

2019  
Report on  
**Transparency**  
in Communications



# Index

<b>Introduction</b>	<b>3</b>
<b>Policies and processes</b>	<b>7</b>
<b>Scope of the report</b>	<b>10</b>
<b>Indicators of this report</b>	<b>11</b>

<b>Report by country</b>	<b>13</b>
--------------------------	-----------

Argentina	14
Brazil	16
Chile	19
Colombia	22
Costa Rica	26
Ecuador	28
El Salvador	30
Germany	32
Mexico	35
Peru	37
Spain	40
United Kingdom	43
Uruguay	47
Venezuela	50

<b>Glossary</b>	<b>53</b>
-----------------	-----------



# Introduction



As testament to our commitment to the fundamental rights of privacy and freedom of expression, we are publishing our fourth Transparency Report with the aim of contributing to a more open and transparent society.

The promotion of and the respect for people's fundamental rights, particularly privacy and freedom of expression, acquires a new dimension in the digital world due to the use of new technologies and the growing importance of data on a global scale.

As telecommunications operators, we have the duty and legal obligation to respond to requests made by competent authorities in all the countries in which we operate to ensure the safety and the rights of their citizens, always in compliance with the respective legislation as well as fundamental rights and freedoms.

Transparency is an essential exercise in this context, that is in a world in which spaces of responsibility are shared when it comes to preserving and guaranteeing people's rights.

## Our Governance

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

The promotion and protection of these issues fall under the supervision of the Board of Directors via the Regulation and Institutional Affairs Committee. The Board of Directors is the body responsible for approving the Group's Global Policies.



More information in the section  
"Policies and processes for implementation"

To be more precise: The aforementioned Regulation and Institutional Affairs Committee (a standing Board committee) is responsible for promoting the implementation of the Global Responsible Business Plan, which includes objectives regarding privacy and freedom of expression. The committee is informed monthly on the implementation of the Plan by the Corporate Ethics and Sustainability Department, which leads the Responsible Business Office that integrates all relevant department heads at global level.

The Corporate Ethics and Sustainability Department coordinates the task of identifying, assessing and addressing the risks and opportunities related to human rights and promoting stakeholder dialogue on these issues.

The results of the human rights impact assessments are presented to the Responsible Business Office (see above) as well as the Committee of the Board of Directors (see above) in charge of monitoring

the Responsible Business Plan with a view to taking them into account in decision-making-processes.

The Data Protection Officer (DPO) is the function responsible within the Group for the protection of personal data and reports directly to the Board of Directors via the Audit and Control Committee (a standing Board committee). The DPO coordinates a Steering Committee involving all relevant corporate areas for specific matters relating to privacy and freedom of expression. As a member of the aforementioned Responsible Business Office, the DPO regularly feeds issues related to his function back into said Office.

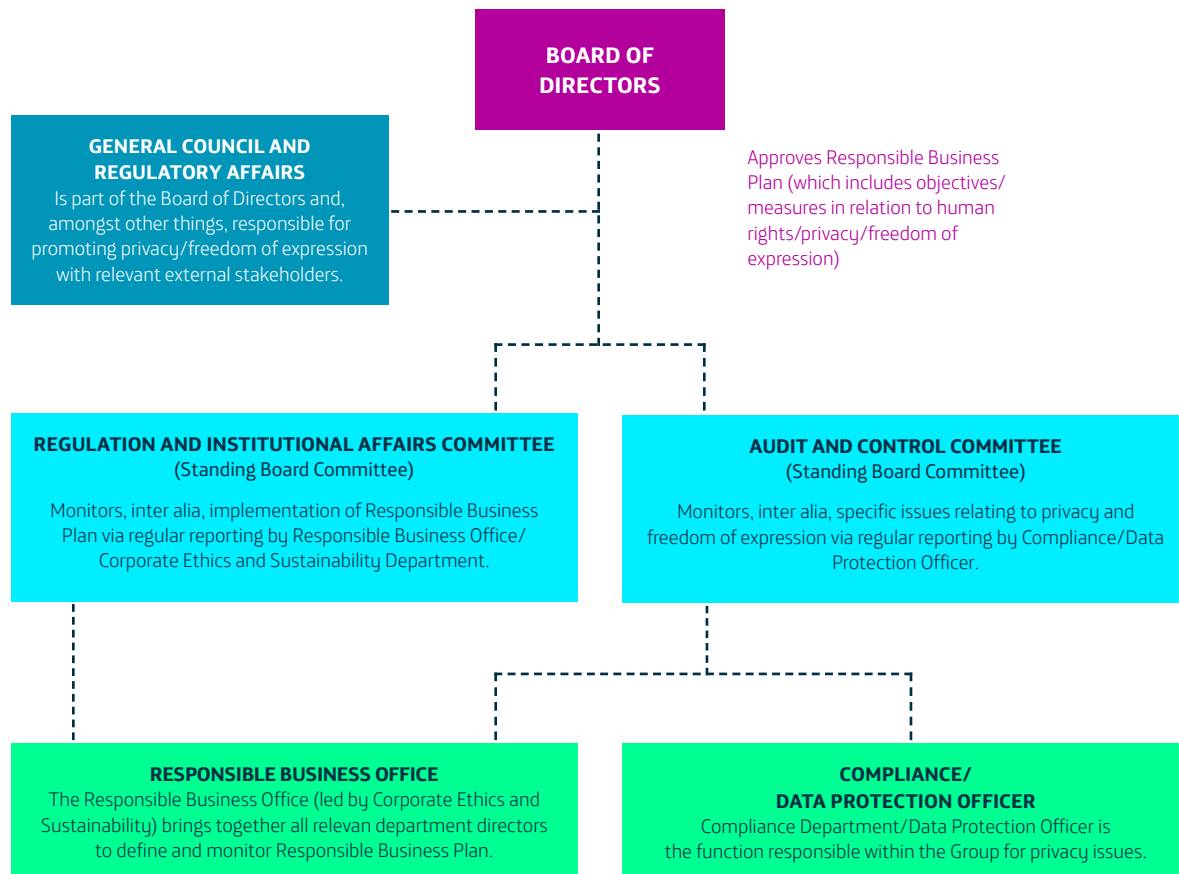
In addition, the General Council and Global Head Regulatory Affairs is part of the Board of Directors

and responsible, amongst other things, for promoting privacy and freedom of expression with relevant external stakeholders. In this function, he also led the publication and dissemination of Telefonica's "Digital Manifesto" in 2018, which calls for a new cooperative effort between governments, business and civil society to define a New Digital Deal adapting the current regulatory environment for the digital age, paying special attention to the issues of privacy and freedom of expression.



More information in  
[www.telefonica.com/digital-manifesto/](http://www.telefonica.com/digital-manifesto/)

The figure below graphically summarizes this governance model:







We have a Transparency Committee for privacy and freedom of expression issues related to requests made by competent authorities, which is made up by the Legal Department, Compliance, Internal Audit and Corporate Ethics and Sustainability. The Transparency Committee analyses the reported data 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 at all times the quality of the data as evidence of complying with current legislation and the protection of people's fundamental rights.

Those requests, which due to their characteristics and exceptional nature so require, are being analysed by the heads of the respective units by means of an appropriate weighing of all potentially compromised interests, including human rights, fundamental freedoms or other interests which may be applicable and, if circumstances arise, by the bodies within the company whose functions include the assessment and management of situations which could eventually lead to a crisis.

## Our commitment and due diligence processes

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 promote the guarantee of and respect for people's fundamental rights and, specifically, with regard to privacy and freedom of expression.

We are a founding member of the Telecommunications Industry Dialogue Group on Freedom of Expression and Privacy (TID), which merged with the Global Network Initiative (GNI) in 2017. This is a global organization which aims at promoting and protecting privacy and freedom of expression, and which is made up of a multistakeholder group, members of which include investors, civil society and private companies like telecommunications operators, internet service providers, and computer and software manufacturers.

As a member of GNI, Telefónica is one of the signatory companies of the "Principles of the Communications Sector on Freedom of Expression and Privacy" and assumes its commitment to implement and comply with them through assessment reviews by independent assessors.

As part of our due diligence process, every four years, we conduct an impact assessment of how our activities (either directly or through our business partners) may be affecting people's fundamental rights. To this end, we work with internal and external experts to identify where and how our activity may

## Issues and human rights matters

 <b>Direct action</b>	<b>Network Deployment</b> <ul style="list-style-type: none"><li>› Property</li><li>› Health and Safety</li><li>› Environment</li><li>› Information</li><li>› Indigenous population</li></ul>	<b>Terms of goods/services</b> <ul style="list-style-type: none"><li>› Equality and non-discrimination</li><li>› Freedom of opinion and expression</li><li>› Responsible communication</li><li>› Privacy</li><li>› Health and Safety</li><li>› Vulnerable groups</li><li>› Intellectual and industrial property and copyright</li></ul>	<b>New technologies, and developements related to Artificial Intelligence</b> <ul style="list-style-type: none"><li>› Privacy</li><li>› Security</li><li>› Equality and non-discrimination</li><li>› Other rights that may be affected</li></ul>	<b>Working conditions</b> <ul style="list-style-type: none"><li>› Equality and non-discrimination</li><li>› Health and Safety</li><li>› Equal and decent working conditions</li><li>› Freedom of association, social dialogue and trade union rights</li><li>› Forced labour and other modern forms of slavery</li><li>› Child labour and the protection of young people at work</li></ul>	
 <b>Indirect action</b>	<b>Supply Chain</b> <ul style="list-style-type: none"><li>› Labour rights</li><li>› Equality and non-discrimination</li><li>› Rights associated with minerals from conflict zones</li></ul>	<b>Mergers and acquisitions and strategic alliances</b>			
 <b>Contributes to</b>	 <b>Environmental impact</b>	 <b>Anti-competitive practices</b>	 <b>Financial responsibility</b>	 <b>Digital divide</b>	 <b>Corruption and bribery</b>

be causing that impact and to define a formal process that facilitates proactive risk management and the exploitation of opportunities, actively involving our main stakeholders.

In 2013, together with BSR "Business for Social Responsibility", we carried out our first impact assessment in all our operations. Privacy and freedom of expression were identified as two issues to be managed within the matrix. In 2017, we updated our impact matrix on the basis of a new assessment by BHR ("Business & Human Rights") in order to understand the potential impacts of our strategy, the Group's new activities, and a constantly changing digital environment.

Privacy and freedom of expression rights were identified as relevant in the following activities:

- » Conditions of products and/or services.

- » New technologies and developments related to artificial intelligence.
- » Joint ventures, acquisitions and strategic alliances.

Once the analysis was completed, a number of activities and themes were identified that merited a deeper analysis.

As a consequence, during 2018, we began evaluating the impact of our activity: during process of network deployment, in the development of new products and services –including those in which Artificial Intelligence is applied–, and on the rights of the children and adolescents. In the latter two, among the issues to be assessed were privacy and freedom of expression.

In 2019 and as a result of this due diligence process, we updated our existing human rights commitment through the adoption of our Global Policy on Human Rights.

# Policies and processes

We have initiated and updated various policies and processes to ensure the protection of the rights to privacy and freedom of expression:

» **Global Human Rights Policy:** Approved in 2019, this policy formalizes our commitment to human rights which is also more generally included in Telefónica's Business Principles, and more specifically, in a set of policies and processes that ensure the respect for and application of internationally recognized social, economic and cultural human rights.

» **Privacy Policy:** Updated in 2018, this policy forms part of Telefónica'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, in general, of our stakeholders, this policy guarantees them control over and the value of their personal data when they are processed by Telefónica.

It establishes the general 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 conservation period.

» **Governance Model Rule on Personal Data Protection:** Its goal is to encompass the most important aspects to be taken into account for the proper management and protection of personal data.

It establishes an organizational and relationship model in which the chief responsible 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, the following relationship and governance structure is established:

» **The DPO Office:** This office is responsible for coordinating the compliance and data functions to ensure the execution of the overall compliance program in the Group and takes on a technical function of data protection supervising compliance with the data protection regulations of the Telefónica Group.

» **Steering Committee:** This committee includes the relevant areas of the company (Legal Department; Regulation and Institutional Affairs; Technology; CDO; Compliance; Corporate Ethics and Sustainability and Internal Audit) and reviews compliance with the governance model in data protection matters.

» **Business Committees:** Through the technical function of data protection, the DPO Office maintains permanent interactions with other areas, via the Compliance Officers, in order to ensure maximum uniformity in the application of common processes, and/or identification, and treatment of specific privacy issues in the area of activity in each area.

» **Rule on Requests made by Competent Authorities:** This rule was approved in 2019 to strengthen the procedure already existing since 2016, with the aim of aligning it with other existing policies 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 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 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 ones with legal competence in the handling of these requests. We have fixed interlocutors as a one-stop shop in our relationship with the competent authorities, so we reject any request that does not come through these official channels.

- » **Global Security Policy:** Updated in 2016, it is guided by national and international standards and regulations in terms of logical and physical security, establishes the guiding principles in security matters which are applicable to all companies that are part of the Telefónica Group.

Security activities are governed by the following principles:

- » **Legality:** Compliance with national and international laws and regulations in security matters.
- » **Efficiency:** The anticipatory and preventive nature of any potential risk and/or threat is highlighted with the objective of anticipating and preventing any potential harmful effect and/or mitigating any damage that may be caused.
- » **Co-responsibility:** The duty of users to preserve the security of the assets that Telefónica makes available to them.
- » **Cooperation and Coordination:** In order to achieve the required levels of efficiency, priority

is given to cooperation and coordination between all business units and employees.

As a result of this policy, during 2017-2018, several regulations were updated to ensure effective compliance with it (Incident and Emergency Management Regulations; Security Risk Analysis Regulations; Network and Communications Security Regulations; Cybersecurity Regulations; Supply Chain Security Regulations and the Government Security Regulations, among others).

#### » **Telefónica Group Responsible**

**Communication Regulation:** Approved in October 2018, its objective is to establish guidelines for Telefónica's actions in relation to our communication and content generation channels. It is based on the principles of legality, integrity and transparency, neutrality and protection of minors. As for 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.

- » **AI Principles of Telefónica:** Approved by the Executive Committee in October 2018, we are committed to designing, developing and using Artificial Intelligence with integrity and transparency. Our IA 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 emphasize 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.

- » **Integration of human rights into Enterprise Risk Management:** Risks related to human rights impacts have always been present in Telefónica's risk mapping model. In 2017 however, the human rights risk was specifically included in this model. The objective is to identify any risk of direct or indirect impact of Telefónica Group's operations on 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 facilitates the definition of the necessary actions 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 a view to planning supervisory activities for internal control reasons.

» **By-Design-Approach: Reputation Risk Assessment and Impact on Human Rights in the Telefónica Group's Value Proposals:**

The objective is to evaluate the possible impact of Telefónica Group products and services in the design phase, for consumers (B2C), clients (B2B) as well as indirectly (B2B2C) in the design and marketing phase. Issues assessed include privacy and freedom of expression.

» **Responsible Business Channel:**



More information in  
[www.telefonica.com/en/web/about\\_telefonica/  
responsible-business-channel](http://www.telefonica.com/en/web/about_telefonica/responsible-business-channel)

Created at the end of 2016 and directly linked to our Business Principles and our Human Rights Policy, its objective is to be a communication channel where any stakeholder can raise grievances or inquiries regarding our impact on, inter alia, privacy and freedom of expression via the form that is available on our website. We have a written procedure in place to ensure the proper functioning of the Responsible Business Channel.



More information in [www.telefonica.com/  
documents/153952/141150866/Responsible\\_Business\\_  
Channel\\_Procedure\\_Receiving\\_Processing\\_Communications.  
pdf/0a35d576-30ca-471b-5eef-d66dd807c69f](http://www.telefonica.com/documents/153952/141150866/Responsible_Business_Channel_Procedure_Receiving_Processing_Communications.pdf/0a35d576-30ca-471b-5eef-d66dd807c69f)

# Scope of the report



Like other companies in our sector, at Telefónica we receive information requests concerning the communications of our customers and users, requests to block access to certain sites or content or to filter content, as well as requests to temporarily suspend services in specific areas (in the event of civil unrest or disturbances of public order, for instance) by judges and courts, law enforcement agencies and other governmental administrations or bodies empowered by local legislation.

It is against this background that this Transparency Report elaborates on:

- » **The commitments, policies and processes** that we follow when responding to these requests from the Competent Authorities.
- » **The legal context** that gives legal power to the authorities to make these types of requests.

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 do not provide them.

- » **The Authorities that have the legal competence** according to the local legislation regarding the indicators we report.
- » **The total number of requests** we receive during the last year in each country we operate, unless we are prohibited to do so or a government or other public entity already discloses such information.

In addition, when technically possible, we report the number of **requests rejected and the accesses affected** for each indicator.

# Indicators of this report

In the following sections we report the number of requests we receive from the competent national authorities in the countries in which we operate. We have not included Guatemala, Nicaragua and Panama, because at the time of publication of this report our divestment process had been completed in these markets.

Any request received from a non-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. At Telefónica we do not deal with private requests, but only with requests from authorities that are empowered to do so by the law.



More information, in the section "Glossary".

Thus, the indicators we report are:

- » **Lawful interceptions:** Orders and requests originating from the competent authorities, within the framework of criminal investigations and, if appropriate, civil cases, with the aim of intercepting communications or accessing data traffic in real time. This includes new interventions, extensions and removals.
- » **Access to metadata:** All requests originating from competent authorities whose aim is to obtain history data involving:
  - » 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 date;
- » Time and duration;
- » Computer equipment identities (including IMSI or IMEI);
- » User or device location.

- » **Blocking and filtering of certain contents:** Requests from competent authorities to block access to specific websites or 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).

- » **Geographical and temporary suspensions of service:** Requests from 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.

In addition, for each indicator we have added the following sub-indicators:

- » **Number of requests rejected or partially addressed:** 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 the request does not comply with local legislation for that type of request.
  - » Because the request does not contain all the necessary elements to execute the latter

(necessary signatures, competent authority, technical description of the request etc.).

- › Because of the technical impossibility of executing the request.

» **Affected accesses:** number of accesses that are affected by a request. Thus, the following scenarios can occur:

- › That a request affects a single access.
- › That the same request affects several accesses (for example, regarding metadata access: A request can request data from several mobile phone and landlines).
- › That several petitions affect the same access (e.g. regarding access to metadata: Multiple requests can be made during a reporting period for the same mobile phone or landline).

Therefore, there are cases in this report where the number of requests exceeds the number of accesses and vice versa.

Regarding the indicator content blocking: The blocking of a web/url affects all users who want to access its content. In such a case, we cannot measure the number of accesses affected. However, we report number of affected URLs.

What is more, this Transparency Report also seeks to inform in a transparent manner about our efforts regarding those requests that may have a potential impact on the rights of privacy and/or freedom of expression as they are framed within what we call "major events".



More information, in the section "Glossary".

In this regard, 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.







# Report by country

Argentina

Brazil

Chile

Colombia

Costa Rica

Ecuador

El Salvador

Germany

Mexico

Peru

Spain

United Kingdom

Uruguay

Venezuela



# Argentina

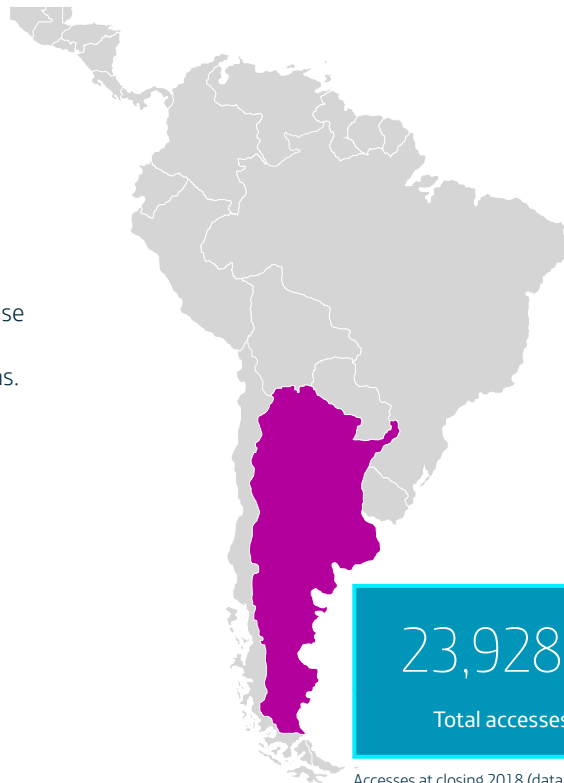
www.telefonica.com.ar

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

In these years, Telefónica Argentina contributed to the development of communications through infrastructure investments and a wide range of fixed and mobile telephony and Internet services.

The Company managed more than 23.9 million accesses at the end of December 2018.

With regard to the financial figures, in 2018 Telefónica's revenue in Argentina stood at 2,315 million euros and the OIBDA was 669 million euros.



23,928.3

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

3,667.3	18,666.8	1,546.1	0.0
Fixed telephony	Mobile telephony	Broadband	Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

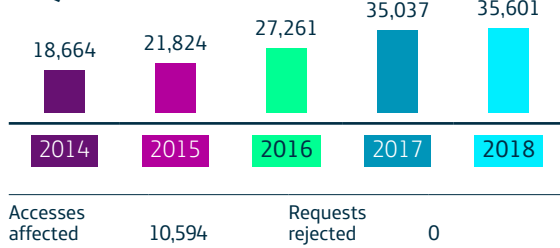
### Legal framework

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

### Competent authorities

- » Judges. The procedure establishes that the latter must officiate at the Directorate for the Capturing of Communications, a body currently dependent on the Supreme Court of Justice of the Nation, which is the body that requests the intervention from the corresponding company.

#### REQUESTS



## Access to Metadata

### Legal framework

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

### Competent authorities

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

## Blocking and filtering of certain contents

### Legal framework:

- » Law 27,078, Article 5: Inviolability of communications.

## Competent authorities

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

## Geographical and temporary suspension of the service

### Legal framework:

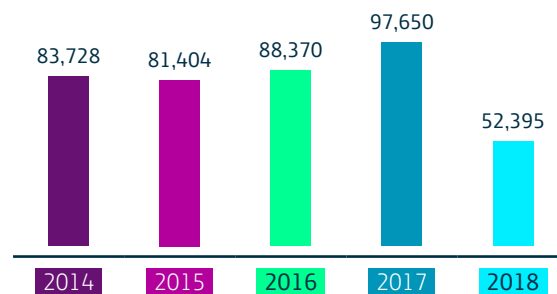
Although there is no specific rule governing this, it may be interpreted as part of what is established in Art. 57 of Law 27,078, as regards;

- » Article 57: Network Neutrality. Prohibitions. IC service providers may not:
  - » Block, interfere, discriminate, disrupt, damage, or restrict the use, sending, receiving, providing or access to any content, application, service, or protocol unless by court order or explicit user request.

### 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\*



\* Data added for Metadata, Content Blocking and suspension of service. Telefonía Argentina counts all the legal requirements that are received, regardless of whether they request Metadata, content blocking or suspension of the service.

Accesses affected	Not available	Requests rejected	Not available
-------------------	---------------	-------------------	---------------

# Brazil

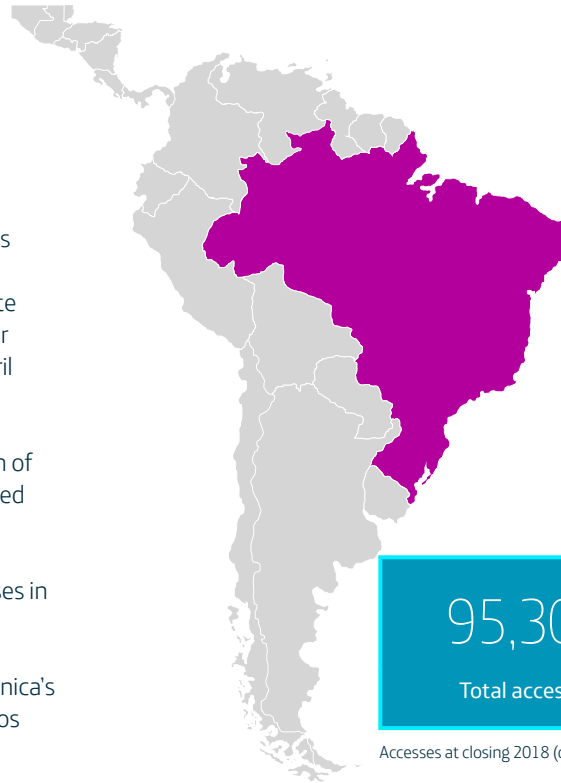
[www.telefonica.com.br](http://www.telefonica.com.br)

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 has closed the acquisition of GVT and has become the leading Brazilian integrated operator.

Telefónica manages more than 95.2 million accesses in Brazil at December of 2018.

With regard to the financial figures, in 2018, Telefónica's revenue in Brazil reached about 10,126 million euros and the OIBDA stood at 4,311 million euros.



95,302

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

13,004.6	73,151.3	7,564.7	1,566.6
Fixed telephony	Mobile telephony	Broadband	Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

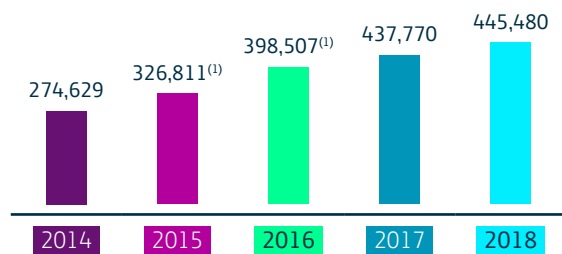
### Legal framework

- » Constitution of the Federal Republic of Brazil: Art. 5.
- » Law N°. 9,296, of 24 July 1996.
- » Resolution N°. 426 of 9 December 2005/Regulation of Fixed Telephone Service - STFC. STFC.
- » Resolution N°. 614 of 28 May 2013/Regulation on Multimedia Communication Service.
- » Resolution N°. 477 of 7 August 2007/Regulation on Personal Service.

### Competent authorities

- » In accordance with article 3 of Brazilian Federal Law N°. 9,296/1996 (Law on Interceptions), only the Judge (in the criminal sphere) can determine the interceptions (both telephonic and telematic), at the request of the Public Prosecutor or the Police Commissioner ("Police Authority").

### REQUESTS



(1) Includes GVT: During 2015 Telefónica acquired GVT.

Accesses affected	445,480	Requests rejected	Not available <sup>(2)</sup>
-------------------	---------	-------------------	------------------------------

(2) The logging system during the reporting period did not have the mechanisms to filter for rejected requests. We are working to make this information available in future reports.

## Access to Metadata

### Legal framework

- » Constitution of the Federal Republic of Brazil: Art. 5.
- » Law N°. 9,296 of 24 July 1996.
- » Law N°. 9,472 of 16 July 1997. Art. 3.
- » Law N°. 12.683 of 9 July 2012. Art. 17-B.
- » Law N°. 12,830, of 20 June 2013. Article 2.
- » Law N°. 12850 of 20 August 2013 Article 15.
- » Law N°. 12965 of 23 April 2014. Art. 7; 10 and 19.
- » Decree N°. 8,771 of 11 May 2016. Article 11.
- » Law N.º 13344 of october 2016, Art. 11.
- » Law N.º 13812 of october 2019, Art. 10.
- » Resolution N°. 426 of 9 December 2005/Regulation of Fixed Telephone Service - STFC. STFC Articles 11, 22, 23 and 24.
- » Resolution N°. 477 of 7 August 2007/Regulation on Personal Service Articles 6, 10, 12, 13, 89 and 90.
- » Resolution N°. 614 of 28 May 2013/Regulation on Multimedia Communication Service Art. 52 and 53.

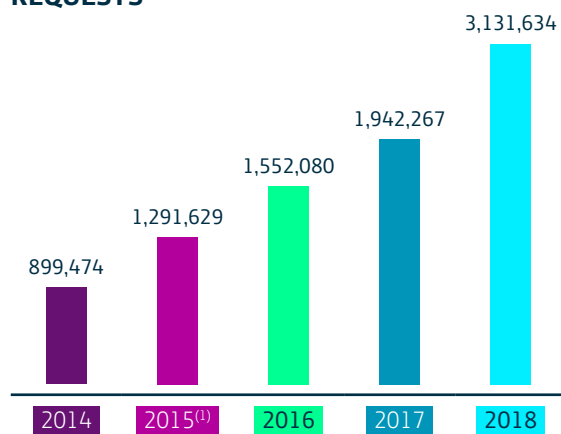
### Competent Authorities

- » Public Prosecutor's Office, Police Commissioners and Judges in any sphere: the name and address of the registered user (subscriber data), as well as the identity of the communication equipment (including IMSI or IMEI).

## Access to Metadata (cont.)

- » 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



(1) The data of the GVT company purchased by Telefónica Brazil in 2015 are not included.

Accesses affected	3,131,634	Requests rejected	Not available <sup>(2)</sup>
-------------------	-----------	-------------------	------------------------------

(2) The logging system during the reporting period did not have the mechanisms to filter for rejected requests. We are working to make this information available in future reports.

## Blocking and filtering of certain contents

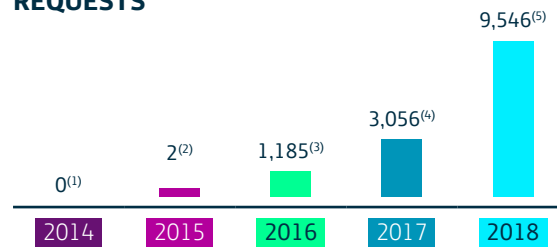
### Legal framework

- » Law N°. 12965 of 23 April 2014. Art. 7 and 19.

### Competent Authorities

- » Exclusively Judges.

### REQUESTS



(1) No data available.

(2) The two cases in 2015 correspond to the blocking of the WhatsApp application.

(3) The increase is due to the fact that after the general blocking measures that affected all potential clients, the public authorities started to practice individual blocking in the field of criminal investigations.

(4) Individual blocking.

(5) In addition to the blocking of individual accounts, 95 URLs have been blocked.

URLs affected	95	Requests rejected	0
---------------	----	-------------------	---

## Geographical and temporary suspension of the service

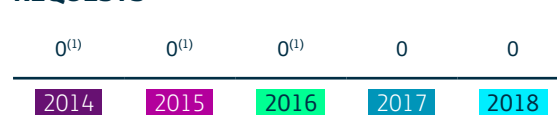
### Legal framework

- » Resolution N°. 73 of 25 November 1998. Article 31.  
» Resolution N°. 477 of 7 August 2007. Article 19.

### Competent Authorities

- » Exclusively Judges.

### REQUESTS



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

Accesses affected	0	Requests rejected	0
-------------------	---	-------------------	---



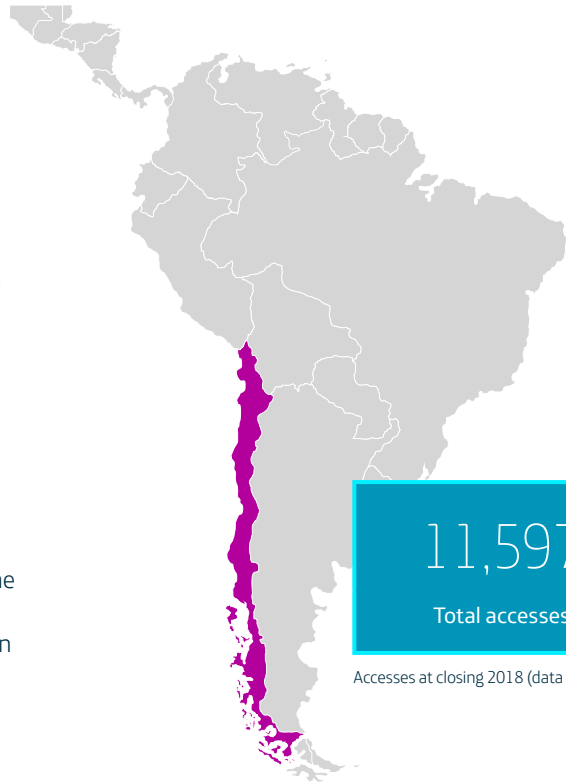
# Chile

[www.telefonicachile.cl](http://www.telefonicachile.cl)

Chile is the first country in Latin America in which Telefónica began its activity, that is in 1989. The Telefónica Group in Chile is a provider of telecommunications services (broadband, digital TV and voice).

Telefónica Chile also concentrates on the expansion of the pay TV business and the progressive adoption of high-speed broadband plans and in the mobile business.

At the end of December 2018, Telefónica had more than 11.5 million accesses in Chile. With regard to the financial figures, Telefónica's revenue in Chile stood at 2,080 million euros and the OIBDA was 617 million euros.



11,597

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

1,222.4

Fixed telephony

8,567.5

Mobile telephony

1,150.2

Broadband

651.3

Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

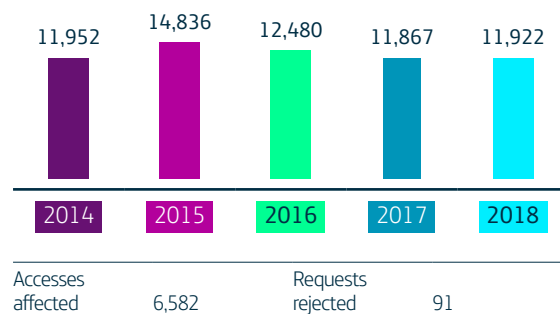
### Legal framework

- » Criminal Procedure Code: Art. 9, 219, 222 and 223.
- » Law 20,000. Drug trafficking and control.
- » Law 19,913 on money laundering.
- » Law 18,314 determining terrorist consultations.
- » Decree Law 211, article 39, letter n).
- » Law 19,974. National Intelligence System Law. Letters a), b), c) y d) of Article 24, in relation to Articles 23 and 28 of the same legal body.
- » Criminal Procedure Code. Art. 177, 113a and 113 ter.
- » Decree 142 of 2005 of the Ministry of Transport and Telecommunications, Regulation on the interception and recording of telecommunication 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.
- » 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



## Access to Metadata

### Legal framework

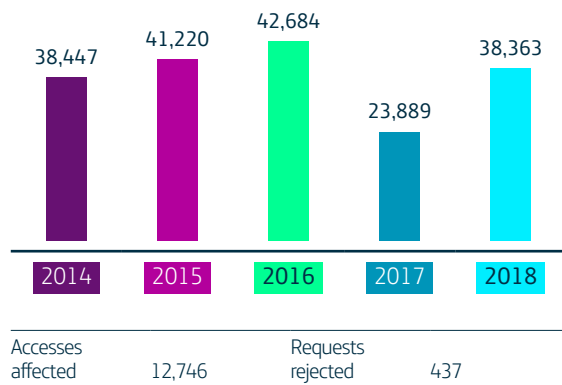
- » Criminal Procedure Code: Paragraph 5 of Art. 222 of the Criminal Procedure Code, in relation to Article 180 of the same legal text, under penalty of contempt of court, Article 240 of the Civil Procedure Code.
- » Inquisitorial Criminal Procedure: Articles 120a and 171 of the Criminal Procedure Code.

### 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). Estate Inteligencia.
- » Agencies with prior judicial authorisation.

## Access to Metadata (cont.)

### REQUESTS



## Blocking and filtering of certain contents

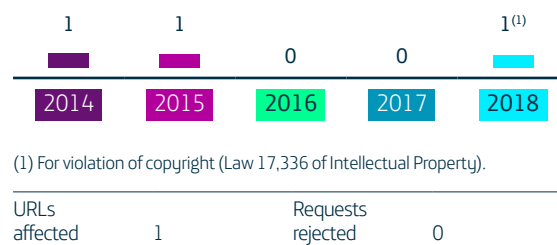
### Legal framework

- » 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



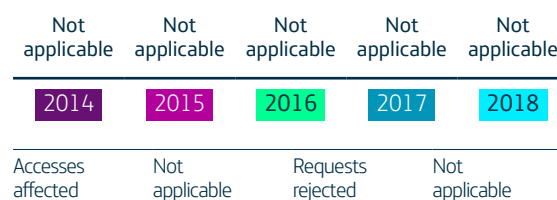
## Geographical and temporary suspension of the service

### Legal framework:

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

Competent Authorities: Not applicable.

### REQUESTS



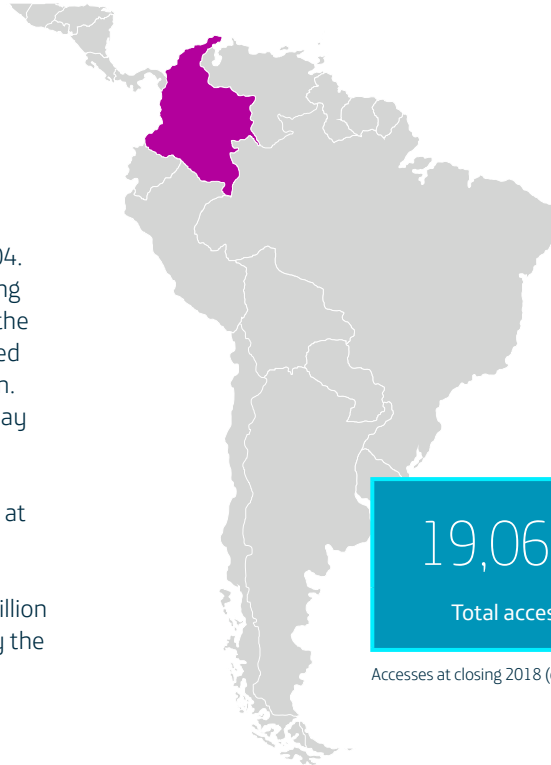
# Colombia

www.telefonica.co

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 Telecom. Today, Telefónica provides voice, broadband and pay television services in the country.

Telefónica Colombia managed 19 million accesses at December of 2018.

Telefónica's revenue in Colombia reached 1,468 million euros and the OIBDA stood at 556 million euros by the end of 2018, .



19,067.8

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

1,582.4

Fixed telephony

15,716.3

Mobile telephony

1,220.4

Broadband

548.2

Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

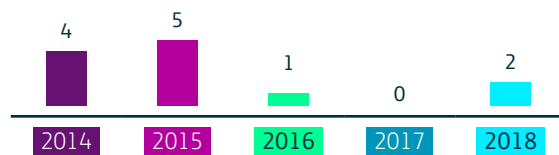
### Legal framework

- » Colombian Constitution: Articles 15 and 250.
- » Law 906, Criminal Procedure Code of 2004. Article 235. Modified by article 52 of Law 1453 of 2011.
- » Law 1621 of 2013, Article 44.
- » Decree 1704 of 2012, Articles 1 to 8.
- » Decree 2044 of 2013, Article 3.

### Competent Authorities

- » Attorney General's Office.
- » Through the Judicial Police group designated for the investigation of the case.

#### REQUESTS\*



\* Only includes interceptions of landlines (fixed lines).

Mobile lines: Interceptions of mobile lines are not reported: The Public Prosecutor of the Nation in Colombia, as the competent authority in accordance with the Constitution and the Law, performs direct interceptions of mobile lines.

Accesses affected	2	Requests rejected	0
-------------------	---	-------------------	---

## Access to Metadata

### Legal framework

- » Colombian Constitution: Article 250.
- » Law 906 of 2004, Art. 235.
- » Law 1621 of 2013 Ar. 44.
- » Decree 1704 of 2012, Art. 1 to 8.

### Competent Authorities

- » Authorities with judicial police functions; these may be of a permanent or transitory nature:

Article 312 of the new criminal procedure code defines that the entities which hold permanent powers of the Judicial Police are as follows:

- » Prosecutor General of the Nation and all the public servants who perform judicial functions (Article 249 CN and articles 112, 113 CPC).
- » Judicial Police: C.T.I., National Police and D.A.S., authorised by the competent judicial authority and by legal mandate (Articles 311 to 320 CPC).
- » "Anti-kidnapping and Extortion" Unified Action Groups (Law 282 of 1996).

Special judicial police functions are exercised (in matters within their competence) by:

- » Controller General of the Nation (Article 267 CN and article 312 CPC).
- » General Procuracy of the Nation (Article 275 CN and article 312 CPC).
- » National Directorate of Taxes and National Customs \_ DIAN (see numeral 2, section II)
- » Public entities which exercise monitoring and control functions.
- » Mayors and police inspectors, in the places in the territory where there are no members of the judicial police of the National Police.
- » National and regional Directors of the INPEC, directors of prison establishments and custodial and surveillance personnel, in accordance with the Penitentiary and Prison Code.
- » Police Inspections (Article 312 CPC).

The offices of internal disciplinary control are authorised for investigations of a disciplinary

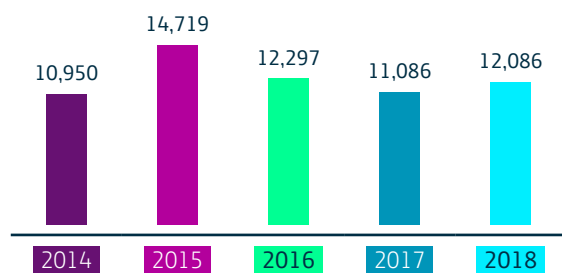


## Access to Metadata (cont.)

nature, in accordance with Law 734 of 2002 (Single Disciplinary Code):

- › 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 judicial authorisation.

### REQUESTS



Accesses affected	36,204	Requests rejected	120
-------------------	--------	-------------------	-----

## Blocking and filtering of certain contents

### Child sexual abuse material

#### Legal framework

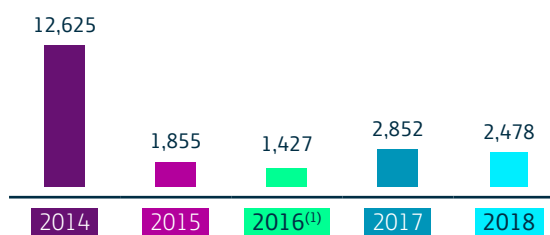
- › Law 679 of 2001: Articles 7 and 8
- › Decree 1524 of 2002: Articles 5 and 6
- › Law 1450 of 2011: Section 56.
- › Resolution CRC 3502 of 2011.

#### Competent Authorities:

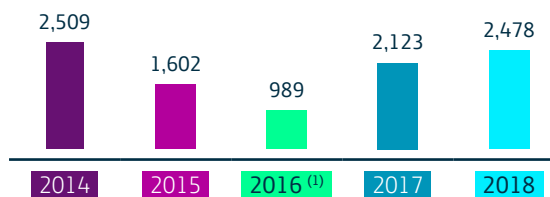
- › The National Police sends the Ministry of Information and Communication Technology a list of URLs with blocking orders so that the Ministry can publish it on

its website and so that it can be viewed by the PSIs (Internal Service Portal). To access this list, the PSIs must have a username and a password which are previously provided by the Ministry, so as to prevent anyone from browsing URLs with a blocking order for containing child sexual abuse.

### Nº OF NEW URLS\*



### Nº OF INCREMENTAL URLS\*\*



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

\*\* Number of URLs which increased throughout the year. These data, in turn, exclude the URLs which were eliminated from the list during the year.

(1) Since September of 2016 the platform "WOLF Content Control" came into operation, which specialises in filtering all illegal content typified by local authorities as 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 Technologies.

URLs affected	2,478	Requests rejected	0
---------------	-------	-------------------	---

## Illegal Games

#### Legal framework

- › Law 1753 of 2015: Article 93, paragraph 3.
- › Law 1450 of 2011: Article 56.
- › Resolution CRC 3502 of 2011.

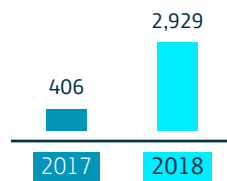
## Blocking and filtering of certain contents (cont.)

### Illegal Games (cont.)

#### Authorities

- » Coljuegos, an industrial and commercial company of the State in charge of the administration of the rental monopoly of games of chance, together with the National Police identify Web portals in which unauthorized games of chance/gambling are commercialized and request the Ministry of Information Technologies and Communications to communicate to the ISPs the list of URLs that they must block.

#### Nº URLs



### Court Order

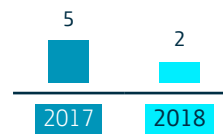
#### Legal framework

- » Law 1273 of 2009: Article 269F.
- » Law 1340 of 2009: Article 18.
- » Law 1450 of 2011: Article 56.
- » Resolution CRC 3502 of 2011.

#### Competent Authorities:

- » The General prosecutor of the Nation and the Superintendence of Industry and Commerce within the investigations they are carrying out request the Ministry of Information Technology and Communications to communicate to the ISPs the URLs they must block.

#### Nº URLs



URLs affected	2,931	Requests rejected	Not available <sup>(1)</sup>
---------------	-------	-------------------	------------------------------

(1) Because of the blocking system established by the law.

## Geographical and temporary suspension of the service

### Legal framework

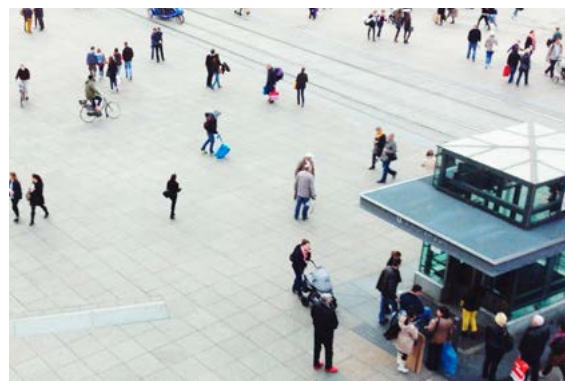
- » Law 1341 of 2009, Art. 8. Cases of emergency, unrest, disaster and prevention.

#### Competent Authorities

- » Priority will be given to the authorities in the transmission of free and timely communications for the purpose of the prevention of disasters, when these are considered essential.

#### REQUESTS

0	0	0	0	0
2014	2015	2016	2017	2018
Accesses affected	0	Requests rejected	0	



# Costa Rica

www.movistar.cr



Telefónica began operating mobile telephony services in Costa Rica in November 2011.

Telefónica Costa Rica managed more than 2.1 million accesses at the end of December 2018.

In terms of financial figures, Telefónica's revenues in Costa Rica reached 211.68 million euros and the OIBDA reached 49.67 million euros.

2,195.8

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

38.1	2,146.3	0.8	10.6
Fixed telephony	Mobile telephony	Broadband	Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

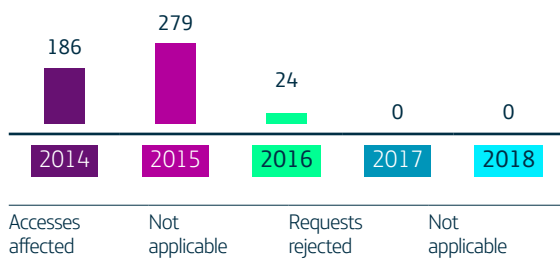
### Legal framework

- » Law Against Organised Crime, Art. 14 y 15.

### Competent Authorities

- » The judges of the Judicial Authorities.
- » Since the creation of the Judicial Centre for the Intervention of Communications (CJIC), the interventions are performed directly by the CJIC judges from the CJIC.

#### REQUESTS



## Access to Metadata

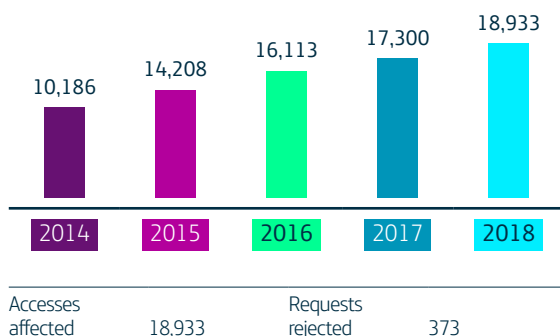
### Legal framework

- » Criminal Procedure Code. Art. 198
- » Jurisprudence of the Constitutional Chamber which guarantees the power of judges, public prosecutors and the police to request metadata associated with communications.

### Competent Authorities

- » Judges, public prosecutors and the judicial police.

#### REQUESTS



## Blocking and filtering of certain contents

### Legal framework

There are no laws in the regulatory framework that allow the blocking or filtering of content.

Competent Authorities: Not applicable.

#### REQUESTS

Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2014	2015	2016	2017	2018
URLs affected	Not applicable	Requests rejected	Not applicable	

## Geographical and temporary suspension of the service

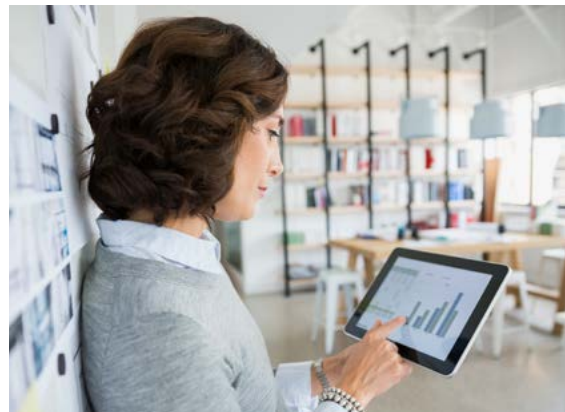
### Legal framework

There are no laws in the regulatory framework that allow the geographical and temporary suspension of the service.

Competent Authorities: Not applicable.

#### REQUESTS

Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2014	2015	2016	2017	2018
Accesses affected	Not applicable	Requests rejected	Not applicable	



# Ecuador

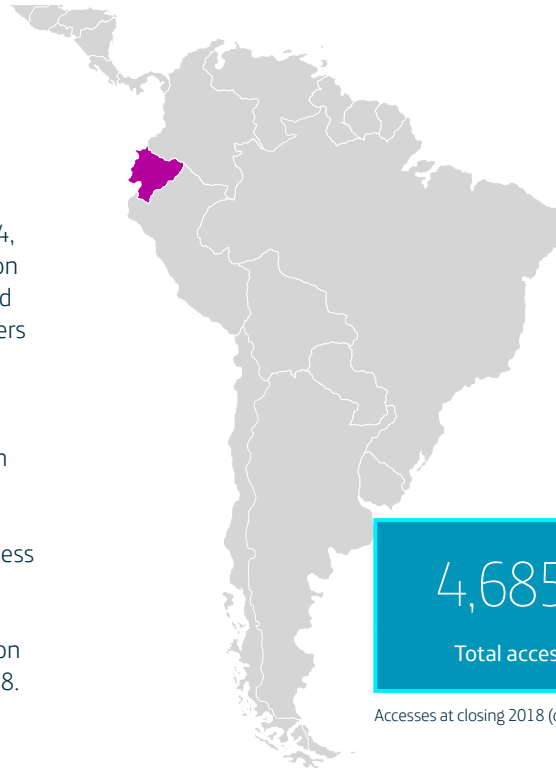
www.telefonica.com.ec

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%).

The company operates in the 24 provinces of the country and communicates to more than 5 million Ecuadorians with mobile services.

Telefónica manages more than 4.6 millones accesess in Telefonica Ecuador at December 2018.

Telefónica's revenue in Ecuador stood at 542 million euros and the OIBDA was 143 million euros in 2018.



4,685.5

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

27.7	4,626.9	30.9	0.0
Fixed telephony	Mobile telephony	Broadband	Pay TV

Accesses at closing 2018 (data in thousands).





## Lawful interceptions

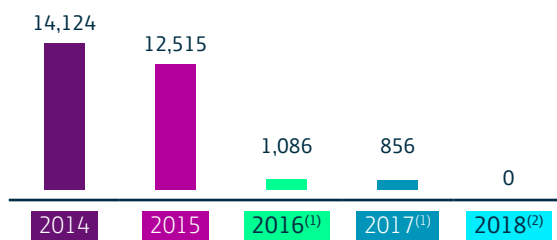
### Legal framework

- » Integral Organic Criminal Code, Articles 476-477.
- » 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 now the prosecution responds directly to requests for intervention and data in criminal matters. Telefónica now only receives them in civil matters.

(2) The Ecuadorian State through the Attorney General's Office ordered that this type of process be carried out without the intervention of the operator from 2018 onwards. That is, the Prosecutor's Office is the only entity authorized to perform this type of interception in real time.

Accesses affected	0	Requests rejected	0
-------------------	---	-------------------	---

## Access to Metadata

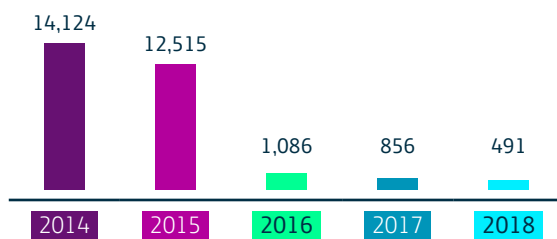
### Legal framework

- » Integral Organic Criminal Code. Section 499.

### Competent Authorities

- » Judges of Criminal Guarantees.

#### REQUESTS



Accesses affected	491	Requests rejected	0
-------------------	-----	-------------------	---

## Blocking and filtering of certain contents

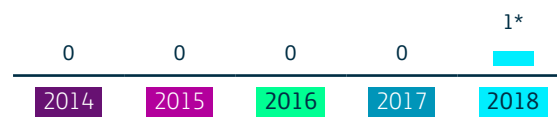
### Legal framework

- » Integral Organic Criminal Code. Article 583.
- » Organic Code of the Social Economy of Knowledge, Art. 563 and 565.

### Competent Authorities:

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

#### REQUESTS



\* For violating intellectual property rights.

URLs affected	1	Requests rejected	0
---------------	---	-------------------	---

## Geographical and temporary suspension of the service

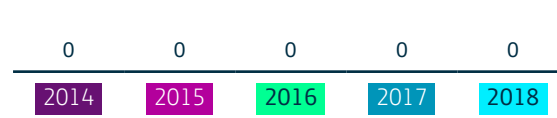
### Legal framework

- » Constitution of Ecuador. Articles 164 and 165.

### Competent Authorities

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

#### REQUESTS



Accesses affected	0	Requests rejected	0
-------------------	---	-------------------	---

# El Salvador

[www.telefonica.com.sv](http://www.telefonica.com.sv)



Telefónica entered the Salvadoran market in 1998 with mobile operations.

Telefónica El Salvador managed more than 2 million accesses as of December 2018.

In terms of financial figures, Telefónica's revenues in El Salvador reached 129 million euros and the OIBDA was 33 million euros.

2,069.1

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

167.7

Fixed telephony

1,890.3

Mobile telephony

3

Broadband

8.1

Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

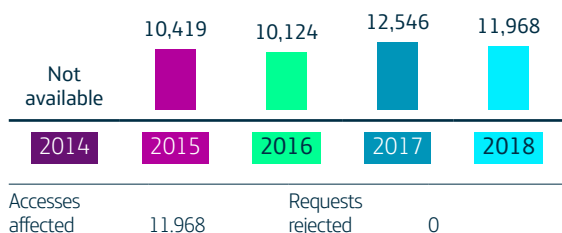
### Legal framework

- » Special Law for the intervention of communications, Art. 13.
- » Political Constitution of the Republic of El Salvador, Art. 24.

### Competent Authorities

- » The Public Prosecutor's Office of the Republic has a Centre for the Intervention of Calls, connected to all the operators providing telephony services in El Salvador, and therefore, within the framework of the investigation of a crime and by virtue of the order of a judge (as established in the Law on Interventions), it is possible for the Public Prosecutor to perform this type of action, but Telefónica is not authorised to do so.

#### REQUESTS



## Access to Metadata

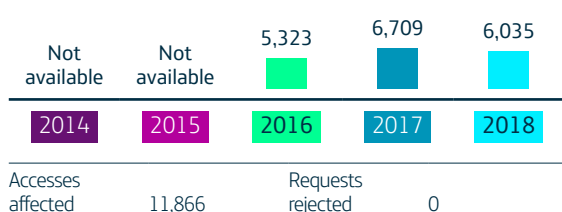
### Legal framework

- » Special Law for the intervention of communications, Art. 43 y 47.

### Competent Authorities

- » The Public Prosecutor's Office of the Republic and the Judges, within the framework of the investigation of a crime.

#### REQUESTS



## Blocking and filtering of certain contents

### Legal framework:

There are no laws in the regulatory framework that allow the blocking or filtering of content.

Competent Authorities: Not applicable.

#### REQUESTS

Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2014	2015	2016	2017	2018
URLs affected	Not applicable	Requests rejected	Not applicable	

## Geographical and temporary suspension of the service

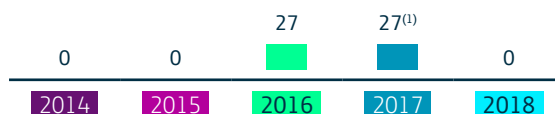
### Legal framework

- » Special Law Against the Crime of Extortion, Art.13-14.
- » Criminal Procedure Code, Art.238.
- » Telecommunications Law, Art. 30-31.

### Competent Authorities

- » The Public Prosecutor's Office of the Republic in the event of the suspension of specific services.
- » Regarding prisons, since operators are obliged to do so, there is no need for a request; however, if new prisons are created or existing ones are relocated, it is the Ministry of Justice and Public Security that will request the blockade of the geographical area.

#### REQUESTS\*



(1) Number of affected areas. With the application of the Special Law Against the Crime of Extortion, operators were forced to block all traffic generated from the penal centers, under penalty of fines and even revocation of the concession to operate.

Accesses affected	0	Requests rejected	0
-------------------	---	-------------------	---

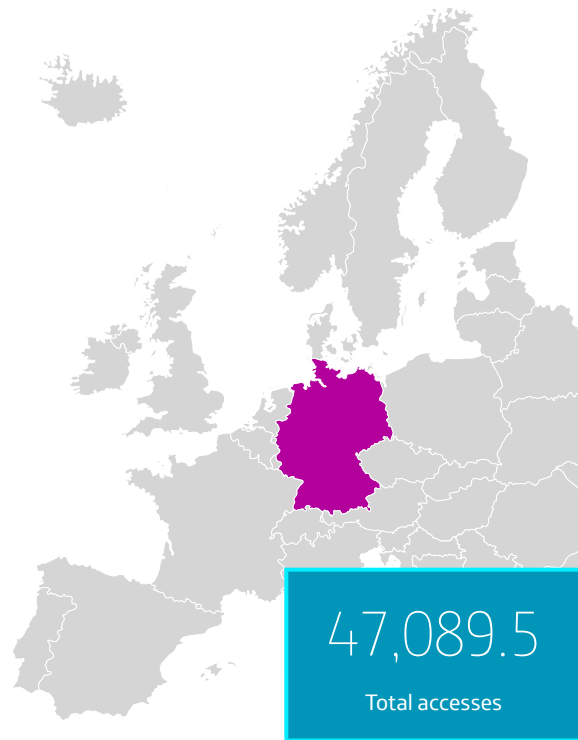
# Germany

www.telefonica.de

Telefónica has been in the country for almost 16 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 DSL fixed network telephony and high-speed Internet. Telefónica manage 47.1 million accesses in Germany.

Telefónica's revenue in Germany reached € 7.320 million and OIBDA was 1,834 million euros.



Accesses at closing 2018 (data in thousands).

## Accesses

1,996.0	42,818.8	2,274.7	0.0
Fixed telephony	Mobile telephony	Broadband	Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

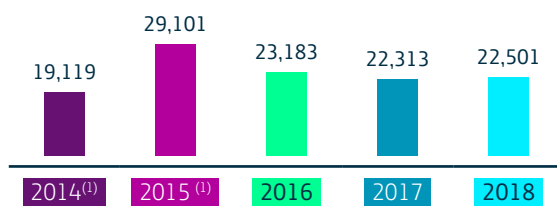
### Legal framework

- » Sec. 110 German Telecommunication Act (*Telekommunikationsgesetz* - TKG).
- » StPO. The German Code of Criminal Procedure.
- » Sec. 100a, 100b German Code of Criminal Procedure (*Strafprozessordnung* - StPO).
- » Article 10 Act (*Artikel 10 Gesetz* - GlO).
- » Customs Investigation Services Law (ZFDG).
- » 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\*



\* The total volume does not include prolonged interventions.

Accesses affected	30,026	Requests rejected	0
-------------------	--------	-------------------	---

## Access to Metadata

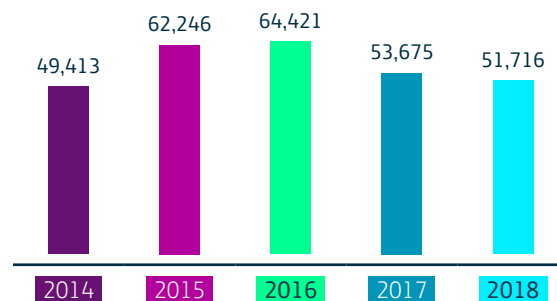
### Legal framework

- » Sec. 96, 113b German Telecommunication Act (*Telekommunikationsgesetz* - TKG).
- » 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. 100g 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



Accesses affected	442,168	Requests rejected	0
-------------------	---------	-------------------	---

## Blocking and filtering of certain contents

### Legal framework:

No existing legal basis in German legal/ regulatory framework or other sources which allows content blocking and filtering.

Competent Authorities: Not applicable.

### REQUESTS

Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2014	2015	2016	2017	2018
URLs affected	Not applicable	Requests rejected	Not applicable	

## Geographical and temporary suspension of the service

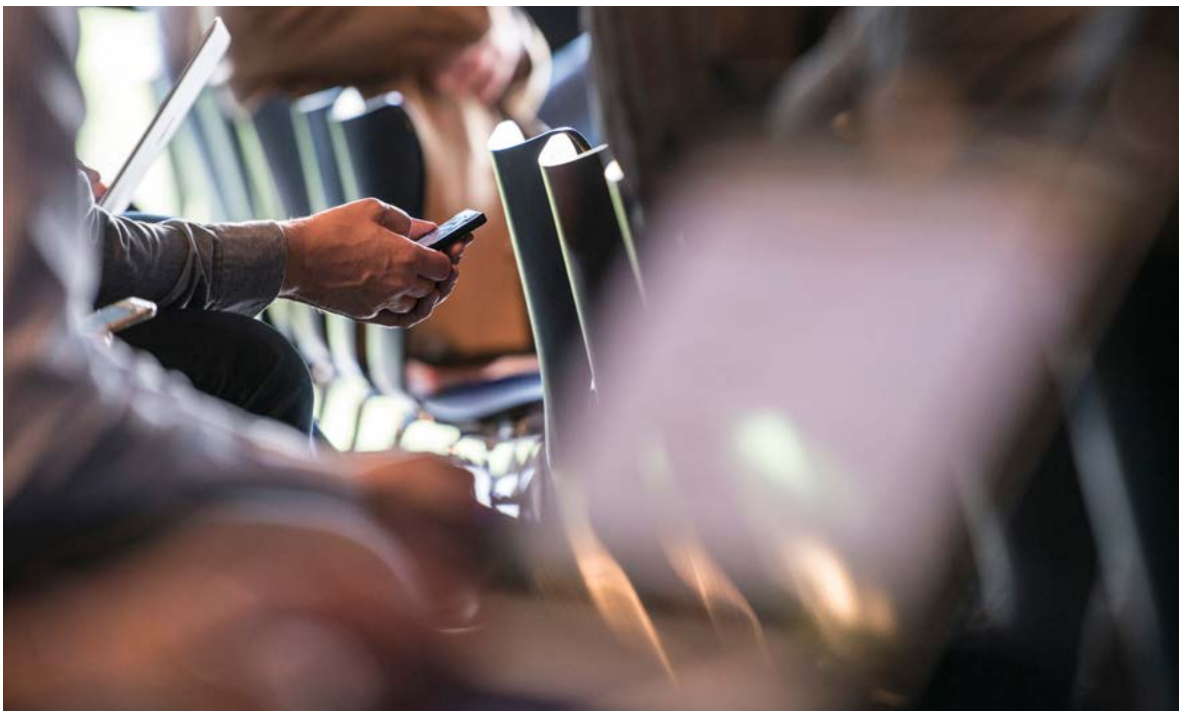
### Legal framework:

No existing legal basis in German legal/regulatory framework or other sources which allows geographical or temporary suspension of services.

Competent Authorities: Not applicable.

### REQUESTS

Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2014	2015	2016	2017	2018
Accesses affected	Not applicable	Requests rejected	Not applicable	





# Mexico

[www.telefonica.com.mx](http://www.telefonica.com.mx)

Telefónica Mexico has participated and competed in the mobile telecommunications market since 2001 and promotes the development of telecommunications in the country.

The commercial offers are available in 231 Customer Service Centers (CAC), 36 Movistar Stores as well as in 26 nationwide Smart Stores, 3 Movistar Experience Centers and more than 7 thousand indirect points of sale throughout the country.

Telefónica in Mexico manages more than 27 million accesses in December 2018.

With regard to the financial figures, in 2018 Telefónica's revenue in Mexico stood at 1,175 million euros and the OIBDA was 150 million euros.

27,013

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

0.0	26,309.9	709.1	0.0
Fixed telephony	Mobile telephony	Broadband	Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

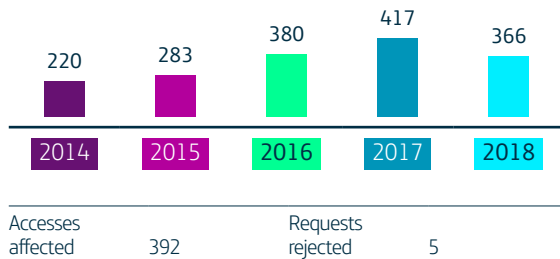
### Legal framework

- » Political Constitution of the United States Mexican, 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 the intervention of communications is appropriate, ordering the concession holder to establish the measure for a certain period of time.

### REQUESTS



## Access to Metadata

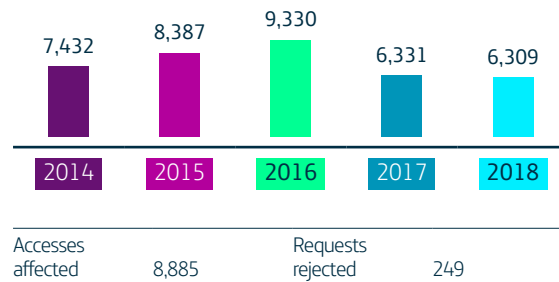
### Legal framework

- » 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



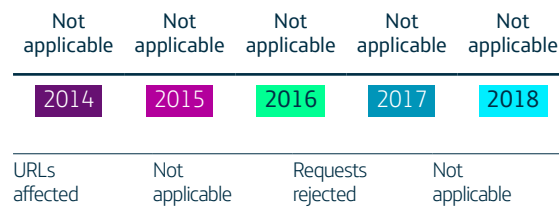
## Blocking and filtering of certain contents

### Legal framework:

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

Competent Authorities: Not applicable.

### REQUESTS



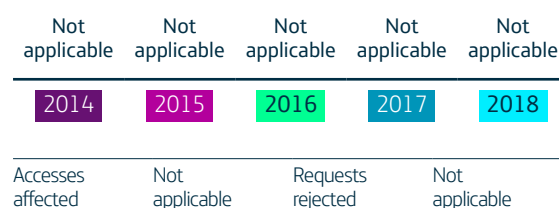
## Geographical and temporary suspension of the service

### Legal framework:

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

Competent Authorities: Not applicable.

### REQUESTS



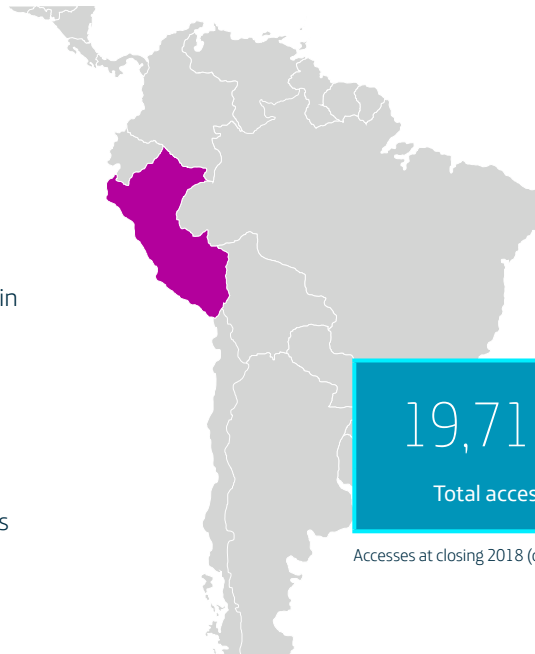
# Peru

[www.telefonica.com.pe](http://www.telefonica.com.pe)

Telefónica began to operate in the Peruvian market in the middle of the 1990s.

The company managed more than 19.7 million accesses at the end of third quarter 2018.

Regarding financial figures, Telefónica's revenue in Peru stood at 2.075 million euros and the OIBDA was 350 million euros.



19,711.7

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

2,545.4

Fixed telephony

13,664.8

Mobile telephony

1,973.3

Broadband

1,528.1

Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

### Legal framework

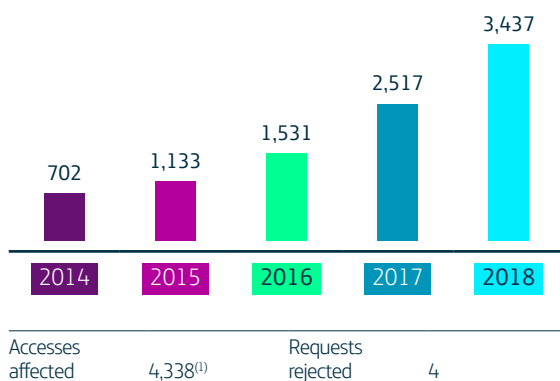
- » Political Constitution of Peru, Art. 2, paragraph 10.
- » Telecommunications Law (Supreme Decree No. 013-93-TCC - Article 4) and its Regulations (Supreme Decree No. 0202007- MTC - Article 13).
- » Law No. 27697: Law which grants power to the public prosecutor for the intervention and control of communications and private documents, in exceptional cases.
- » Legislative Decree No. 1182.

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.
- » National Police Force of Peru, which must require judicial validation within 24 hours.

### REQUESTS



(1) Lines effectively intervened.

## Access to Metadata

### Legal framework

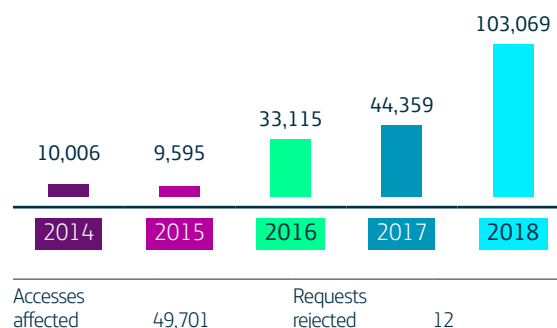
- » Political Constitution of Peru, Art. 2, paragraph 10.
- » Telecommunications Law (Supreme Decree No. 013-93-TCC - Article 4) and its Regulations (Supreme Decree No. 020- 2007MTC - Article 13).
- » Law No. 27697: Law which grants power to the public prosecutor for the intervention and control of communications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

- » Judges (Judicial Authority).
- » Public Prosecutor's Office of the Nation, Criminal Prosecutors and Public Prosecutors, with the authorisation of the Judge.
- » National Police Force of Peru, which must require judicial validation within 24 hours

### REQUESTS



## Blocking and filtering of certain contents

### Legal framework:

- » Copyright Law.

### Competent Authorities:

- » INDECOPI (National Institute for the Defense 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 Defense 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, to confiscate, to order the temporary or definitive closure of the establishments where the offence is committed.

For INDECOPI, to the extent that through the websites would be performing acts that violate the right of public communication of the denouncing companies, the administration can order the blocking of access in Peruvian territory to the offending website, through blocking based on DNS and blocking based on URL.

### REQUESTS

0	0	0	0	4 <sup>(1)</sup>
2014	2015	2016	2017	2018

(1) Requests of INDECOPI (Precautionary measures in intellectual property cases).

URLs affected	4	Requests rejected	0
---------------	---	-------------------	---

## Geographical and temporary suspension of the service

### Legal framework:

- » Regulation of the Telecommunications Law (S.D. No. 020-2007-MTC - Articles 18 and 19).
- » The concession contracts establish that, in the event of an emergency, crisis or a threat to national security, the concession holder will provide the telecommunication services prioritising actions to support the State and following the instructions of the MTC.

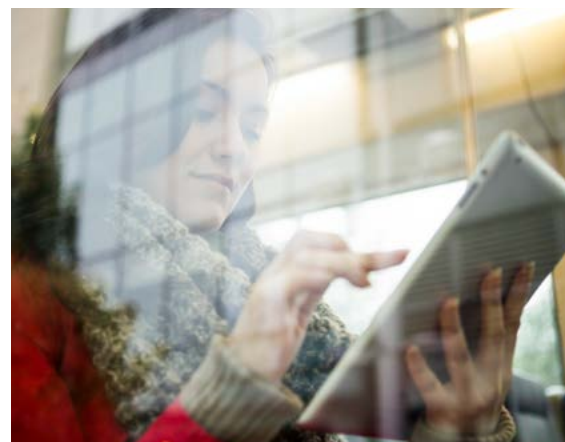
### Competent Authorities:

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

### REQUESTS

0	0	0	0	0
2014	2015	2016	2017	2018

Accesses affected	0	Requests rejected	0
-------------------	---	-------------------	---





# Spain

www.telefonica.com

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 services. Telefónica España is the biggest provider of telecommunication services in Spain for access, including voice, data, television and internet access. Additionally it is offering its clients the most innovative services and cutting edge technology to achieve its aim of becoming the first digital telco.

Telefónica España handled more than 41.5 million accesses at the end of December 2018.

Revenue from operations amounts to 12,706 millones de euros and its OIBDA reached 4,763 million euros in 2018.



Accesses at closing 2018 (data in thousands).

## Accesses

9,029.1	18,384.4	6,129.6	3,847.6
Fixed telephony	Mobile telephony	Broadband	Pay TV

Accesses at closing 2018 (data in thousands).





## Lawful interceptions

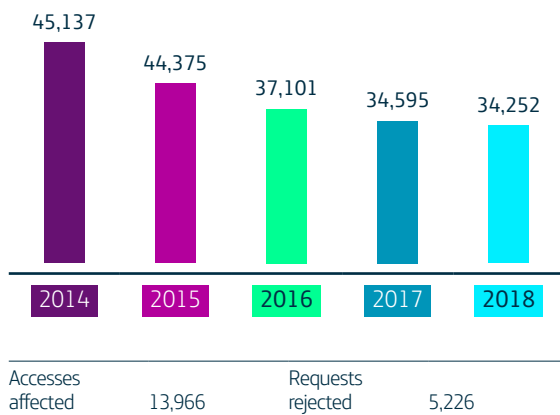
### Legal framework

- » Spanish Constitution, Art. 18.
- » Law of criminal prosecution, Art. 588.
- » General Law 9/2014 on Telecommunications, Articles 39-42.

### Competent Authorities

- » Judges of the 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.

### REQUESTS



## Access to Metadata

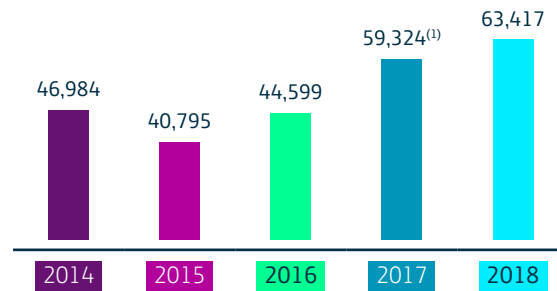
### Legal framework

- » Law 25/2007 on Data Conservation, Articles 1-10.
- » General Law 9/14 on Telecommunications, Articles 39-42.

### Competent Authorities

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

### REQUESTS



(1) In 2017, a new system of sending judicial orders by 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 agents, a single warrant could result in multiple data requests, even if it was counted as one.

Accesses affected	Not available <sup>(1)</sup>	Requests rejected	9,933
-------------------	------------------------------	-------------------	-------

(1) The nature of certain requests (in a request there may be requests to an indeterminate number of users) and the configuration of the communication tools with the authorities do not allow to provide this data..

## Blocking and filtering of certain contents

### Legal framework

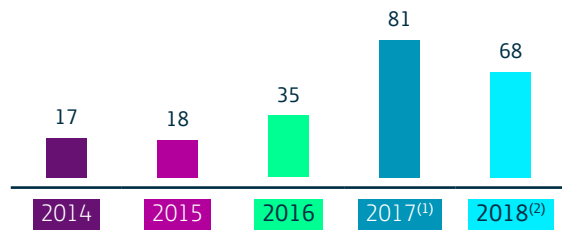
- » Royal Decree 1889/2011 of 30 December, regulating the functioning of the Intellectual Property Commission, Articles 22 and 23.
- » Revised Text of the Intellectual Property Law, approved by Royal Legislative Decree Law 1/1996 of 12 April, Article 138.
- » Law 34/2002 of 11 July on services of the information society and electronic commerce, Article 8.

### Competent Authorities

- » National Markets and Competition Commission.
- » Mercantile/Civil/Accounting Administrative/Criminal Courts.
- » National Intellectual Property Commission.
- » General Gambling Directorate.
- » Agency for Medicine/Doping/Health/Sport.

## Blocking and filtering of certain contents (cont.)

### REQUESTS\*



\* Telefonía España executes court orders and/or administrative orders which are in accordance with legal regulations, to block access to certain web resources.

### INTELLECTUAL PROPERTY

64 Requests	455 Blocks
----------------	---------------

### GAMES

3 Requests	1.356 Blocks
---------------	-----------------

### MEDICINE

1 Requests	1 Blocks
URLs affected 1,812	Requests rejected 0

## Geographical and 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

Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
2014	2015	2016	2017	2018
Accesses affected	Not applicable	Requests rejected	Not applicable	Not applicable



# United Kingdom

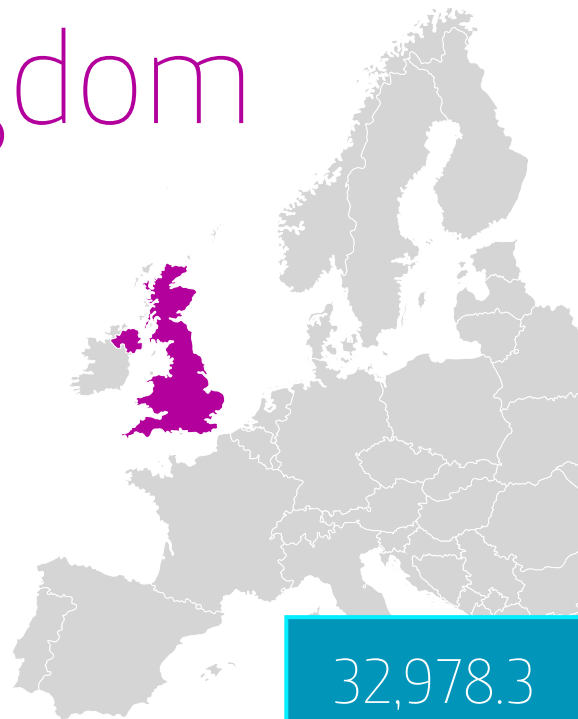
[www.o2.co.uk/](http://www.o2.co.uk/)

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

O2 runs 2G, 3G and 4G networks across the UK, as well as operating O2 Wifi, with over 6 million clients, and owning half of Tesco Mobile. O2 has over 450 retail stores.

The company managed more than 32 million accesses at the end of 2018 in the UK.

With regard to the financial figures, in 2018 Telefónica's revenue in UK stood at €6,790 million and OIBDA amounts up to €1,865 million.



32,978.3

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

306.9	25,044.1	28.1	0.0
Fixed telephony	Mobile telephony	Broadband	Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

### Legal framework

During 2018 the provisions for lawful intercept under the Regulation of Investigatory Powers Act 2000 (RIPA) and the Intelligence Services Act 1994 (ISA) were replaced by the Investigatory Powers Act 2016 (IPA). This process was completed by November 2018. The Investigatory Powers Commissioner (IPC) is now fully established and the Investigatory Powers Commission's Office (IPCO) has replaced the Interception of Communications Commissioner's Office (IOCCO). IPCO is overseeing implementation and compliance with the lawful intercept requests made pursuant to the IPA.

### Competent Authorities

The principles of RIPA have been continued under the IPA but with additional oversight by the judiciary. 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 crime 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 Defense 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 get 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 authorized by the warrant is proportionate to what is sought to be achieved by that interception.

As of November 2018 all requests for lawful intercept have been pursuant to the IPA, and in addition to the authorisation by the Secretary of State (or their deputy) that was required by RIPA, there must also be approval of the warrant by 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\*

Not available	Not available	Not available	Not available	Not available
2014	2015	2016	2017	2018

\* Section 57 of the IPA prohibits the disclosure of the existence of any lawful intercept warrant save for in excepted 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.



More information in [www.ipco.org.uk/docs/IPCO%20Annual%20Report%202017%20Web%20Accessible%20Version%2020190321.pdf](http://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202017%20Web%20Accessible%20Version%2020190321.pdf)

Accesses affected	Not applicable	Requests rejected	Not applicable
-------------------	----------------	-------------------	----------------

## 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) are due to be 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

#### RIPA regime

- » Under S.22 (4) of RIPA a notice may be issued by a person holding a prescribed office, rank or position within a relevant public authority designated with the power to acquire communications data by order under S.25 (2) and under the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480). The persons that can issue a notice are typically senior police officers or other senior officials in relevant security services.
- » Under S.22 (3) of RIPA persons within a public authority may be given an authorisation to directly obtain the communications data in question in certain circumstances.

#### Future

- » Under S.61 of the IPA an authorisation to release data may be made by a designated senior officer in a relevant public authority. Similarly to RIPA, under the IPA the persons that may authorise release of data are typically senior police officers or other senior officials in relevant security services. These officials will, save for in urgent situations, be required to obtain pre-authorisation from the Office of Communications Data Authorisations, which will make an independent decision on whether to grant or refuse communications data requests.

### REQUESTS\*

Not available	Not available	Not available	Not available	Not available
2014	2015	2016	2017	2018

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

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

Accesses affected	Not applicable	Requests rejected	Not applicable
-------------------	----------------	-------------------	----------------

## Blocking and filtering of certain contents

### Legal framework:

- » Section 97A of the Copyright Designs and Patents Act (1988).
- » S.37 (1) Supreme 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 between the CSPs and the law enforcement community to prevent child exploitation. This is a voluntary code of practice and 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. Legal adult sites are considered legal content (unlike IWF sites which are child abuse sites).



More information, in the code of practice:  
[www.mobilebroadbandgroup.com/documents/mbg\\_content\\_code\\_v2\\_100609.pdf](http://www.mobilebroadbandgroup.com/documents/mbg_content_code_v2_100609.pdf)



## Blocking and filtering of certain contents (*cont.*)

### Competent Authorities:

- » Internet Watch Foundation.
- » Courts.

### REQUESTS\*

Not available	Not available	Not available	Not available	Not available
2014	2015	2016	2017	2018

\* Only IWF, no stats available.

URLs affected	Not applicable	Requests rejected	Not applicable
---------------	----------------	-------------------	----------------

## Geographical and 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

0	0	0	0	0
2014	2015	2016	2017	2018
Accesses affected	Not applicable	Requests rejected	Not applicable	



# Uruguay

www.movistar.com.uy

Telefónica has been present in Uruguay since 2005. Besides digital solutions it mainly offers mobile telephony to its customers.

In 2018, Telefónica's revenue in Uruguay reached 221 million euros and the OIBDA was 82 million euros.



## Accesses

1,676.1

Total accesses

0.0

Fixed telephony

1,676.1

Mobile telephony

0.0

Broadband

0.0

Pay TV

Accesses at closing 2018 (data in thousands).



## Lawful interceptions

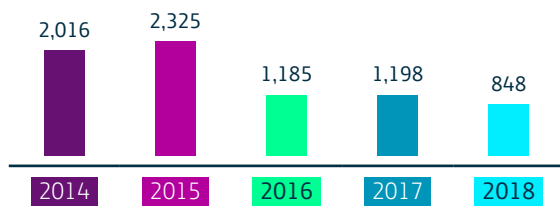
### Legal framework

- » Constitution of the Republic, Article 28
- » Law 18,494, Article 5.
- » Reserved decree of 13 March 2014.

### Competent Authorities

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

#### REQUESTS



Accesses affected	561	Requests rejected	67
-------------------	-----	-------------------	----

## Access to Metadata

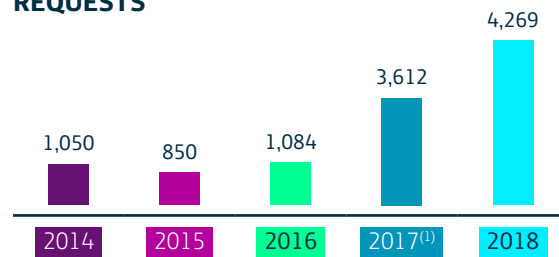
### Legal framework

- » Constitution of the Republic, Article 28
- » Law 18,494, Article 5.
- » Reserved decree of 13 March 2014.

### Competent Authorities

- » Judges, by means of a written and wellfounded request.

#### REQUESTS



(1) The increase in comparison to 2016 is due to the fact that from 2017 onwards a tool has been used that allows the accounting of every access affected. 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.

Accesses affected	4,269	Requests rejected	93
-------------------	-------	-------------------	----



## Blocking and filtering of certain contents

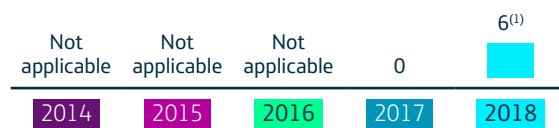
### Legal framework:

- » Law 19.535 of 25 September 2017, Articles 244 y 245.
- » Decree 366/2017 of 21 December 2017 developed according on Art.244 and 245 of law 19.535.

### 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



(1) Games and sports betting online.

URLs affected	147	Requests rejected	1
---------------	-----	-------------------	---

## Geographical and temporary suspension of the service

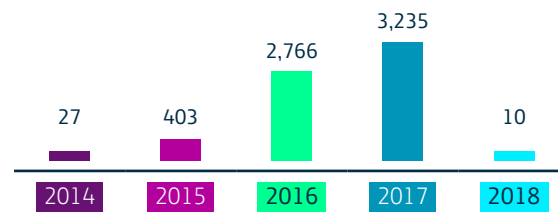
### Legal framework:

- » Law 19,355, Article 166: 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 3 communications in the month or 6 in the year).

### Competent Authorities:

- » Ministry of the Interior (Executive Power).

### REQUESTS\*



\* Temporary and individual suspension of 911 emergency services for periods of between 3 and 6 months.

Accesses affected	1,189	Requests rejected	0
-------------------	-------	-------------------	---





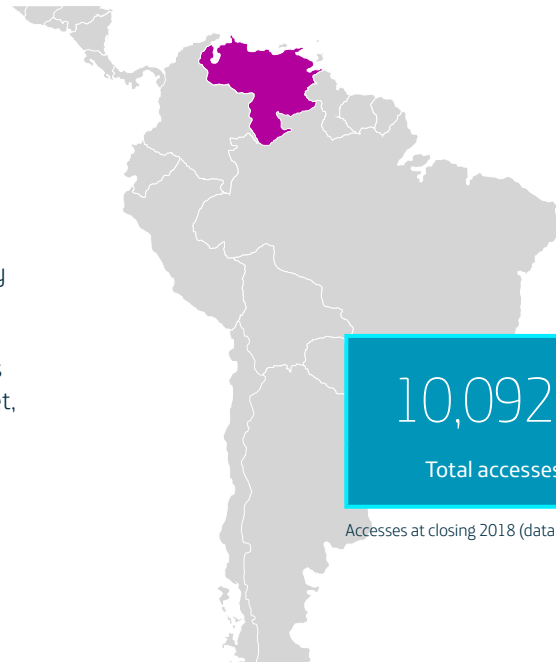
# Venezuela

www.telefonica.com.ve

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

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

In 2018, Telefónica's income in Venezuela was 18 million euros and the OIBDA stood at 3 million euros.



10,092.3

Total accesses

Accesses at closing 2018 (data in thousands).

## Accesses

423.2	9,235.5	7.2	426.4
Fixed telephony	Mobile telephony	Broadband	Pay TV

Accesses at closing 2018 (data in thousands).





## Lawful interceptions

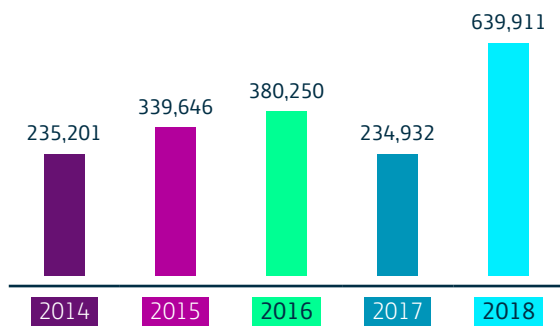
### Legal framework

- » 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 Research Agency Criminal and investigations (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 organs and bodies.

### REQUESTS



Accesses affected	1,091,668	Requests rejected	11,367
-------------------	-----------	-------------------	--------

## Access to Metadata

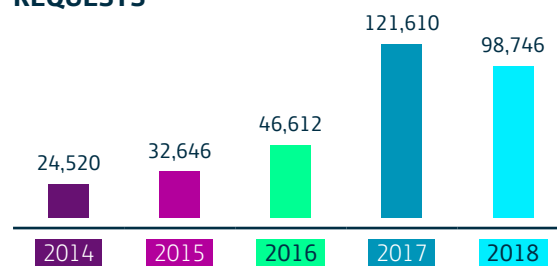
### Legal framework

- » Administrative Ruling No. 171. Rules Concerning the Collection or Capture of Personal Data from Applicants for Mobile and Fixed Telephony Services via Wireless Networks or Non-Geographic Number with Nomadic Voice Service.
- » Law against Kidnapping and Extortion, Article 29.

### Competent Authorities

- » The Public Prosecutor's Office.
- » The Scientific Research Agency Criminal and investigations (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\*



Accesses affected	953,097	Requests rejected	1,978
-------------------	---------	-------------------	-------

## Blocking and filtering of certain contents

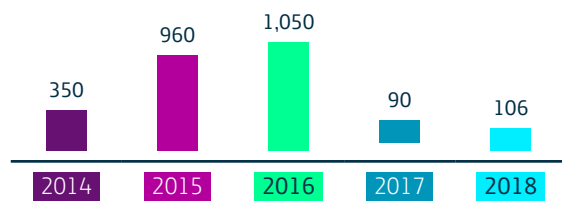
### Legal framework:

- » 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



URLs affected	106	Requests rejected	19
---------------	-----	-------------------	----

## Geographical and temporary suspension of the service

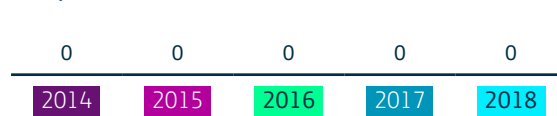
### Legal framework:

- » Organic Law on Telecommunications, Article 5.

### Competent Authorities:

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

#### REQUESTS



Accesses affected	0	Requests rejected	0
-------------------	---	-------------------	---





# Glossary

Competent authority

Personal data

Location data

Traffic data

DPI

IMEI

IMSI

IOCCO

MAJOR EVENTS

PSI

SUTEL

TELCOR

URL





# 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.

### 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.



## CONCEPT



## EXPLANATION

### 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 (e.g. bbc. co.uk), the opposition party's websites prior to elections, human rights groups' websites, etc.).
- » 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 shutdownNot applicableaccess 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 organization, to find all the information on internal procedures on a website with high levels of security.

### SUTEL

The SUTEL is a maximum deconcentration body in Costa Rica, attached to Aresep, the Public Services Regulatory Authority, created by virtue of Law 8,660, published on 13 August 2008. SUTEL is responsible for applying the regulation to the telecommunications sector and ensuring efficiency, equality, continuity, quality, greater and better coverage and information, as well as better alternatives for the provision of telecommunications services.

### TELCOR

TELCOR, the Nicaraguan Institute for Telecommunications and Postal Services, is the Regulatory Body of Telecommunications and Postal Services, a state institution whose functions include the regulation, standardizing, technical planning, supervision, application and control of the fulfilment of the Laws and Regulations which govern the installation, interconnection, operation and provision of Telecommunications and Postal Services.

### 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.



*Telefonica*

---