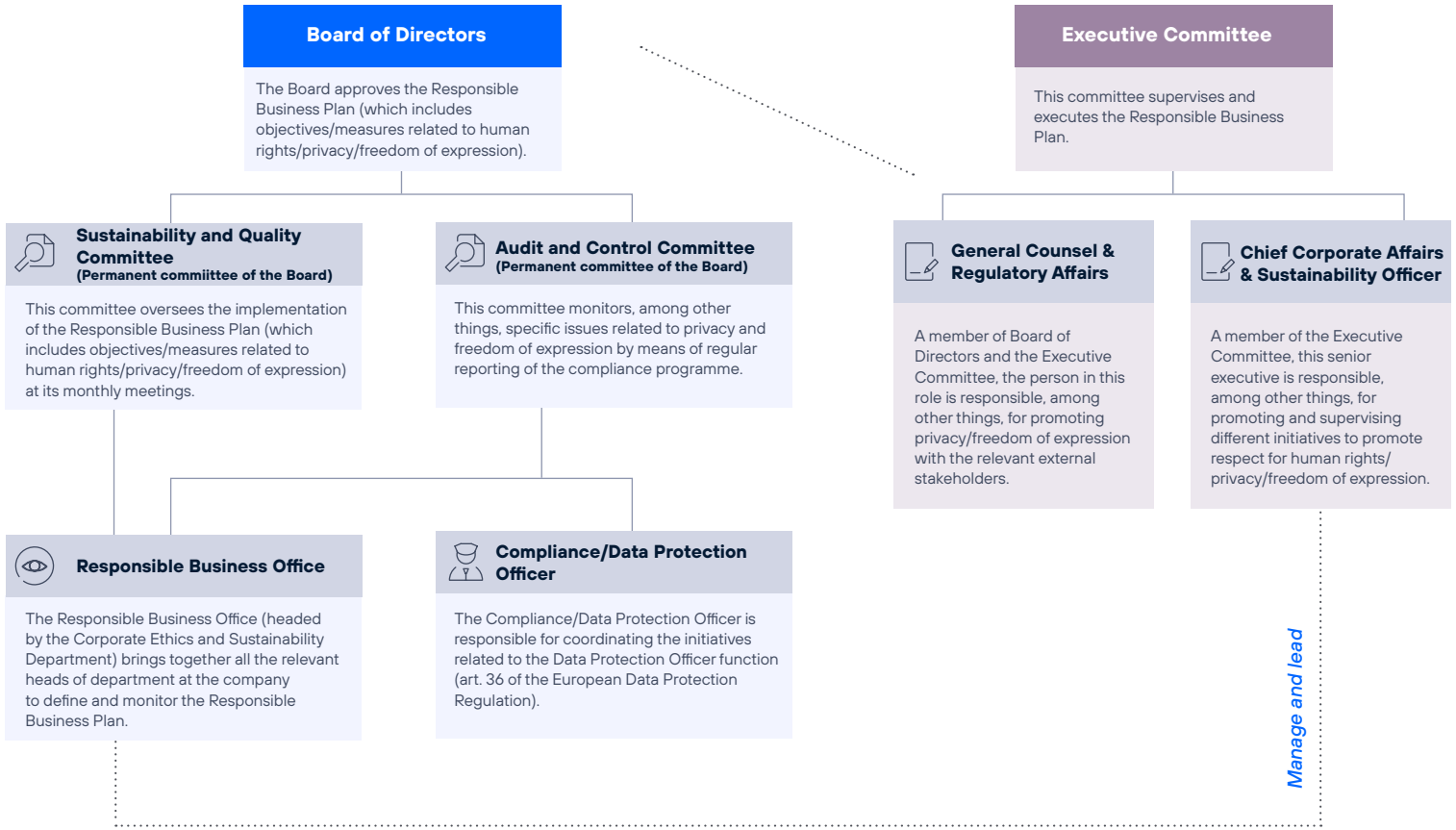
Our governance

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 Quality Committee** (one of the Board's permanent committees). In addition, we have a **Responsible Business Office** whose purpose is to define and monitor the Responsible Business Plan.

This governance model, headed by the Board of Directors, focuses on ensuring that our commitment to human rights is incorporated into all activities and levels of the company.

Human Rights Governance: Privacy and Freedom of Expression



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. As a member of the Responsible Business Office, the DPO regularly reports to the Responsible Business Office on issues related to the DPO function.

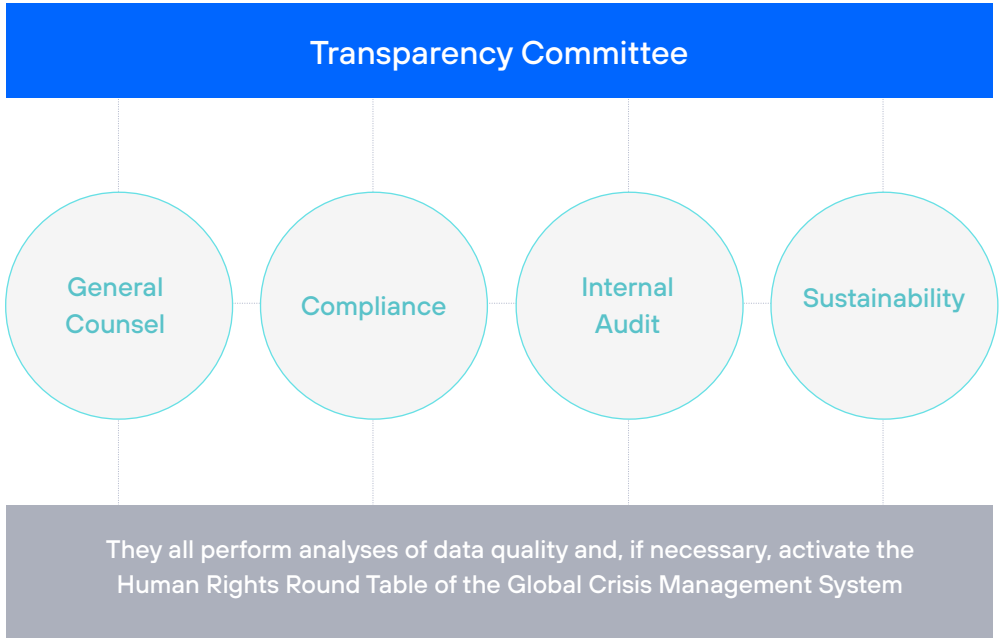
The **General Counsel & Regulatory Affairs** is a member of the Board of Directors and is responsible, among other matters, for promoting privacy and freedom of expression with relevant external stakeholders. In this function, he also led the publication and dissemination of Telefónica´s Digital Pact in 2020, which calls for a new cooperative effort between governments, business and civil society to define a New Digital Deal adapting the current regulatory environment to the digital age, paying special attention to the issues of privacy and freedom of expression.

In addition, in terms of governance and management of this report – which covers requests from competent authorities and their relationship with the rights to privacy and freedom of expression – we have a **Transparency Committee,** which is made up of the heads of the corporate areas of **General Counsel, Compliance, Internal Audit and Sustainability.** The Transparency Committee analyses the reported data in this report and may make such observations as they deem relevant, both in general terms or specifically regarding data reported by the business units. The objective is to ensure the quality of the data at all times as evidence of complying with current legislation and protection of the fundamental rights of individuals.

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:

→ a) certain requests by authorities
→ b) 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 Round Table" (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

We have designed and updated different policies and procedures in order to ensure the rights of privacy and freedom of expression are protected as well as access to information and non-discrimination guaranteed.

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:**
Approved in 2019, 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 processes that seek to ensure respect for and application of internationally recognised social, economic and cultural human rights.

→ **Global Privacy Policy:**
Updated in 2018, 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 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 ultimate responsibility for the personal data protection 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:

→ **DPO Office:** This office is responsible for supervising compliance with the Telefónica Group's data protection regulations.

→ **Steering Committee:** This committee includes representatives from the relevant areas of the company (General Counsel; Regulation and Institutional Affairs; Technology; CDO; Compliance; Ethics and Sustainability; and Internal Audit) and reviews the general status of compliance of the governance model in data protection matters.

→ **Business Committees:** Through the technical data protection function, the DPO Office interacts on a permanent basis with other areas, via the Compliance Officers, in order to ensure maximum uniformity in applying common processes, and/or identifying and handling specific privacy issues in the sphere of activity in each area.

→ **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 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 the participation of 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 2021 and inspired by the principles of honesty and trust, this policy is guided 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, several regulations were updated to ensure effective compliance with it (the Incident and Emergency Management Regulation, Security Risk Analysis Regulation, Network and Communications Security Regulation, Cybersecurity Regulation, Supply Chain Security Regulation and Security Governance Regulation, among others).

→ **Responsible Communications Regulation:**
Approved in October 2018, 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 sponsorships 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 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 rules are applied in all of the markets in which we operate and are extended to our entire value chain through our partners and suppliers.

During 2021 we worked on implementing these principles across all our operations following a threefold approach:

- **Strategic model:** Through these principles, we commit to design, develop and use Artificial Intelligence 1) in a fair and non-discriminatory manner, 2) in a transparent and accountable way, 3) with people as the priority, 4) with privacy and security by design and 5) with suppliers and partners who commit to these or similar ethical standards in Artificial Intelligence.

> **Organisational and relationship model**
We are implementing responsible AI through an organisational and relationship model that defines what areas of the company are involved, what their roles are and how they relate to each other in order to achieve a responsible use of AI.

We promote a self-responsibility approach with on-demand escalation. Product managers/developers who purchase, develop and/or use Artificial Intelligence must carry out a simple self-assessment of the product/service they are developing already in the design phase through an online questionnaire. This self-assessment explicitly covers potential human rights risks associated with the use of Artificial Intelligence. This self-assessment will be integrated into a three-tiered governance model, supported by a broader Community of Experts (among them a single-point-of-contact representative for questions relating to AI & Ethics, the Responsible AI Champion). If a product manager/developer (level 1) has doubts about a potential adverse impact of a given product/service after completing the self-assessment, and this doubt cannot be resolved with the help of the RAI, they will be automatically directed to a multidisciplinary group of experts within the company (level 2) who will work with the product manager/developer to try to solve the issue at hand. In the event this issue turns out be a potential risk to the company´s reputation, the matter is escalated to the Responsible Business Office

which brings together all relevant department directors at global level (level 3).

→ **Operating model**

The operating model describes the processes to implement the Responsible AI approach in the organisation on a day-to-day basis. Integrated within the broader Responsibility by Design approach, it includes a methodology called "Responsible AI by Design", inspired by methodologies in place such as Privacy and Security by Design. The operating model consists , among other things, of:

> **Training and awareness activities:** Telefónica has developed courses related to AI and ethics that are accessible to all employees through the standard corporate portals.

> The self-assessment questionnaire, where each AI principle is operationalised through a series of questions along with a series of recommendations. The questionnaire is integrated in the global "Responsible Design" initiative of the Telefónica Group.

> A set of technical tools that help to answer the questions of the self-assessment questionnaire.

→ **Internal Control:**

Telefónica has a robust control model that is adapted when necessary to comply with the requirements of applicable legislation.

Initiatives and processes

→ **Human rights training:**

In late 2019 we began working on specific human rights training. As in previous years, in 2021 we provided general training for all employees through the Responsible Business Principles and Human Rights Course and more specific training for professionals (Legal, Compliance and Data Protection Officers, M&A team, Public Affairs, Institutional Relations and Operations) whose work has a greater impact on human rights.

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

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

The objective is to identify any risks of direct or indirect impact due to 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, that is, 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 further analysis with the help of human rights experts in the company so as to address possible adverse human rights impacts in the further development of the product/service in the future.

→ **Transparency initiatives:**

One of the challenges and key elements of privacy is guaranteeing transparency. At Telefónica we seek to put this 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. A case in point is our Global Privacy Centre and the Privacy or Transparency Centres of our OBs. 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. This data is collected in the so-called 'Personal Data Space' of the 4th platform. It is accessible through different channels such as the Transparency Centre in the My Movistar app.

In 2021, we finished the process of totally renovating Movistar's Transparency Centre which is available on the Movistar website in Spain: https://www.movistar.es/Microsites/centro-transparencia/

This centre offers customers access to their privacy preferences and management of the data collected in the Personal Data area.

In the Transparency Centre, through the Privacy Permissions section, customers can manage the legitimate bases relating to the use of their data for certain purposes. And in the Access and Download section we offer useful visualisations of different types of data, with a user-friendly experience and respecting privacy criteria, with the option to download a more detailed document.

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

The Transparency Centre takes us a step further in delivering on our promise to empower our customers with control and transparency over their data, always in accordance with applicable privacy regulations. For example, in Europe this processing is fully aligned with the European Data Protection Regulation.

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

In accordance with our Policy for the Elaboration and Organisation of the Regulatory Framework, the Internal Audit 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 its wording and implementation.

The 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 them and carry out its monitoring, evaluation and updating and who are empowered to carry out sample supervisions of the controls whenever they deem it appropriate to do so.

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 GNI (Global Network Initiative)

We ranked first among all telecommunications companies in the Digital Rights Ranking, which was published in February 2021. It evaluates companies' commitments, policies and practices affecting freedom of expression and customer privacy, including governance and oversight mechanisms.

As member of the Global Network Initiative (GNI) in 2021, we participated in different initiatives related to the impact of COVID-19 on privacy and freedom of expression. We also successfully passed the GNI's independent evaluation process. The GNI´s positive assessment was based on a report from an independent external advisor (Deloitte) that examined Telefónica's policies, processes and governance model to safeguard the freedom of expression and privacy of its customers.

Indicators of 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,** but only deal with requests from authorities that are empowered to do so by the law. However, as a sole exception, in order to proactively fight against contents and images of sexual abuse of minors on the internet, at Telefónica we proceed 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 location 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 pornography, 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 made by competent authorities to temporarily or geographically limit the provision of a service. These requests are usually connected with circumstances involving situations of force majeure, such as natural catastrophes, acts of terrorism, etc.

Individual access restrictions are also taken into account.

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

Requests rejected or partially dealt with

Number of times that we have rejected a request or that we have 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 be notable variations in data for each of the indicators with respect to previous years, which are usually due to technical, methodological or legislative reasons.

There may also be variations from 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 exceptional situation in which Venezuela finds itself and the challenges we face in verifying our global processes in the country. In this situation, Telefónica must prioritise compliance with current legislation, the maintenance of connectivity in the country and the well-being of our employees.

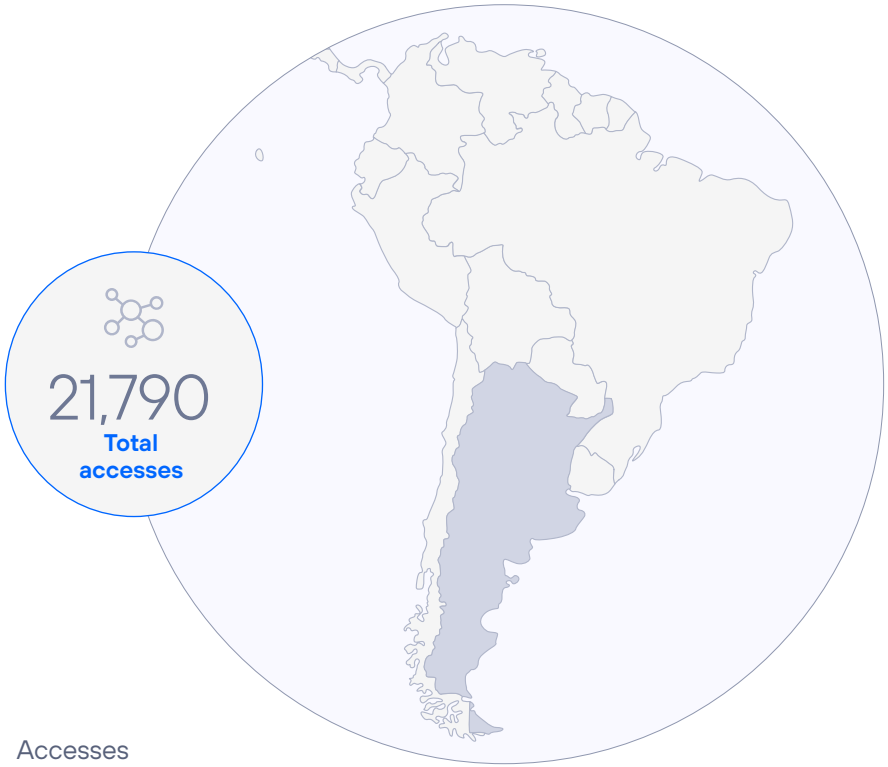
Finally, following the events that have taken place since the conflict between Russia and Ukraine began in February 2022, numerous international measures have been taken, some of them with a possible impact on human rights in general and privacy and freedom of expression in particular. Although this event does not fall within the reporting period covered by this report (January 2021 - December 2021) and we do not have a presence as an operator in these regions, we have the commitment and responsibility to consider possible impacts that our activity could have on human rights in general, and privacy and freedom of expression in particular. This leads us to consider this crisis and its international consequences in the various committees within Telefónica to ensure respect for human rights, privacy and freedom of expression in the event that Group intervention is necessary, which would then be reported in next year's report.

Report by country

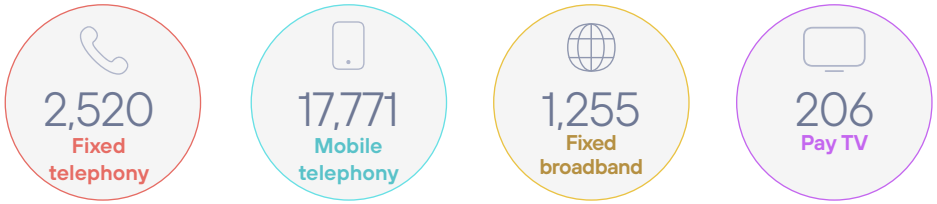
- Argentina
- Brazil
- Chile
- Colombia
- Ecuador
- Germany
- Mexico
- Peru
- Spain
- United Kingdom
- Uruguay
- Venezuela

Argentina

www.telefonica.com.ar



Accesses



Accesses at closing 2021 (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 communications.

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 21.7 million accesses at the end of December 2021.

With regard to the financial figures, Telefónica's revenue in Argentina stood at 2,056 million euros and the OIBDA was 229 million euros.

Data as of the end of 2021

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 an access; prosecutors 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

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

*In 2019, we began to register data for Access to Metadata, Content Blocking and Service Suspension separately and not in aggregated format as in previous years. Therefore year-on-year comparisons should be made from 2019 onwards.

Blocking and filtering of certain contents

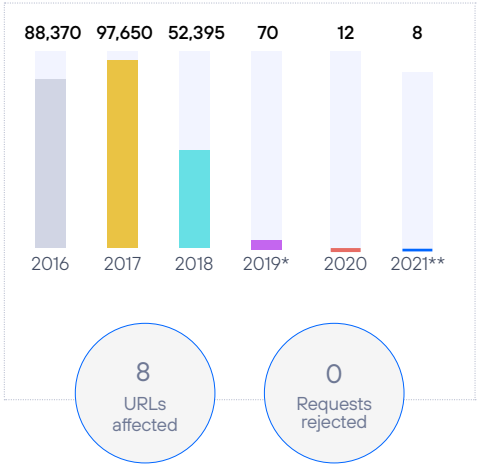
Legal framework

→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



* In 2019, we began to register data for Access to Metadata, Content Blocking and Service Suspension separately and not in aggregated format as in previous years. Therefore year-on-year comparisons should be made from 2019 onwards.

**In 2021 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

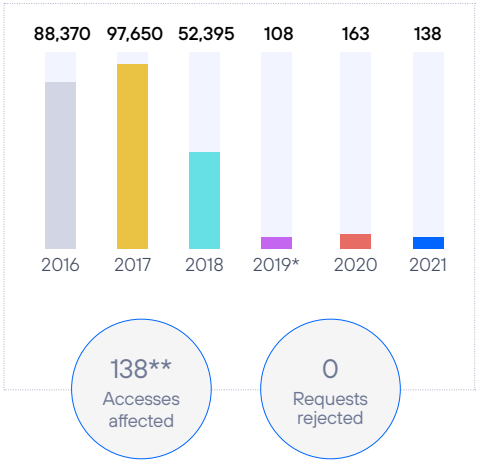
Although there is no specific rule governing this, it may be interpreted as part of what is established in Art. 57 of Law 27,078, which stipulates:

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, according to Art. 57.

Requests



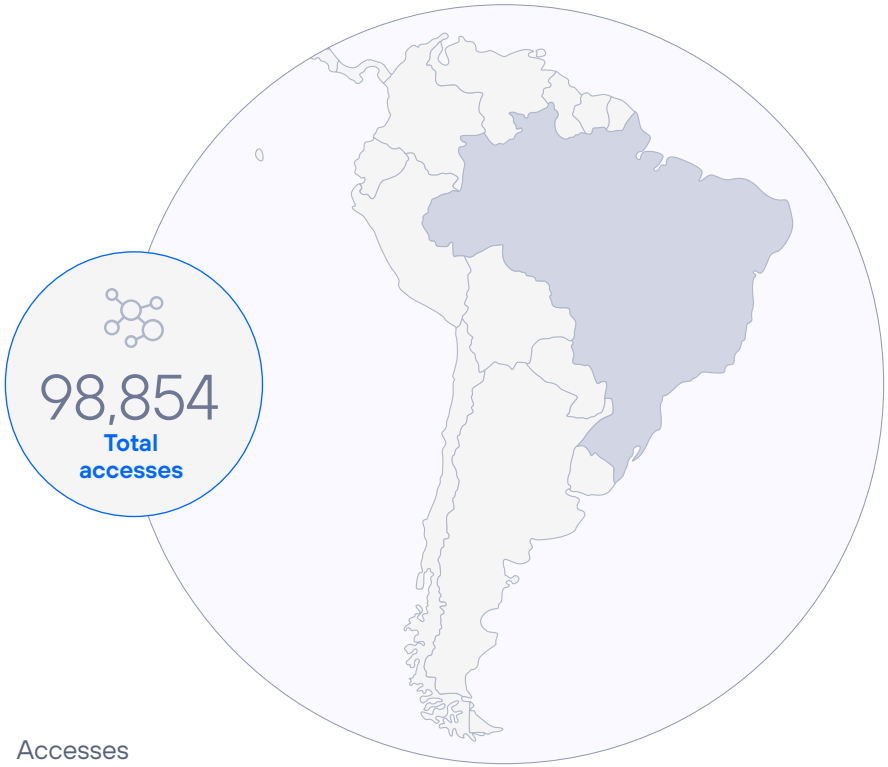
* In 2019, we began to register data for Access to Metadata, Content Blocking and Service Suspension separately and not in aggregated format as in previous years. Therefore year-on-year comparisons should be made from 2019 onwards.

They correspond to requests to temporarily restrict the mobile data traffic of certain customers.

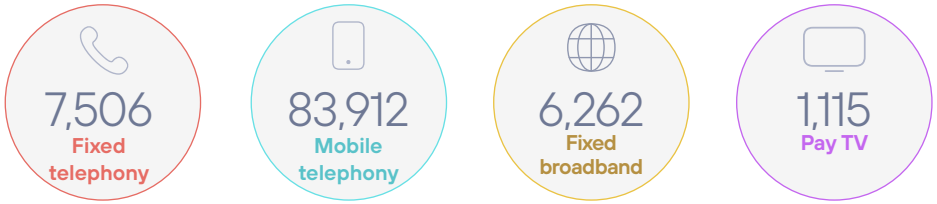
** Individual data blocking.

Brazil

www.telefonica.com.br



Accesses



Accesses at closing 2021 (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 managed more than 98.8 million accesses in Brazil at December 2021.

With regard to the financial figures, in 2020, Telefónica's revenue in Brazil reached 6,910 million euros and OIBDA stood at 3,138 million euros.

Data as of the end of 2021

Lawful interceptions

Legal framework

→ Constitution of the Federal Republic of Brazil, Article 5.

→ Law N° 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 № 9296/1996 (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

*The registration system during the reporting period did not have the mechanisms to filter according to rejected requests. Work is underway to make this data available in future reports.

Access to Metadata

Legal framework

→ Law N° 9.296, 24/07/1996.

→ Law N° 9.472, Article 3, 16/07/1997.

→ Law N° 12.683, Article 17 B, 09/07/2012.

→ Law N° 12.830, Article 2, 20/07/2013.

→ Law N° 12850, Article 15, 20/08/2013.

→ Law N° 12965, Articles 7, 10 and 19, 23/04/2014.

→ Decree N° 8.771, Article 1, 11/05/2016.

→ Law N° 13344, Article 11, 10/2016.

→ Law N° 13812, Article 10, 05/2019.

→ Resolution N° 73 of 25 November 1998 / Regulation of Telecommunications Service - Article 65 - K .

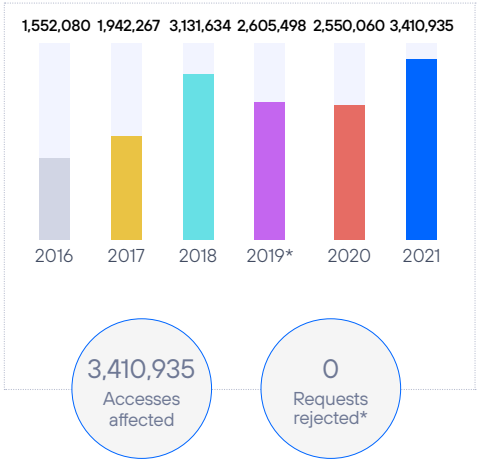
→ Resolution № 632 of 7 March, 2014 / General Regulation of Consumer Rights of Telecommunications Services - RGC - Article 3, V.

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



*The registration system during the reporting period did not have the mechanisms to filter according to rejected requests. Work is underway to make this data available in future reports.

Blocking and filtering of certain contents

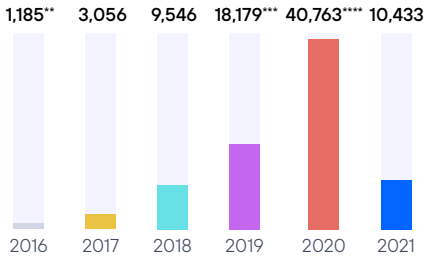
Legal framework

Law Nº 12965, Articles 7 and 19, 23/04/2014.

Competent authorities

Exclusively Judges.

Requests



10,433 Accesses affected

0 Requests rejected*

* The registration system during the reporting period did not have the mechanisms to filter according to rejected requests. Work is underway to make this data available in future reports.

** Clarification: After the general blocking measures that affected all potential customers, public authorities started to carry out individual blocking in the field of criminal investigations.

***In 2019, only URL blocking was counted, while reporting WhatsApp service suspensions of individual accounts in the "Suspension of Service" indicator.

****The increase compared to 2019 was due to a campaign by the Brazilian Ministry of Justice to combat piracy (Operation 404).

Geographical or temporary suspension of the service

Legal framework

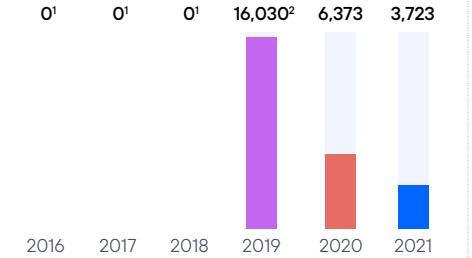
→ Resolution Nº. 73 of 25 November 1998. Article 31.

→ Resolution Nº. 477 of 7 August 2007. Article 19.

Competent authorities

Exclusively Judges.

Requests



3,723 Accesses affected

0 Requests rejected*

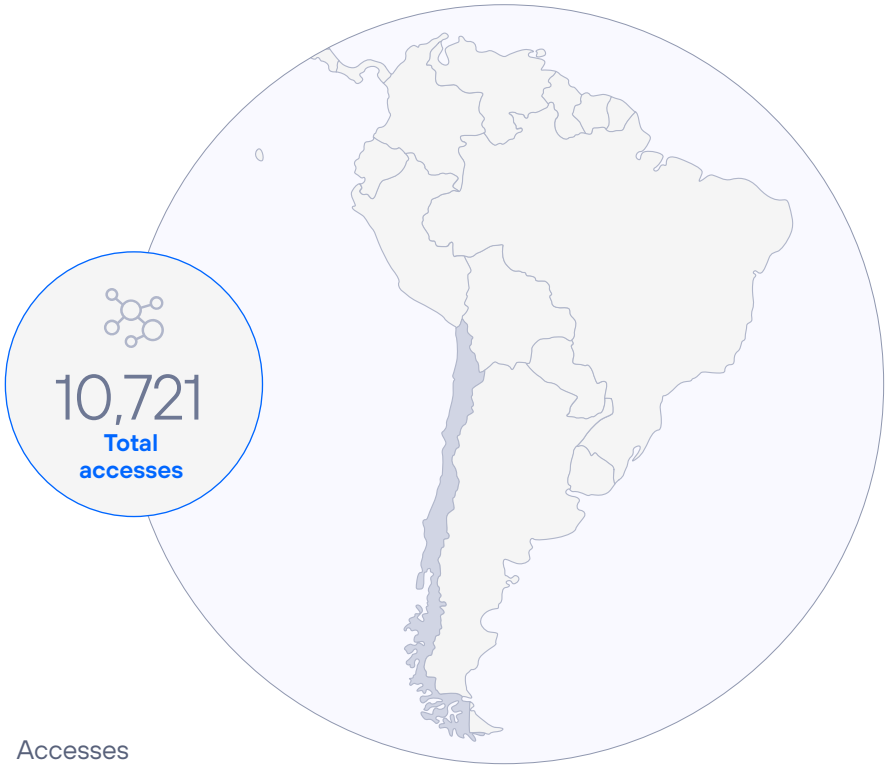
*The registration system during the reporting period did not have the mechanisms to filter according to rejected requests. Work is underway to make this data available in future reports.

1 There were no data available, as they were recorded together with the cases known as atypical and low-volume requests.

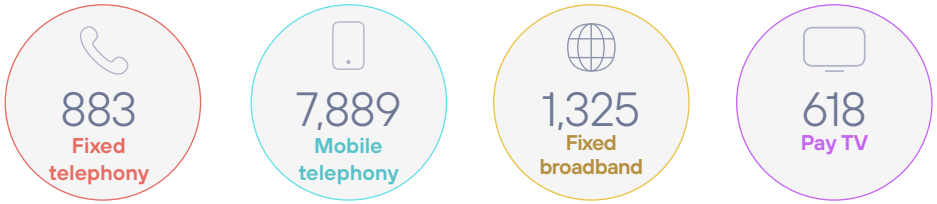
2 This data is not comparable to other years since 2019 service suspensions of individual accounts are now being counted in this indicator (previously reported as content blocking).

Chile

www.telefonicachile.cl



Accesses



Accesses at closing 2021 (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 2021, Telefónica Chile had more than 10.7 million accesses. With regard to the financial figures, Telefónica's revenue in Chile stood at 1,769 million euros and OIBDA was 920 million euros.

Data as of the end of 2021

Lawful interceptions

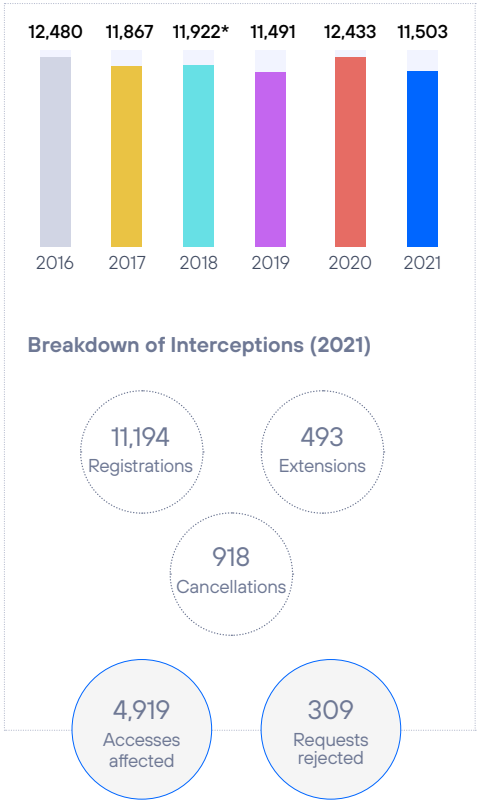
Legal framework

- N°5 of Article 19 of the Political Constitution. Inviolability of Communications.
- Code of Criminal Procedure, 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 conducts. N°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.
- Code of Criminal Procedure, 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



*These cancellations are not considered within the total of requests since these are cancellations that occur automatically as the deadline for interception is found in the initial request itself.

Access to Metadata

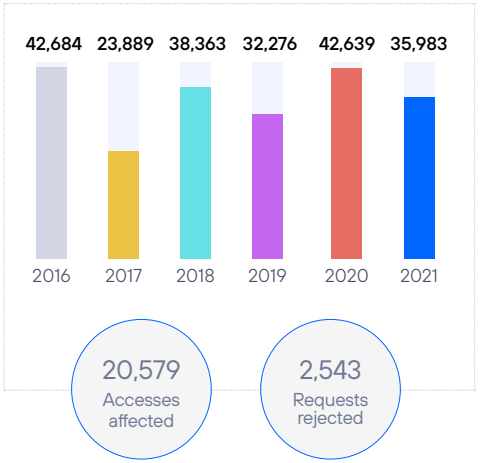
Legal framework

- N° 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: the 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.
- Criminal Procedure Code: Paragraph 5 of Article 222 of the Criminal Procedure Code, 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 120bis 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



Blocking and filtering of certain contents

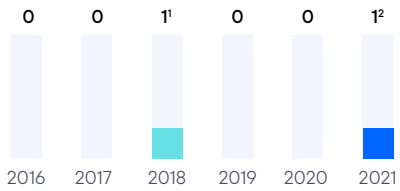
Legal framework

- 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 organically dependent on 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



1. For violation of copyright (Law 17,336 of Intellectual Property).
2. Blocking 1 URL and 2 IP addresses, on intellectual property grounds.

Geographical or temporary suspension of the service

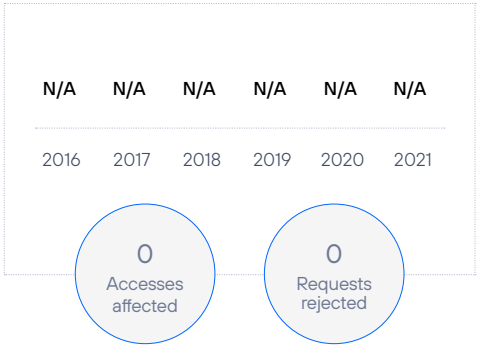
Legal framework

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

Competent authorities

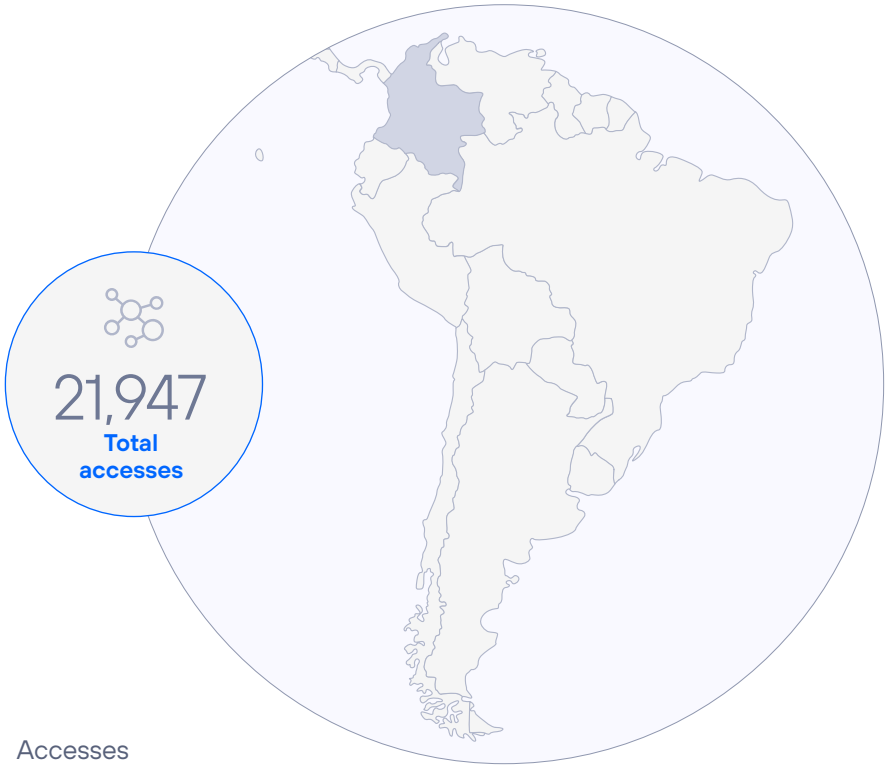
Not applicable.

Requests

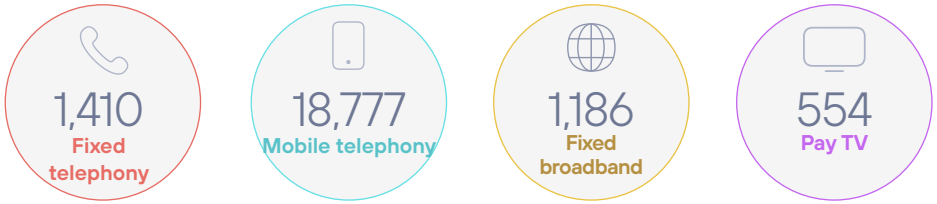


Colombia

www.telefonica.co



Accesses



Accesses at closing 2021 (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.

Telefónica Colombia managed 21.9 million accesses at December 2021.

Telefónica's revenue in Colombia reached 1,312 million euros and OIBDA stood at 413 million euros .

Data as of the end of 2021

Lawful interceptions

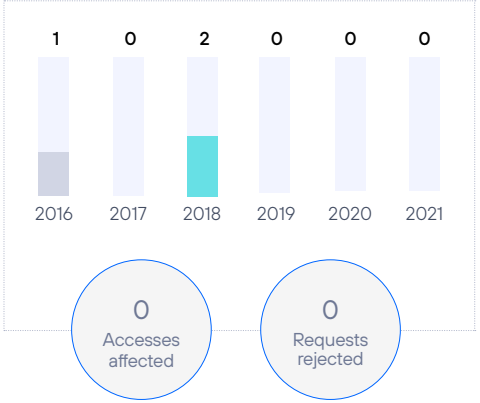
Legal framework

- 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*



*Requests concerning landlines (fixed lines)

Mobile lines: Interceptions of mobile lines are not reported. 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 of the Criminal Procedure Code)

Judicial police duties are performed, on a permanent basis, by the persons vested with the responsibility for this function who belong to the Technical Investigation Corps (CTI) of the Attorney General's Office, the National Police and the Administrative Department of Security, through its specialised agencies.

In locations of the national territory where there are no members of the judicial police of the National Police, these duties 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)

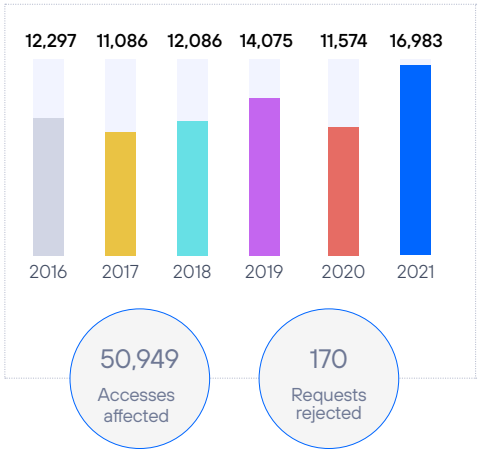
Judicial police functions are performed on a temporary basis by the public bodies authorised to do so by decision of the Attorney General's Office. These public bodies must act in accordance with the authorisation granted to them and in the matters which have been specified in the aforementioned decision.

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.

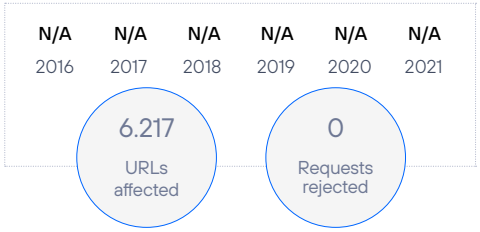
The Attorney General's Office, defendant or defendant's counsel will have recourse, when necessary, to Colombian or foreign private laboratories or laboratories of public or private universities, whether Colombian or foreign.

Requests



Blocking and filtering of certain contents

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; for example, 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.

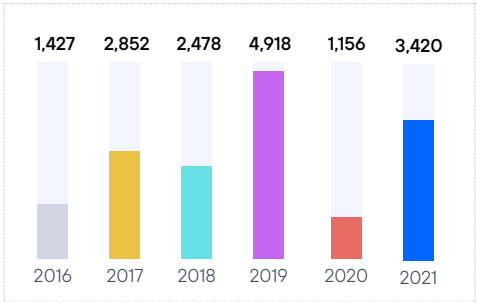
Competent authorities

- 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.

N° 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).

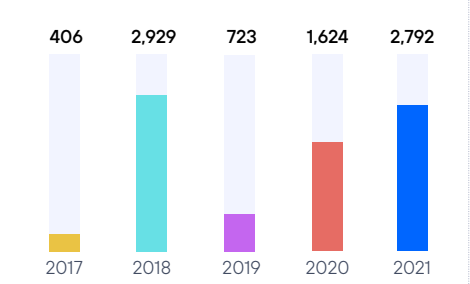
→ Law 1450 of 2011, Article 56.

→ 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.

N° 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

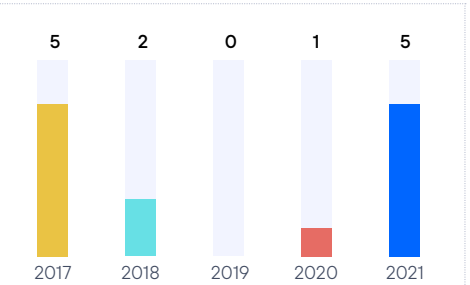
→ Constitutional Court Ruling C-600 of 2019

→ 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.

N° 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.

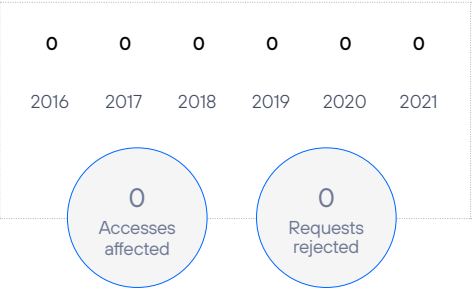
→ Decree 2434 of 2015, CRC (Communications Regulatory Commission) Ruling 4972 of 2016 - this makes it obligatory to prioritise calls between authorities to deal with emergencies.

This prioritisation means terminating calls by users who are not on the list of numbers.

Competent authorities

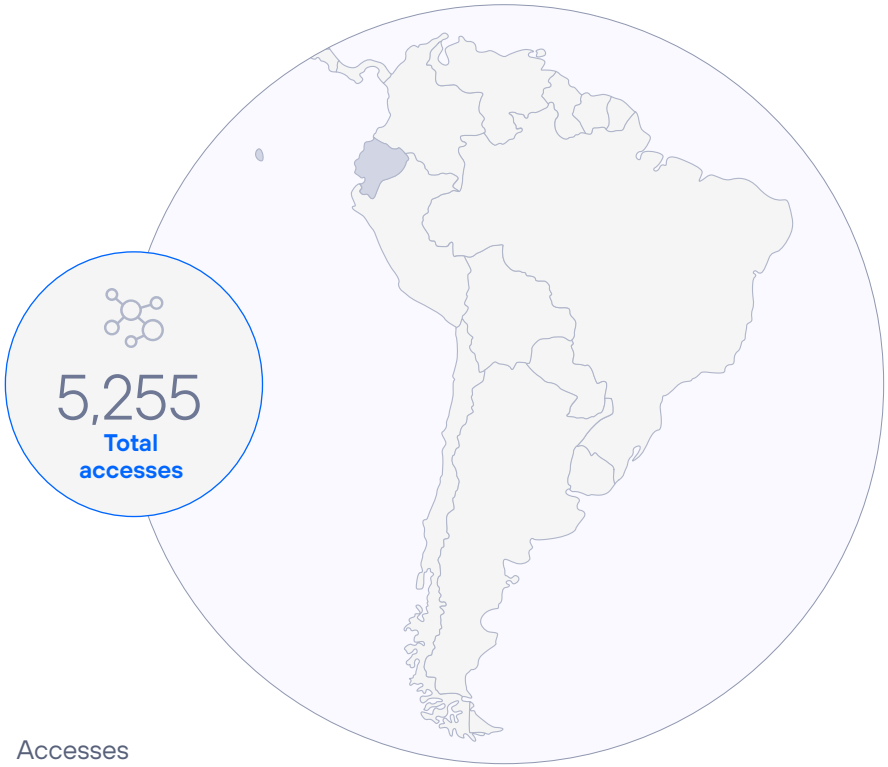
Priority will be given to the authorities in the transmission of free and timely communications in order to prevent disasters, when such communications are considered essential.

Requests

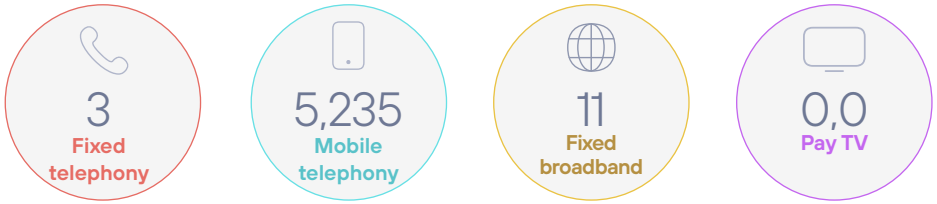


Ecuador

www.telefonica.com.ec



Accesses



Accesses at closing 2021 (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 5.2 million accesses in Telefonica Ecuador at December 2021.

Telefónica's revenue in Ecuador stood at 398 million euros and the OIBDA was 122 million euros.

Data as of the end of 2021

Lawful interceptions

Legal framework

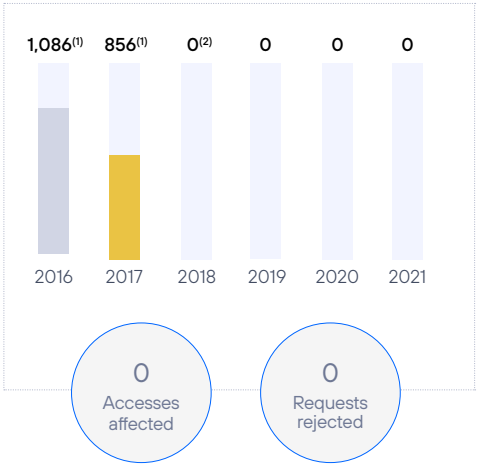
→Organic Integral Penal Code, Articles 476 and 477.

→Concession Contract signed between OTECEL S.A. and the Ecuadorian State.

Competent authorities

Competent prosecutor within an investigation.

Requests



(1) Due to a change in regulation, the prosecution now responds directly to requests for intervention and data in criminal matters.

(2) Since 2018, the Attorney General's Office has been the only entity authorised to perform this type of interception in real time; the operator does not intervene in the process.

Access to metadata

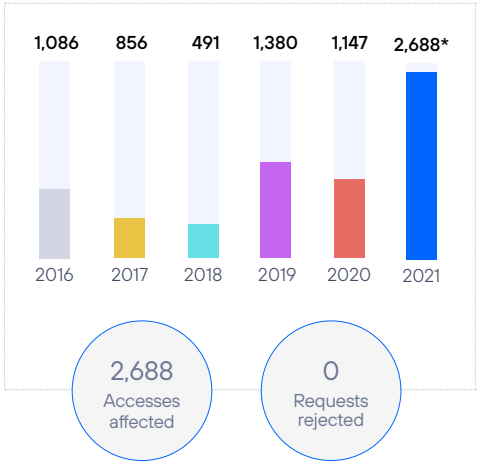
Legal framework

→Organic Integral Penal Code, Article 499.

Competent authorities

→Judges of Criminal Guarantees.

Requests



* Most of the 2021 petitions are 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

*For violating intellectual property.

Geographical or temporary suspension of the service

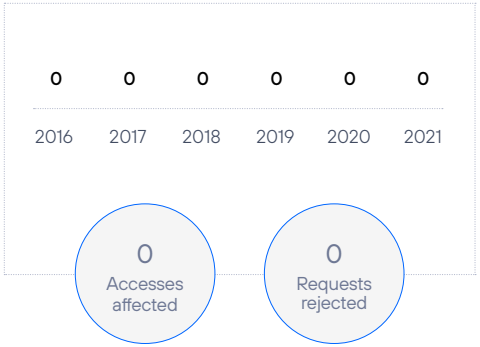
Legal framework

Constitution of Ecuador, Articles 164 and 165.

Competent authorities

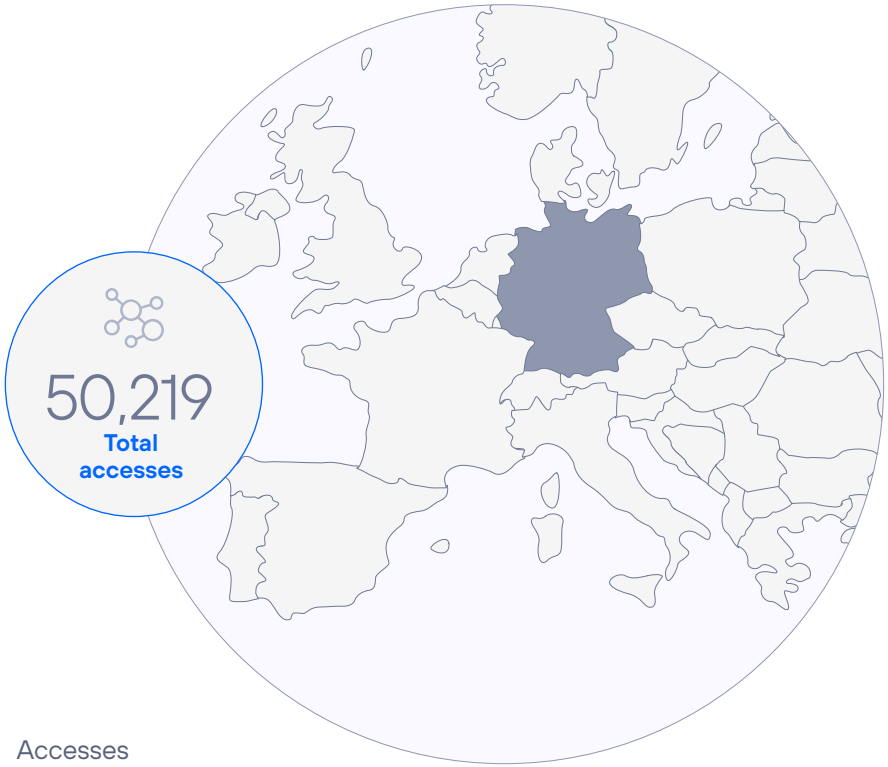
Those that the President of the Republic delegates on behalf of the President, in accordance with the circumstances reflected by the Law.

Requests

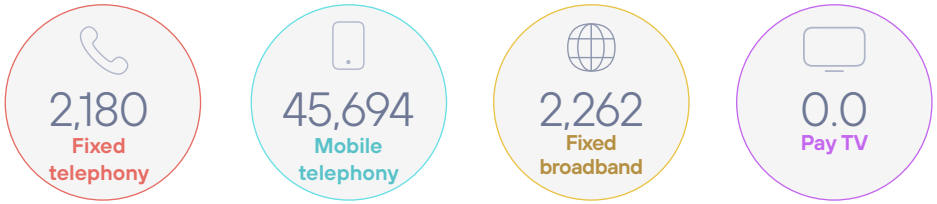


Germany

www.telefonica.de



Accesses



Accesses at closing 2021 (data in thousands).

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

Telefonica Deutschland offers its private and business customers post-paid and prepaid mobile telecom products as well as innovative mobile data services based on the GPRS, UMTS and LTE technologies. In addition, the integrated communications provider also offers ADSL fixed network telephony and high-speed Internet. Telefónica manages 50.2 million accesses in Germany.

Telefónica's revenue in Germany reached 7,765 million euros and OIBDA was 2,424 million euros.

Data as of the end of 2021

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), for example, 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 not to become ineffective.

Requests*

* Total volume includes new requests, extensions and cancellation of interceptions.

** In 2020, the increase compared to 2019, is due to a change in the registration process. That is, registrations have been made by number of requests and not by number of petitions, which allows to give more granular information (a petition may contain several requests, see glossary).

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

Access to metadata

Legal framework

→Section 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).

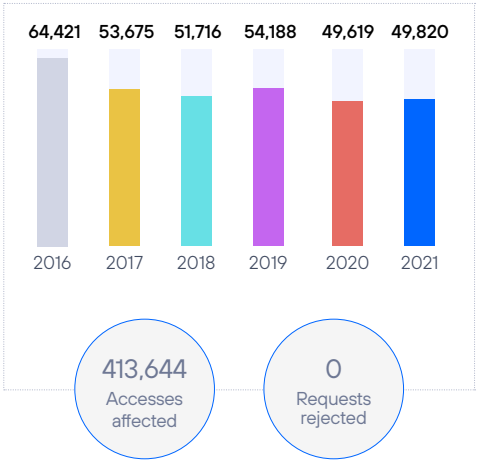
→Police Acts of the federal states (Landespolizeigesetze).

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 not to become ineffective.

Requests*



* Number of petitions

Blocking and filtering of certain contents

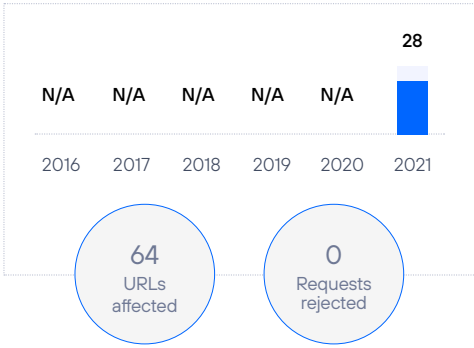
Legal framework

CUII "Clearingstelle Urheberrecht im Internet", sector agreement of Internet Service Providers (ISPs) and copyright industries (11/03/2021).

Competent authorities

Not applicable.

Requests



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

Type: 27 intellectual property and 1 financial supervision.

Geographical or temporary suspension of the service

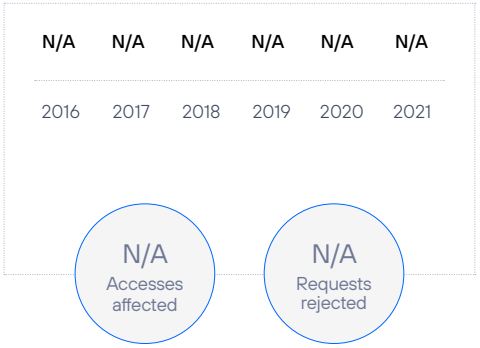
Legal framework

CUII "Clearingstelle Urheberrecht im Internet", sector agreement of Internet Service Providers (ISPs) and copyright industries (11/03/2021).

Competent authorities

Not applicable.

Requests



Mexico

www.telefonica.com.mx

Accesses

Accesses at closing 2021 (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 93,000 locations, 90,000 km and over 25.2 million customers.

The commercial offers are available in 315 Customer Service Centers (CAC), and more than 4,200 indirect points of sale throughout the country.

Telefónica in Mexico managed more than 24.1 million accesses in December 2021.

With regard to the financial figures, Telefónica's revenue in Mexico stood at 1,010 million euros and the OIBDA was 82 million euros.

Data as of the end of 2021

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*

*For technical reasons, requests are counted as petitions.

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 which are made to the concession holders and receiving the corresponding information, by means of agreements published in the Official Gazette of the Federation.

Requests

Blocking and filtering of certain contents

Legal framework

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

Competent authorities

Not applicable.

Requests

2016	2017	2018	2019	2020	2021
N/A	N/A	N/A	N/A	N/A	N/A

N/A
URLs affected

N/A
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

2016	2017	2018	2019	2020	2021
N/A	N/A	N/A	N/A	N/A	N/A

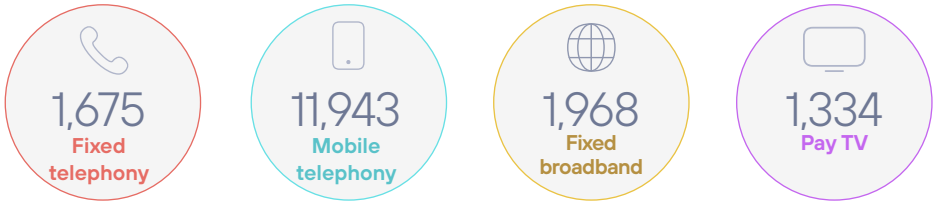
N/A
Accesses affected

N/A
Requests rejected

Peru

www.telefonica.com.pe

Accesses



Accesses at closing 2021 (data in thousands).

Telefónica began to operate in the Peruvian market in the middle of the 1990s. The company managed more than 16.9 million accesses at the end of December 2021.

Regarding financial figures, Telefónica's revenue in Peru stood at 1,533 million euros and the OIBDA was 252 millon euros.

Data as of the end of 2021

Lawful interceptions

Legal framework

→Political Constitution of Peru, Article 2, paragraph 10.

→Telecommunications Law (Supreme Decree N° 013-93-TCC - Article 4°) and its Regulations (Supreme Decree N° 020-2007-MTC - Article 13°).

→Law N° 27697: Law that grants power to the prosecutor for the intervention and control of communications and private documents in exceptional cases.

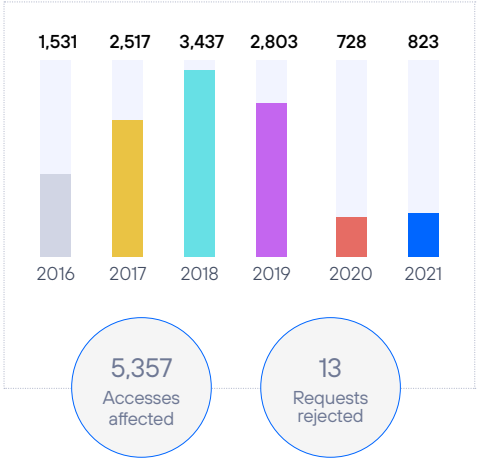
In all the concession contracts there is a clause related to the secrecy of telecommunications and the protection of personal data which establishes that the company will safeguard them and maintain the confidentiality of the personal information related to their customers, unless there is a specific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



*Includes registrations, extensions and cancellation of interceptions. For technical reasons, requests are counted as petitions.

Access to metadata

Legal framework

→Political Constitution of Peru, Article 2, paragraph 10.

→Telecommunications Law (Supreme Decree N° 013-93-TCC - Article 4°) and its Regulations (Supreme Decree N° 020-2007-MTC - Article 13°).

→Law N° 27697: Law that grants power to the prosecutor for the intervention and control of communications and private documents in exceptional cases.

→Law N° 31284: IMEI Geolocation information

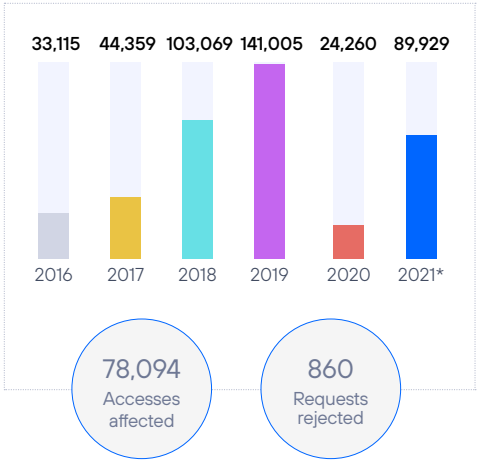
→Legislative Decree N° 1182 which regulates the use of telecommunications for the identification, location and geolocation of communication equipment in the fight against delinquency and organised crime.

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



*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; being 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 would acts would be performed that violate the right of public communication of the complainant companies, the administration can order the blocking, in Peruvian territory, of access to the offending website, through blocking based on DNS and blocking based on URL.

Requests*

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

Geographical or temporary suspension of the service

Legal framework

Telecommunications Law Regulations (D.S. N° 020-2007-MTC - Articles 18 and 19).

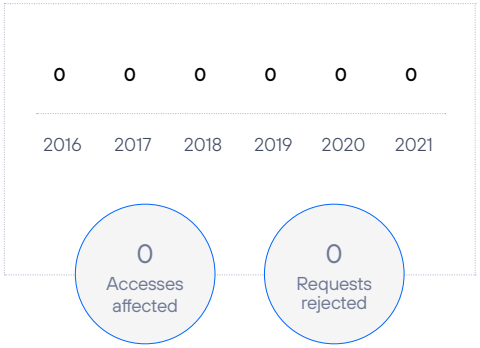
The concession contracts establish that, in the event of an emergency, crisis or a threat to national security, the concession holder will provide telecommunication services, prioritising actions to support the State and following the instructions of the MTC.

Competent authorities

→ Ministry of Transport and Communications (MTC).

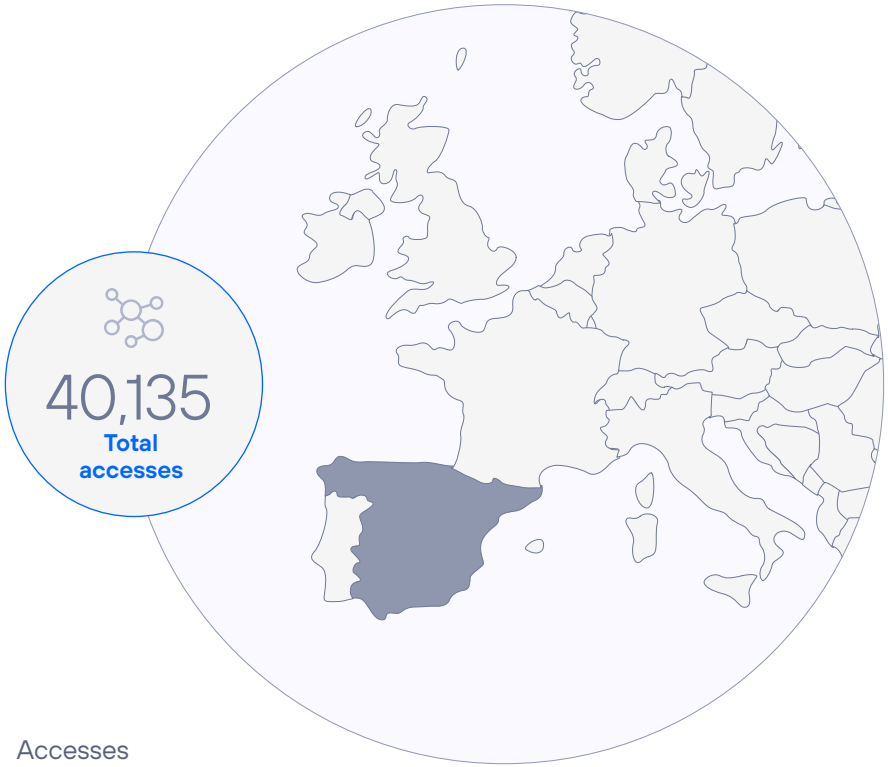
→ National and Civil Defence System.

Requests

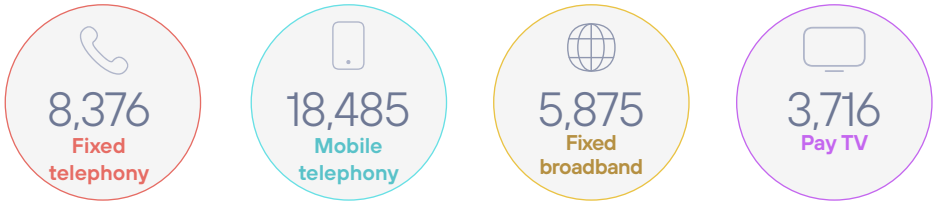


Spain

www.telefonica.es



Accesses



Accesses at closing 2021 (data in thousands).

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

Telefónica España 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 España handled more than 40.1 million accesses at the end of December 2021.

Revenue from operations amounted to €12,417 million euros and OIBDA reached 3,377 million euros in 2021.

Data as of the end of 2021

Lawful interceptions

Legal framework

→Spanish Constitution, Article 18.

→Criminal Procedure Code, Article 588.

→Law 9/2014 (General Telecommunications Law), Articles 39 and 42. This law was been amended in accordance with the provisions of Royal Decree Law 14/2019 of 31 October, adopting urgent measures for public security reasons in the field of e-government, public sector procurement and telecommunications. Thus, there is a new wording of Articles 4(6) and 81(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 with character prior to 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."

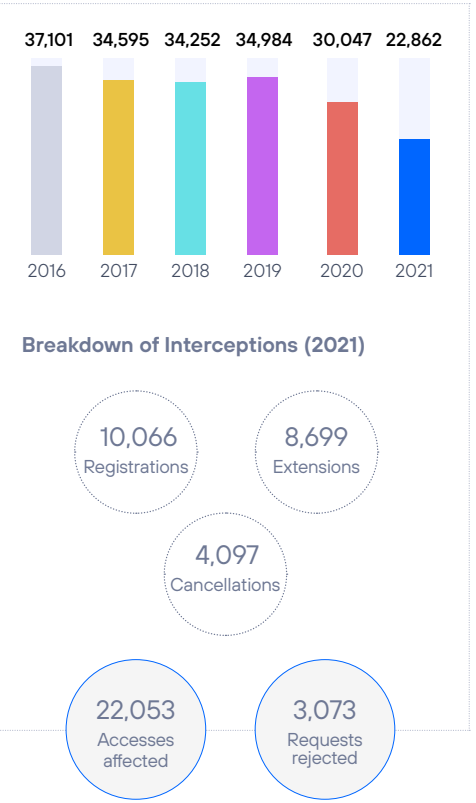
Competent authorities

→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 assume responsibility for 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



Access to metadata

Legal framework

→ Law 25/2007, Law on Data Conservation, Articles 1-10.

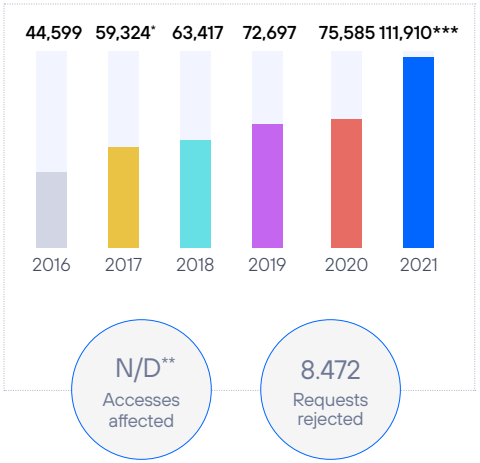
→ Law 9/14, General Communications Law, Articles 39-42.

Competent authorities

→ Courts.

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

Requests



* In 2017, a new system of sending judicial orders from the State Security Forces and Corps was implemented, in which each request for data gives rise to an individual request.
With the previous system, which is still in place for most of these agencies, a single warrant could result in multiple data requests, even if it was counted as one.

** 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 requests from the competent authorities [see note 1] was extended and the use of the digital system was generalised in 2021. In this system, requests tend to be by access numbers, so a larger quantity is received.

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

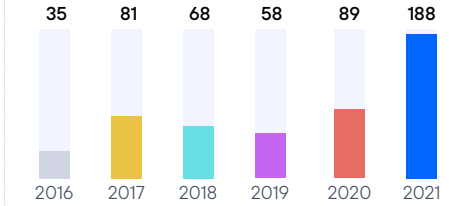
→ Mercantile/Civil/Cont. Administrative/ Criminal Courts.

→ National Intellectual Property Commission.

→ General Gambling Directorate.

→ Spanish Agency for Medication and Healthcare Products.

Requests



Intellectual property

	2020	2021		2020	2021
№ of requests	53	138	№ of URLs affected	2,117	2,297

Crimes

	2020	2021		2020	2021
№ of requests	18	30	№ of URLs affected	178	136

Medication

	2020	2021		2020	2021
№ of requests	10	12	№ of URLs affected	10	29

Illegal gambling

	2020	2021		2020	2021
№ of requests	8	8	№ of URLs affected	978	1,300

3,762 URLs affected

1 Requests rejected

*Of the total requests, three are considered continuous throughout the reporting period. The reason is the application of judicially authorised dynamic, weekly and monthly blocking processes:
1) Judgment of 11 February, 2020 of the Mercantile Court 7 of Madrid, which found in favour of the Claim of TELEFÓNICA AUDIOVISUAL DIGITAL, S.L.U. (TAD), to protect the contents of the Movistar+ Platform. 2) Judgments of the Commercial Courts № 2 and 8 of Barcelona, regarding the lawsuit filed by the partners of MPA (Motion Picture Association). 3) Protocol, under the impulse of the Ministry of Culture, for the reinforcement of the protection of intellectual property rights, which implements the application of judgments and court orders. All of them enable a weekly and monthly list to be prepared and sent with URLs/Domains that Telecommunications Operators/Internet Access Providers in Spain must block or unblock, as requested.

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

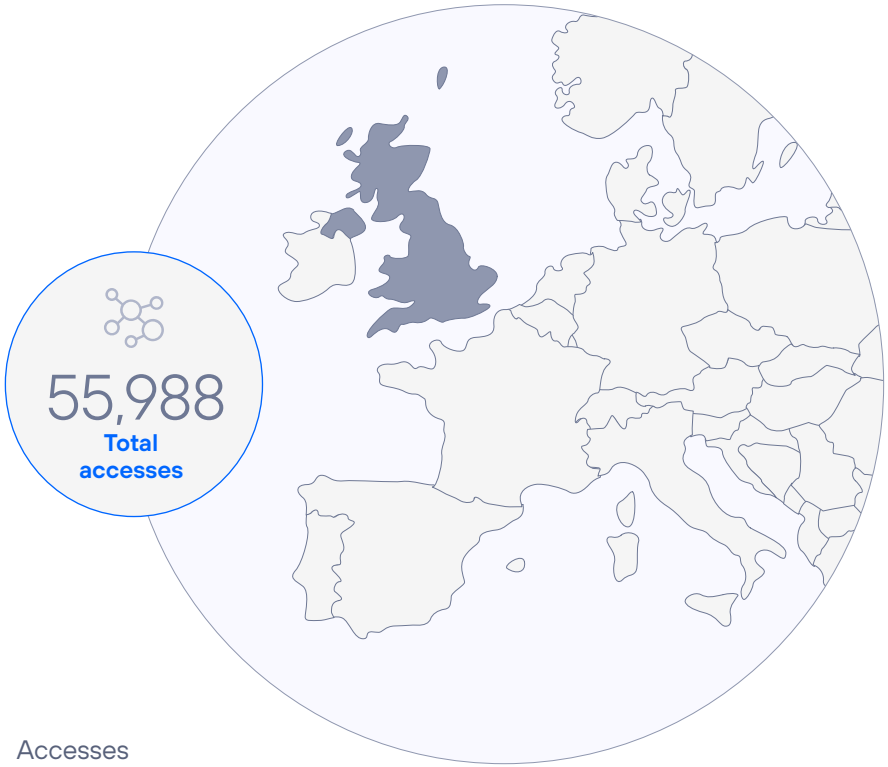
2016	2017	2018	2019	2020	2021
N/A	N/A	N/A	N/A	N/A	N/A

N/A
Accesses affected

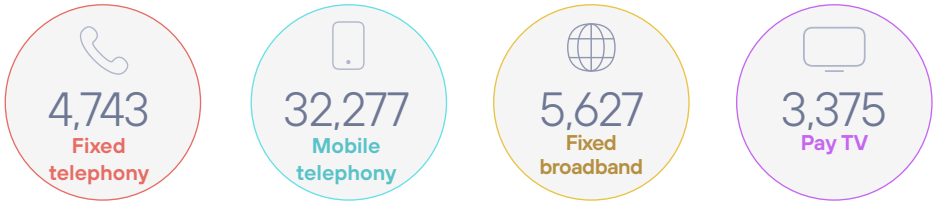
N/A
Requests rejected

United Kingdom

www.telefonica.com/en



Accesses



Accesses at closing 2021 (data in thousands).

Telefónica started operating in the United Kingdom in 2006, after acquiring O2, which became the trade name of Telefónica UK Limited.

The company offers a wide range of products and services over its 2G, 3G, 4G and 5G networks. In addition, O2 owns 50% of Tesco Mobile, as well as O2-Wifi.

In May of 2021, Liberty Global (Virgin Media) and Telefónica entered into an agreement to merge their businesses in the United Kingdom. This is one of the largest transactions in Telefonica's history.

The company managed more than 55.9 million accesses at the end of 2021 in the UK.

With regard to the financial figures, in 2021 Telefónica's revenue in UK stood at €2,628 million and OIBDA amounted to €919 million.

The deal between O2 and Virgin Media in 2021 has been one of the most significant transactions in the history of the Telefónica Group so far. After reaching an agreement with Liberty Global on 7 May 2020 to merge their respective businesses in the United Kingdom and create a joint venture (JV) owned 50% by each company, on 1 June 2021, the transaction was completed, having received regulatory approvals, and fulfilled the necessary recapitalisation and the rest of the conditions agreed for the completion of the aforementioned transaction.

Data reported hereafter is up to the creation of the JV (01/06/2021).

Lawful interceptions

Legal framework

In 2018, the statutory interception provisions under the Regulation of Instruction Powers Act 2000 (RIPA) and the Intelligence Services Act 1994 (ISA) were replaced by the Investigatory Powers Act 2016 (IPA). This process was completed in November 2018.

The Investigatory Powers Commissioner (IPC) is fully established and the Investigatory Powers Commissioner's Office (IPCO) has replaced the Interception of Communications Commissioner's Office (IOCCO). The role of the IPCO is to oversee implementation and compliance with lawful interception requests made under the IPA.

Competent authorities

The principles of the RIPA have continued under the IPA but with additional oversight by the judicial authorities. Under the IPA, the Secretary of State for a relevant Government department can issue an intercept warrant where he/she believes it is necessary in the interests of national security, for the purpose of preventing or detecting serious crimes or for the purpose of safeguarding the economic well-being of the United Kingdom.

There are eight authorized agencies in the United Kingdom who may request a warrant to be issued by the Secretary of State. They are:

- A person who is the head of an intelligence service;
- The Director General of the National Crime Agency;
- The Commissioner of Police of the Metropolis;
- The Chief Constable of the Police Service of Northern Ireland;
- The chief constable of the Police Service of Scotland;
- The Commissioners for Her Majesty's Revenue and Customs;
- The Chief of Defence Intelligence; and
- A person who is the competent authority of a country or territory outside the United Kingdom for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.

In order to obtain a warrant for lawful interception, the requesting authority must make an application to the relevant Secretary of State. The Secretary of State must consider, in deciding whether to issue the warrant, whether (amongst other things), there are established grounds to justify the issue of the warrant (see above) and whether the interception authorised by the warrant is proportionate to what is sought to be achieved by that interception.

As of November 2018 all requests for lawful interception have been pursuant to the IPA and must be authorised by the Secretary of State (or their deputy) in the form of a warrant and a judge. The judge will consider the same factors as the Secretary of State (i.e., whether there are grounds for the issuing of the warrant and whether the conduct is proportionate to the objective).

Requests*

*Section 57 of the IPA prohibits the disclosure of the existence of any lawful intercept warrant save for in exceptional circumstances as per section 58 of the IPA.

IPCO produces a yearly report on the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities. This gives details of the overall numbers but not by company. Please see: https://www.ipco.org.uk/publications/annual-reports/

Access to Metadata

Legal framework

The provisions for disclosure of communications data under RIPA and the ISA, and the Counter Terrorism and Security Act 2015 (CTSA) were superseded by the IPA in February 2019.

The provision for communications data retention, previously retained under the Data Retention Investigatory Powers Act 2014 (DRIPA 2014), is now made under section 87 of the IPA.

Competent authorities

Under Section 61 of the IPA, a senior official designated by a relevant public authority may authorise the disclosure of data. Similar to RIPA, under the IPA, persons who may authorise the disclosure of data are usually senior police officers or other senior officials of the relevant security services. These officials, except in emergency situations, will be required to obtain prior authorization from the Communications Data Clearance Office, which makes an independent decision on whether to grant or refuse requests for communications data.

Requests*

*Section 82 of IPA makes it a criminal offence to disclose details of requests made for communications data.

As stated previously IPCO produces a yearly report, which gives the total industry number. Individual company numbers are not disclosed.

Blocking and filtering of certain contents

Legal framework

→ Section 97A of the Copyright Designs and Patents Act (1988).

→ S.37 (1) Senior Courts Act 1981.

→ Article 11 of the IP Enforcement Directive.

The only content filtering the UK government require from UK broadband and mobile operators is use of the Internet Watch Foundation (IWF) blocking list for illegal child abuse sites. This is part of an agreement with the law enforcement community to prevent child exploitation. This is not a legal requirement. In 2004, Telefónica UK was a founder signatory to the UK mobile operators' child protection code of practice for the self-regulation of new forms of content on mobiles. This Code also explains that we will voluntarily block access to 18-rated content unless a customer has confirmed they are over 18. This is legal content. e.g. legal adult sites (unlike IWF sites which are child abuse sites).

The existence of this code of practice and compliance with it by UK mobile operators is unusual. It is unusual in that it is not something (to our knowledge) that is replicated in other countries and also it is unusual in that it is not binding but yet still complied with by the mobile operators.

The code of practice can be viewed here: https://www.mobileuk.org/codes-of-practice

Competent authorities

→ Internet Watch Foundation.

→ Courts.

Requests*

*Only IWF, no stats available.

In 2021, Virgin Media received 6 requests to block websites for content intellectual property infringement.

Geographical or temporary suspension of the service

Legal framework

Telefónica UK has obligations to be able to provide service limitations in network overload situations – e.g. major disaster, etc– to provide priority service to emergency responders. The Mobile Telecommunications Privileged Access Scheme (MTPAS) was created under the Civil Contingencies Act 2004 (CCA). Eligibility is restricted to organisations that have a part to play in responding to, or recovering from, an emergency as defined in the CCA.

At the onset of an emergency response, the relevant Police commander will use an agreed protocol to notify all mobile network operators that a major incident has been declared and request that call traffic levels are monitored. If networks become congested, the network operators are asked to consider invoking MTPAS to give emergency responders a much higher likelihood of being able to make a call than other customers.

Competent authorities

- The relevant Police commander will use an agreed protocol.
- Suspension of services are negotiated between the emergency authorities and the CSP and Telefónica UK can resist if we feel the action would not impact network loading.

Requests

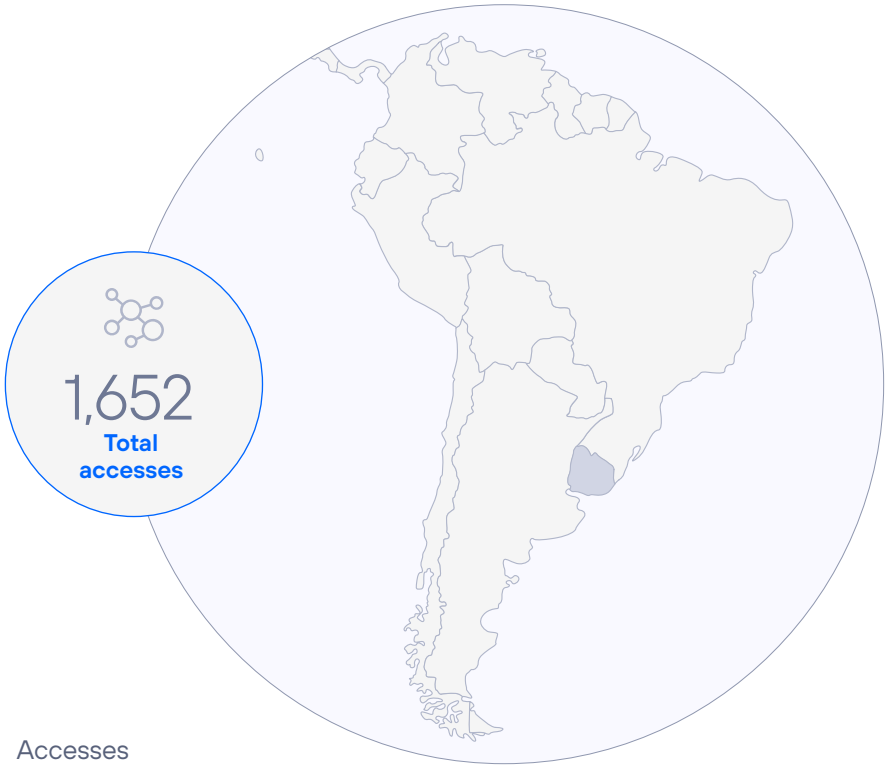
2016	2017	2018	2019	2020	2021
0	0	0	0	0	0

0 Accesses affected

0 Requests rejected

Uruguay

www.telefonica.com.uy



Accesses

0.0	1,652	0.0	0.0
Fixed telephony	Mobile telephony	Fixed broadband	Pay TV

Accesses at closing 2021 (data in thousands).

Telefónica has been present in Uruguay since 2005.

In 2021, Telefónica's revenue in Uruguay reached 184 million euros and the OIBDA was 75 million euros.

Data as of the end of 2021

Lawful interceptions

Legal framework

→Constitution of the Republic, article 28.

→Law 18,494, article 5.

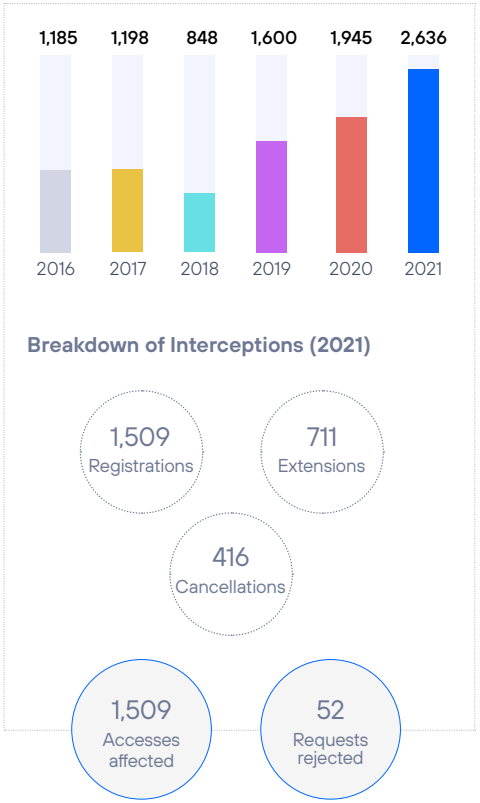
→Reserved Decree of 13 March 2014.

→Decree 214 of the Ministry of the Interior 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



Access to Metadata

Legal framework

→Constitution of the Republic, Article 28.

→Law 18,494, Article 5.

→Reserved Decree of 13 March 2014.

→Decree 214 of the Ministry of the Interior of 26 October, 2021.

Competent authorities

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

Requests*

* The increase in comparison to 2016 is due to the fact that from 2017 onwards a tool has been used that allows every access affected to be counted. Until then, the same request could contain more than one affected access. As of 2017, each request corresponds to one affected access. Therefore, the increase in 2017 is due to the change in the accounting criteria.

Blocking and filtering of certain contents

Legal framework

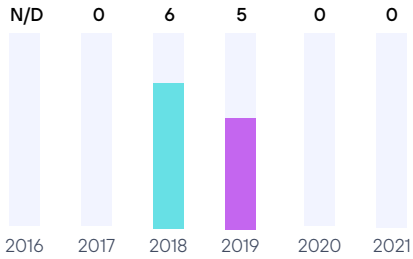
→ Law 19.535 of 25 September 2017, articles 244 and 245.

→ Decree 366/2017 regulated the provisions of articles 244 and 245 of Law 19,535, 21/12/2017.

Competent authorities

The Executive 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.

Requests*



*Games and sports betting online.

Geographical or temporary suspension of the service

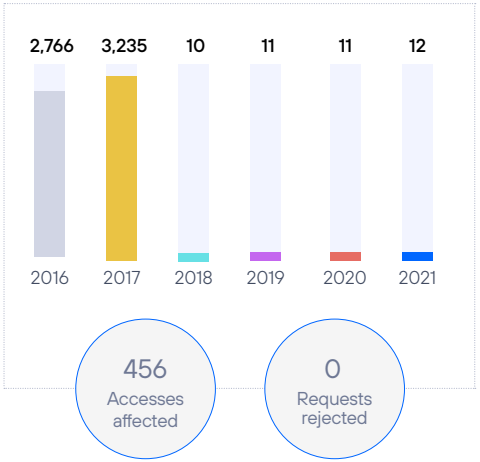
Legal framework

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 Power).

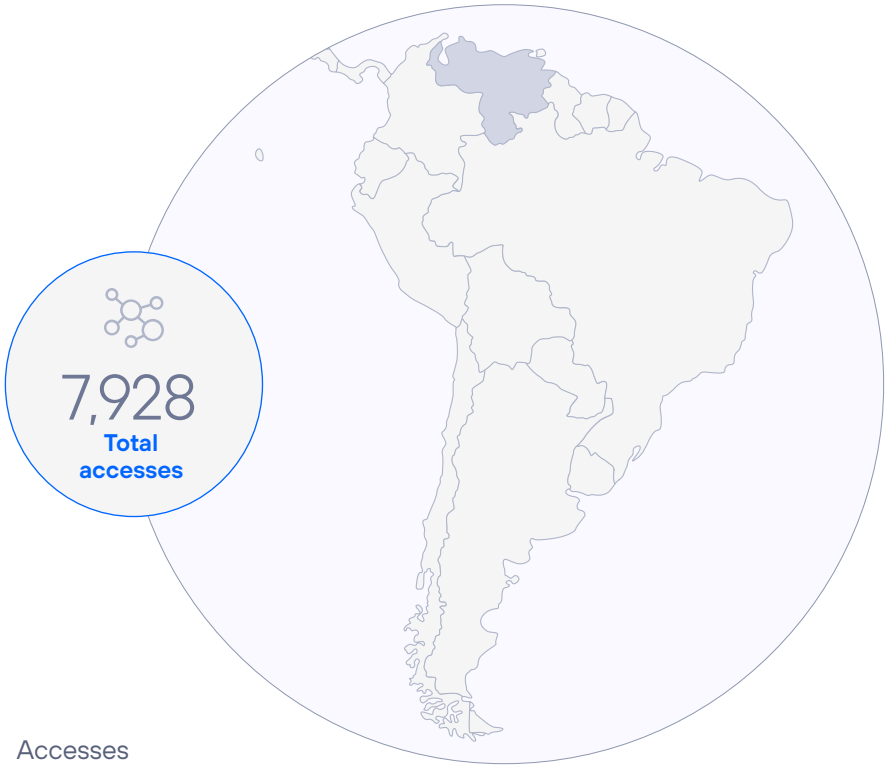
Requests*



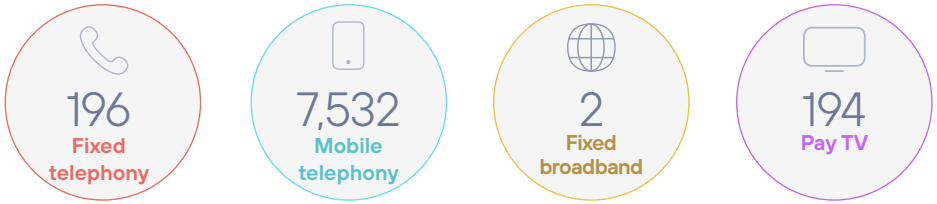
*Temporary suspension for a period of 3 to 6 months.

Venezuela

www.telefonica.com.ve



Accesses



Accesses at closing 2021 (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 2021, Telefónica's income in Venezuela was 82 million euros and the OIBDA stood at 40 million euros.

Data as of the end of 2021

Lawful interceptions

Legal framework

→Organic Criminal Procedure Code, art. 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.

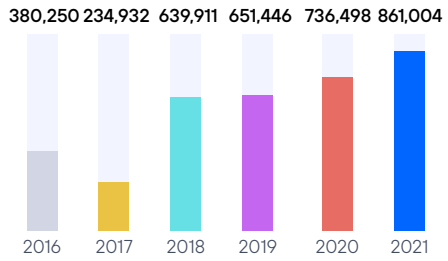
→The Scientific and Criminal Investigation Service Corps (CICPC).

→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.

Requests*



1,584,547 Accesses affected

21,601 Requests rejected

*There are no requests for extensions and cancellations because the only interventions that are made are only for location and subscriber data in real time.

Access to Metadata

Legal framework

→Administrative Ruling № 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).

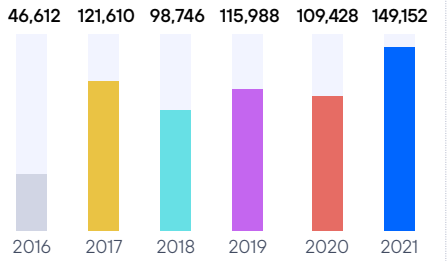
→The components of the Bolivarian National Armed Forces, within the limits of their competence.

→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.

Requests



997,679 Accesses affected

1,613 Requests rejected

Blocking and filtering of certain contents

Legal framework

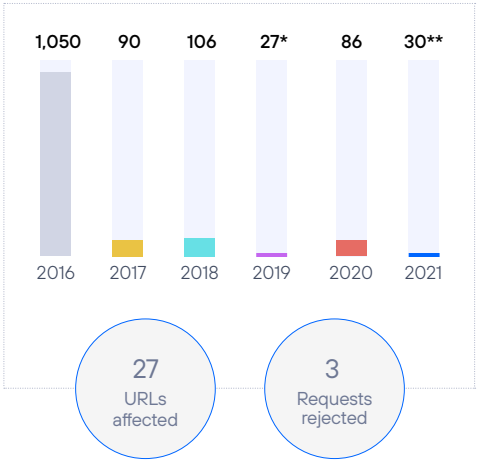
→ Organic Law on Telecommunications, article 5.

→ Law on Social Responsibility in Radio, Television and Electronic Media, article 27.

Competent authorities

National Telecommunications Commission (CONATEL).

Requests



*Online gambling

** URLs affected: 27 (each request contains only one request, 3 blocking requests were previously implemented).

Typology: No details.

Rejected requests: 3

Geographical or temporary suspension of the service

Legal framework

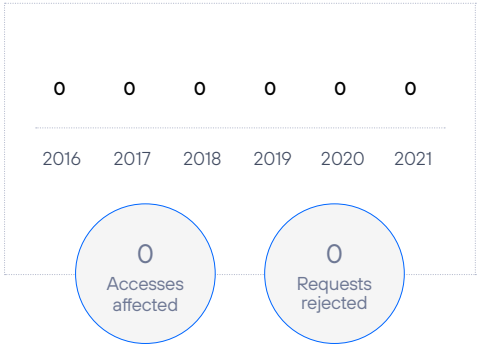
Organic Law on Telecommunications, article 5.

Competent authorities

→ Ministry of Transport and Communications (MTC).

→ National and Civil Defence System.

Requests



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 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 are the initials which 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 are the initials which stand for International Mobile Station Equipment Identity. It has a serial number which physically identifies the terminal. The IMEI enables the operator to identify valid terminals which, 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	We consider "major events" to be 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, human rights groups' websites, etc.).

CONCEPT	EXPLANATION
MAJOR EVENTS (cont.)	→ Specific shutdown of any kind of telecommunications services, resulting from political causes, (e.g., concerning a small number of cells). → 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 change proposals) involving 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.
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 individualized 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 are the initials which stand for a 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, videos, etc.

Telefónica