Telefónica

Report on **Transparency** in Communications **2019**

CONTENTS

Introduction and Scope of the Report

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

Respect for and promotion of human rights, particularly privacy and freedom of expression, take on a new dimension in a digital world characterized by the use of new technologies, Artificial Intelligence and a growing importance of data on a global scale.

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

Transparency is key in this context, even more so in a world in which spaces of responsibility are shared when it comes to preserving and guaranteeing the rights of individuals.

As part of this exercise in transparency, our report elaborates on:

i. our governance regarding human rights in general and privacy and freedom of expression in particular;

ii. our human rights due diligence;

iii. commitments, policies and processes we follow when responding to requests from Competent Authorities;

iv. information on the legal context that provides the Competent Authorities with the legal basis to make these kinds of requests[1];

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

vi. the total number of requests we received last year in each of the countries we operate in, unless we are prohibited from publishing this information so or unless a government or any other public entity already discloses said information;

vii. and, in addition, whenever technically possible, we report the number of requests that we reject, the accesses that are affected by each indicator and the URLs and/or IPs affected in the event of any blocking or content restrictions.

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

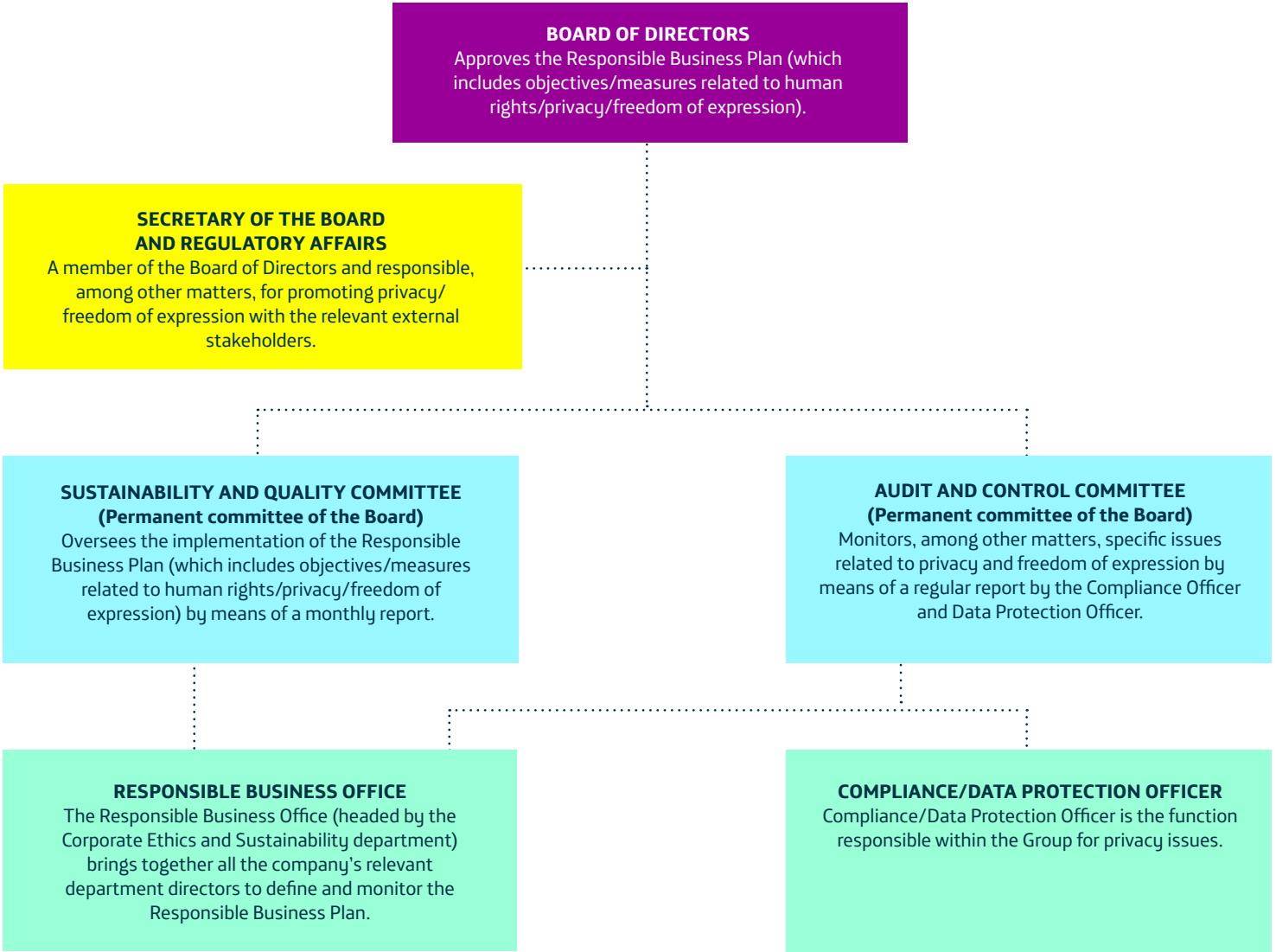
Our Governance

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

Our human rights activities are defined and implemented by means of the Responsible Business Plan, which sets out the company's sustainability strategy and objectives and is directly approved and monitored by the Board of Directors and its Sustainability and Quality Committee (one of the Board's permanent committees).

Our Human Rights Policy and our due diligence process, which are based, amongst others, on the UN Guiding Principles on Business and Human Rights and the Principles of the GNI (Global Network Initiative), form an integral part of the Responsible Business Plan.

This governance model, headed by the Board of Directors and the Responsible Business Office and involving all the relevant departments, seeks to ensure that our commitment to human rights is incorporated into all activities and levels of the company.



In addition, the DPO (Data Protection Officer) 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 (one of the Board's permanent committees). The DPO coordinates the 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.

Lastly, the General and Regulatory Affairs Secretary is a member of the Board of Directors and is responsible, among other matters, for promoting privacy and freedom of expression with relevant external stakeholders. In this function, he also led the publication and dissemination of Telefónica´s "Digital 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.

What is more, we have a Transparency Committee for privacy and freedom of expression issues related to requests made by Competent Authorities, which is composed by the Legal Department, Compliance, Internal Audit and Corporate Ethics and Sustainability. The Transparency Committee analyses the reported data in this report and may make such observations as they deem relevant, both in general terms or specifically regarding data reported by the business units. The objective is to ensure at all times the quality of the data as evidence of complying with current legislation and the protection of fundamental rights of individuals.

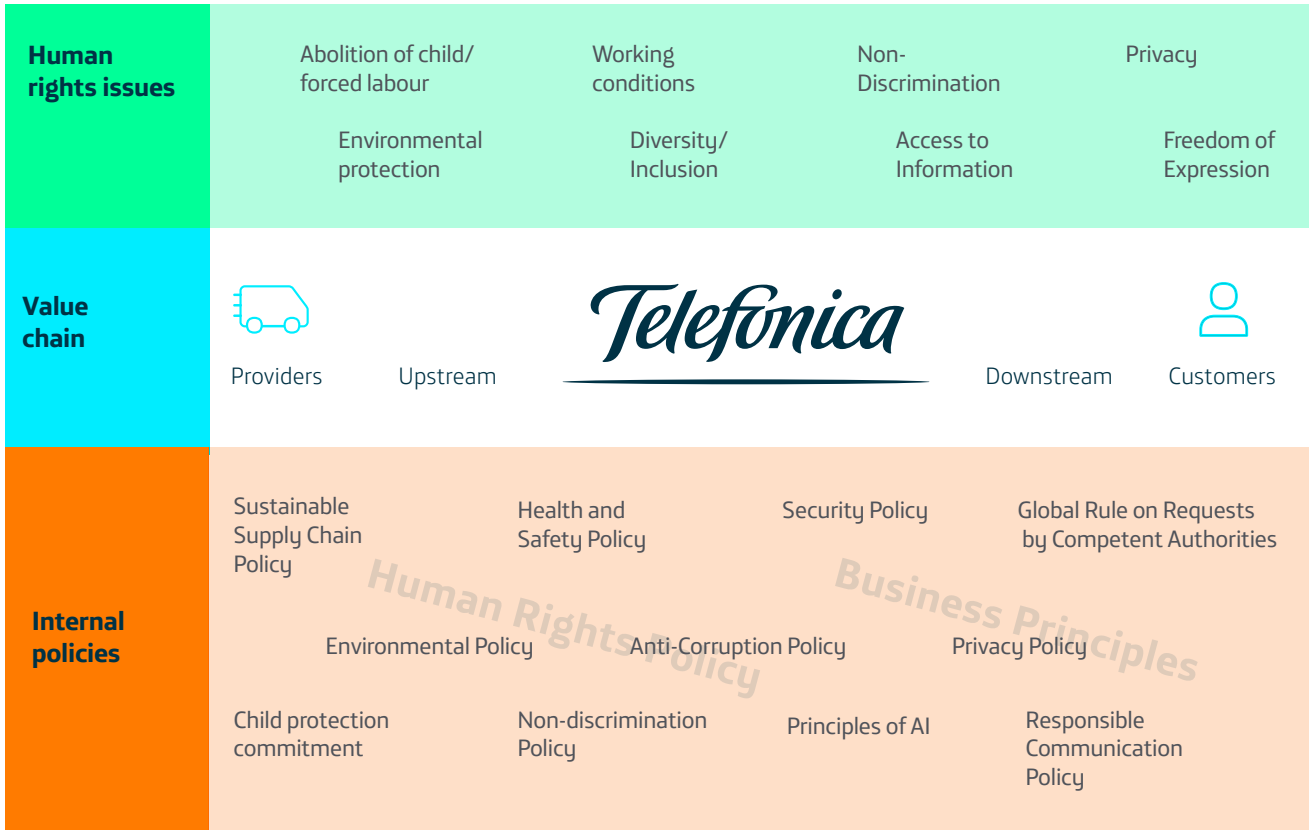
Those requests, which due to their characteristics and exceptional nature so require, are analysed by the heads of the respective business units by means of the appropriate weighting of all the interests potentially involved, including human rights, fundamental freedoms and any other interests that may be applicable 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.

The procedure established in the Global Crisis Management System is applied in the event of a crisis. Its taxonomy of critical incidents that could lead to a crisis lists, amongst others, requests from authorities which may have an impact on freedom of expression and privacy and/or legislations with a potentially high negative impact on human rights (freedom of expression, etc.). The Global Crisis Management System stipulates that, in the event of a crisis related to privacy and/or freedom of expression issues, the Chair of the Crisis Committee may convene the so-called "Human Rights Round Table" (made up of the relevant departments) in order to analyse the situation, design and apply a response strategy, report to the Executive Committee and conduct further analysis in order to prevent such risks in the future.

Our Human Rights Due Diligence

Since 2006 human rights have been an integral part of our Business Principles. The UN Guiding Principles on Business and Human Rights have served as a fundamental guide to promote the guarantee of and respect for people´s fundamental rights and, specifically, with regard to privacy and freedom of expression.

In line with our Global Human Rights Policy, we have a human rights due diligence process in place to identify, prevent, mitigate and remedy (potential and actual) human rights impacts. An integral part of our human rights due diligence process involves human rights impact assessments; these are conducted every four years at global level with the help of external human rights expert organisations and in close consultation with our stakeholders. The objective of these global impact assessments is to find out how our activities/business relationships and products/services impact on all existing human rights (see human rights issues analyzed in impact assessments in figure to the right) and, on this basis, identify the human rights issues that are most salient to our business activity. Additional, specific assessments are carried out on any significant issue for which the impact assessment identifies special concern.



In addition, local human rights impact assessments are conducted in the markets in which we operate to integrate the local context into the overall assessment. We also have a complaint and remedy mechanism, our Responsible Business Channel, which allows stakeholders to confidentially and anonymously make complaints and queries (in several languages) concerning any aspect related to the Business Principles and human rights in general as well as privacy and/or freedom of expression in particular. We have a procedure in place that guarantees the proper management of the Channel.

In 2013, in coordination with BSR (Business for Social Responsibility), we conducted our first impact assessment across all our operations and published our first public commitment to human rights. Privacy and freedom of expression were identified as two relevant issues in this first impact assessment to be managed from a human rights perspective. In 2019, we updated our impact matrix with a new assessment by BHR (Business & Human Rights) in order to understand the potential impacts of our Group´s new strategy and activities in an ever-changing digital environment. The rights to privacy and freedom of expression were again identified as significant (view our website on human rights for further information on the latest global impact assessment). Once the analysis was concluded, several activities and topics were identified as deserving specific evaluations, such as the impact assessments on the network deployment process, the development of new products and services (including those in which Artificial Intelligence is applied) and the rights of children.

All the aforementioned activities regarding impact assessments form the basis for adapting our internal policies and processes with a view to preventing, mitigating and/or remedying potential impacts on human rights in general and, in particular, privacy and freedom of expression. Below we highlight the most important internal policies and processes with regard to privacy and freedom of expression that have been adapted as a result of the latest impact assessments.

Applicable Policies and Processes

We have designed and updated different policies and procedures in order to ensure the protection of the rights of privacy and freedom of expression, access to information and non-discrimination.

Global Human Rights Policy:
Approved in 2019, this policy formalises our commitment to human rights included in a general manner in Telefónica's Business Principles and elaborates in greater detail on a set of policies and processes that seek to ensure the respect for and the application of internationally recognised social, economic and cultural human rights.

Global Privacy Policy:
Updated in 2018, this policy forms part of Telefonica's strategy to design a digital experience based on trust.
Aware of the importance of deserving the trust of our customers and/or users and, generally speaking, of our stakeholders, this policy guarantees them control over and the value of their personal data when they are processed by Telefónica.

It stipulates 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.

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

Regulation on the Model of Governance of Data Protection:
The objective of this regulation is to address the most important aspects to be taken into account for the proper management and protection of personal data.

It establishes an 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:

- **DPO's 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 commitee:** 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.

Global 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 2019 and inspired by the principles of honesty and trust, this policy is guided by the relevant domestic and international standards and regulations and establishes the guiding principles in matters of security that are applicable to all the companies that form part of the Telefónica Group.

The security activities are governed by the following principles:

- **Legality:** Necessary compliance with domestic and international laws and regulations in matters of security.
- **Efficiency:** The anticipatory and preventive nature of any potential risk and/or threat is highlighted with the aim of anticipating and preventing any potential harmful effect and/or mitigating any damage that might be caused.
- **Co-responsibility:** The duty of users to preserve the security of the assets that Telefónica places at their disposal.
- **Cooperation and Coordination:** Cooperation and coordination between all the business units and employees are priorities for the achievement of the appropriate levels of efficiency.

As a result of this policy, several regulations were updated during 2019-2020 to ensure effective compliance with it (The Incident and Emergency Management Regulation, Security Risk Analysis Regulation, Network and Communications Security Regulation, Cybersecurity Regulation, Supply Chain Security Regulation and Security Governance Regulation, among others).

Responsible Communications Regulation:
Approved in October 2018, its aim is to establish guidelines for Telefónica´s actions with regard to our communication and content generation channels. It is based on the principles of legality, integrity and transparency, neutrality and protection of minors.

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. In our communication to customers and through advertising we prohibit certain conducts that are contrary to our Business Principles. Thus, in our messages and our sponsorships we do not tolerate any abuse of the consumer's good faith, violations of people's dignity, the promotion of alcohol, tobacco, drugs, eating disorders and terrorism, incitement to hatred, violence and discrimination or the commission of unlawful behaviour, nor any abuse of the child's naivety.

Artificial Intelligence Principles:
Approved by the Executive Committee in October 2018, we are committed to designing, developing and using Artificial Intelligence with integrity and transparency. Our 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.

During 2019 we have worked on implementing these principles across all our operations, focusing on three inter-related pillars:

- **Training for employees:** We conducted an online training course on Ethics and Artificial Intelligence for our employees, explaining (a) how Artificial Intelligence, if used inappropriately, can have a negative impact on human rights and (b) what steps should be taken in practice to address potential human rights risks associated with the use of Artificial Intelligence.
- **A self-assessment questionnaire** for the product managers who buy, develop and/or use Artificial Intelligence. For each of our Artificial Intelligence Principles specific questions are posed regarding the algorithm used, so that product managers can identify the associated risks and are given recommendations to manage them.
- **Governance:** We have a governance model aimed at effectively implementing our Artificial Intelligence Principles.

Human rights training:
In late 2019 we began working on specific human rights trainings, which will continue throughout 2020 by integrating a deep dive on human rights in the mandatory training course on our Business Principles and conducting specific workshops for those employees whose work may have an impact on human rights. The areas in which these workshops will be conducted are:

- **Legal and Compliance:** To promote and respect privacy and freedom of expression in the context of requests made by Competent Authorities (on the basis of the GNI Principles) as well as in mergers, acquisitions and divestment processes.
- **Public Affairs and Institutional Relations:** To promote privacy and freedom of expression by means of proactive advocacy with external stakeholders (e.g. governments, international organisations and NGOs).
- **Product managers and developers:** To integrate human rights from the design phase and focusing on products and services that incorporate new technologies such as Artificial Intelligence.

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.

Human rights by Design:

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

Transparency Initiatives:

One of the challenges and key elements of privacy is guaranteeing transparency. At Telefónica we seek to put this into practice by including transparency as one of the guiding principles of the Global Privacy Policy and developing different initiatives bringing this principle to life. A case in point is our Global Privacy Centre and the Privacy Centres of our OBs in the markets. In addition, Telefónica has been working on providing customers with access to the data they generate while using our services, data that are collected in the so-called "Personal Data Space". In 2020, we will launch the Transparency Centre in Spain to provide access to and management of the data collected in the Personal Data Space. Through the "Permissions" section, customers can manage their consent for the use of data for certain purposes. And the "Access and Download" section offers useful visualisations of different types of data, with a user-friendly experience and respecting privacy criteria. It also provides the option of downloading a document with a higher level of detail of those data sets.

The experience of the Transparency Centre has been designed to be user-centred, avoiding the use of complex legal language. Aura, Telefónica's artificial intelligence, accompanies and provides in each visualisation an explanation of the purpose and nature of the data within Telefónica, offering clarity, transparency and increasing trust.

With the Transparency Centre we further empower our customers with control and transparency functions over their data.

Effective application of policies and processes:

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

The observance and compliance with the regulations (e.g. the above-mentioned privacy and security policies, etc.) are subject to review and supervision by those responsible for the internal policies who lead the proposal, creation, dissemination and implementation of them and carry out its monitoring, evaluation and updating and who are empowered to carry out sample supervisions of the controls whenever they deem it appropriate to do so.

GNI (Global Network Initiative) and RDR (Ranking Digital Rights)

As testament to our commitment to the fundamental rights of freedom of expression and privacy, we are constituent members of the TID (Telecommunications Industry Dialogue) Group for Freedom of Expression and Privacy, a group that merged with the GNI (Global Network Initiative) in 2017. The GNI is a global organisation whose members are investors, think tanks and members of civil society and private companies: telecommunication operators, internet service providers and equipment and software manufacturers.

As a member of GNI, Telefónica is one of the signatories of the principles of the communications sector regarding freedom of expression and privacy and we are committed to their implementation and are held accountable by means of indepedent assessments through external auditors. Thus, in 2019 we successfully underwent our first independent assessment by the GNI. The GNI's Board of Directors, composed of multiple stakeholders, determined that Telefónica is making good-faith efforts to implement the GNI's principles of freedom of expression and privacy with improvements over time. The GNI's positive evaluation was based on a report by an independent external consultant (Deloitte) which assessed Telefónica's policies, processes and governance model for safeguarding freedom of expression and privacy.

In addition, we ranked first among all the telecommunications companies in the 2019 Ranking Digital Rights, which assesses companies' commitments, policies and practices regarding freedom of expression and privacy, including governance and supervisory mechanisms.

Indicators of this Report

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

Any request received from a national authority must comply with the judicial and/or legal processes that correspond to the country in question. At Telefónica we only repond to requests from Competent Authorities as laid down in our Global Rule on Requests made by Competent Authorities. At Telefónica **we don´t respond to private requests**, but only deal with requests from authorities that are empowered to do so by the law. However, as a sole exception, in order to proactively fight against contents and images of sexual abuse of minors on the internet, at Telefónica we proceed to block these materials in accordance with the guidelines and lists provided by the Internet Watch Foundation.

The indicators we report in this report are:

- **Lawful interceptions:** Requests made by Competent Authorities within the framework of criminal and, where appropriate, civil investigations with the aim of intercepting communications or accessing traffic data in real time.
  This year we have incorporated the breakdown of interceptions, whenever technically and/or legally possible, in the following way:
  - Registrations: Requests for a new interception.
  - Extensions: Requests to extend an existing interception.
  - Cancellations: Requests to disconnect an existing interception.
- **Access to metadata:** Requests made by Competent Authorities that seek to obtain historical data referring to:
  - registered users' name and address (subscriber information);
  - data identifying the source and destination of a specific communication (e.g., telephone numbers, Internet service user names, etc.);
  - communication dates;
  - times and duration;
  - type of communication;
  - computer equipment identities (including IMSI or IMEI);
  - user or device location.
- **Content blocking and restriction:** Requests made by Competent Authorities to block access to specific websites or any given content. These involve requests to block access to websites or contents, but not requests to delete user content. To give an example, blocking requests are issued because websites or contents infringe local laws (usually in relation to child pornography, online betting games, copyright, libel, the illegal sale of medicine, weapons, registered trademarks). This year we have incorporated the breakdown by blocking type when the tools and legislation so permit.
- **Geographical or temporary suspensions of the service:** Requests made by Competent Authorities to temporarily or geographically limit the provision of a service. These requests are usually connected with circumstances involving situations of force majeure, such as natural catastrophes, acts of terrorism, etc.

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

- **Requests rejected or partially dealt with:** number of times that we have rejected a request or that we have only provided partial information or no information in response to a request for one of the following reasons:
  - Because it does not comply with local legislation for that type of requirement.
  - Because it does not contain all the necessary elements to enable the execution (necessary signatures, competent authority, technical description of the requirement, etc.).
  - Because it is technically impossible to execute the request.

- **Accesses affected:** number of accesses affected by each request. We count the affected URLs for the blocking and restriction of contents.

What is more, this Transparency Report also seeks to inform in a transparent manner about our efforts regarding those requests and situations that may have a potential impact on the rights of privacy and/or freedom of expression. We classify these requests/ situations as "major events" (see definition in glossary).

In this context we should highlight the amendment of General Law 9/2014 on Telecommunications in Spain, by virtue of the provisions of Royal Decree-Law 14/2019 of 31st October, which adopts urgent measures for reasons of public security in matters of digital administration, public sector procurement and telecommunications. This law and the articles affecting legal interceptions are elaborated on in the legal context of the Spain country section.

In addition, we also 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
- Ecuador
- 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 21.2 million accesses at the end of December 2019.

With regard to the financial figures, in 2019 Telefónica's revenue in Argentina stood at 2,163 million euros and the OIBDA was 499 million euros.

21,221
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

3,143 Fixed telephony	**16,538** Mobile telephony
1,371 Broadband	**153.2** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

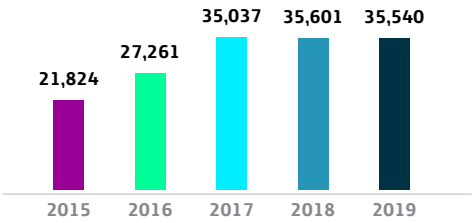
Legal framework

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

Requests



Breakdown of Interceptions (2019)

Registrations	14,727
Extensions	6,328
Cancellations	14,485
Accesses affected	14,727
Requests rejected	0

ACCESS TO METADATA

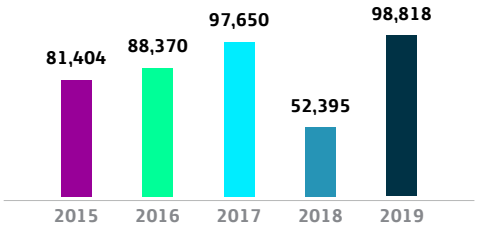
Legal framework

- 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.

Requests



*In 2019, we began to register the data on the indicators 1) access to metadata, 2) blocking and filtering of certain contents and 3) geographical or temporary suspension of the service separately in Argentina and not in an aggregated manner as in previous years, which is why the 2019 data is not comparable to the rest.

Accesses affected	98,818
Requests rejected	0

BLOCKING AND FILTERING OF CERTAIN CONTENTS

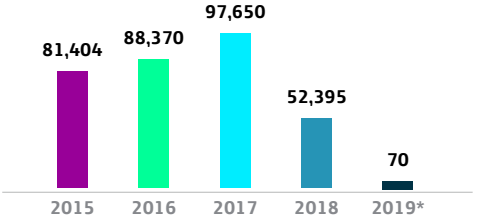
Legal framework

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.

Requests



*In 2019, we began to register the data on the indicators 1) access to metadata, 2) blocking and filtering of certain contents and 3) geographical or temporary suspension of the service separately in Argentina and not in an aggregated manner as in previous years, which is why the 2019 data is not comparable to the rest.

Type of blocking	Online gambling
URLs affected	68
Requests rejected	0

GEOGRAPHICAL OR TEMPORARY SUSPENSION OF THE SERVICE

Legal framework

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

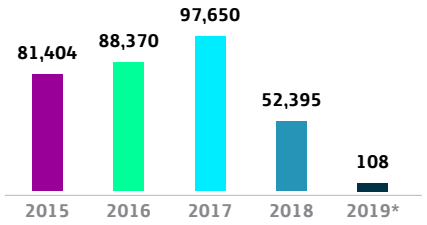
Article 57: Network Neutrality. Prohibitions. IC service providers may not:

a) 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



*In 2019, we began to register the data on the indicators 1) access to metadata, 2) blocking and filtering of certain contents and 3) geographical or temporary suspension of the service separately in Argentina and not in an aggregated manner as in previous years, which is why the 2019 data is not comparable to the rest.

The requests reported are to temporarily restrict the mobile data traffic of certain customers.

Accesses affected	108	Requests rejected	0

Brazil

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 93,7 million accesses in Brazil at December of 2019.

With regard to the financial figures, in 2019, Telefónica's revenue in Brazil reached about 10,035 million euros and the OIBDA stood at 4,262 million euros.

93,732.3
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

10,817
Fixed telephony

74,573.1
Mobile telephony

7,009.2
Broadband

1,319.7
Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

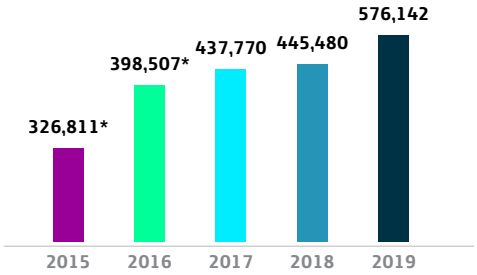
Legal framework

- Constitution of the Federal Republic of Brazil: Art. 5.
- Law Nº. 9,296, of 24 July 1996.
- Resolution Nº. 426 of 9 December 2005/ Regulation of Fixed Telephone Service - STFC. STFC.
- Resolution Nº. 614 of 28 May 2013/Regulation on Multimedia Communication Service.
- Resolution Nº. 477 of 7 August 2007/Regulation on Personal Service.

Competent authorities

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

Requests*



Breakdown of Interceptions (2019)

Registrations	556,520*
Extensions	-
Cancellations	19,622

*Includes registrations and extensions of interceptions.

Accesses affected	556,520	Requests rejected	0

ACCESS TO METADATA

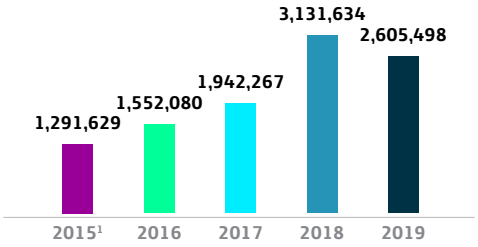
Legal framework

- Constitution of the Federal Republic of Brazil: Art. 5.
- Law Nº. 9,296 of 24 July 1996.
- Law Nº. 9,472 of 16 July 1997. Art. 3.
- Law Nº. 12.683 of 9 July 2012. Art. 17-B.
- Law Nº. 12,830, of 20 June 2013. Article 2.
- Law Nº. 12850 of 20 August 2013 Article 15.
- Law Nº. 12965 of 23 April 2014. Art. 7; 10 and 19.
- Decree Nº. 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 Nº. 426 of 9 December 2005/ Regulation of Fixed Telephone Service - STFC. STFC Articles 11, 22, 23 and 24.
- Resolution Nº. 477 of 7 August 2007/ Regulation on Personal Service Articles 6, 10, 12, 13, 89 and 90.
- Resolution Nº. 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).
- 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



Accesses affected	2,605,498	Requests rejected	0

BLOCKING AND FILTERING OF CERTAIN CONTENTS

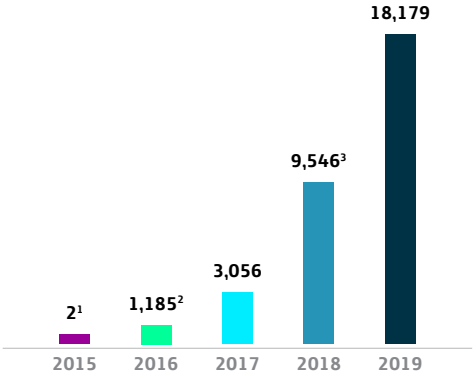
Legal framework

Law Nº. 12965 of 23 April 2014. Art. 7 and 19.

Competent authorities

Exclusively Judges.

Requests



URL's affected	18,179
Requests rejected	0

Copyright	Image Rights
0.03%	0.07%

Debt enforcement	Piracy
0.01%	99.88%

Others
0.02%

1. The two cases in 2015 correspond to the blocking of the WhatsApp application.
   * In February 2015, the judicial authority determined that the operators should block their customers' access to the WhatsApp application until the fulfilment of the original order sent to the application. The request had a legal basis within the area of the criminal proceedings conducted by the Commissioner for Child and Adolescent Protection.
   ** On 16/12/2015, the Company received another order for a 48hour access period to the WhatsApp application. The measure was adopted with the same legal basis as the case mentioned in the previous point.
2. Clarification: After the general blocking measures that affected all potential customers (whatsapp case), public authorities started to practice individual blocking in the field of criminal investigations.
3. In 2019, only URL blocking is counted, which is why we report the service suspensions of individual accounts in the "Suspension of Service" indicator.

GEOGRAPHICAL OR TEMPORARY SUSPENSION OF THE SERVICE

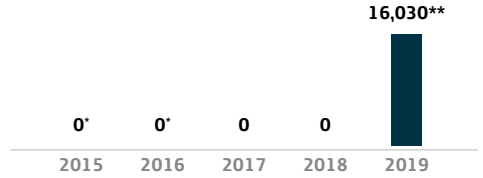
Legal framework

- Resolution Nº. 73 of 25 November 1998. Article 31.
- Resolution Nº. 477 of 7 August 2007. Article 19.

Competent authorities

Exclusively Judges.

Requests



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

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

Accesses affected	16,030
Requests rejected	N/A

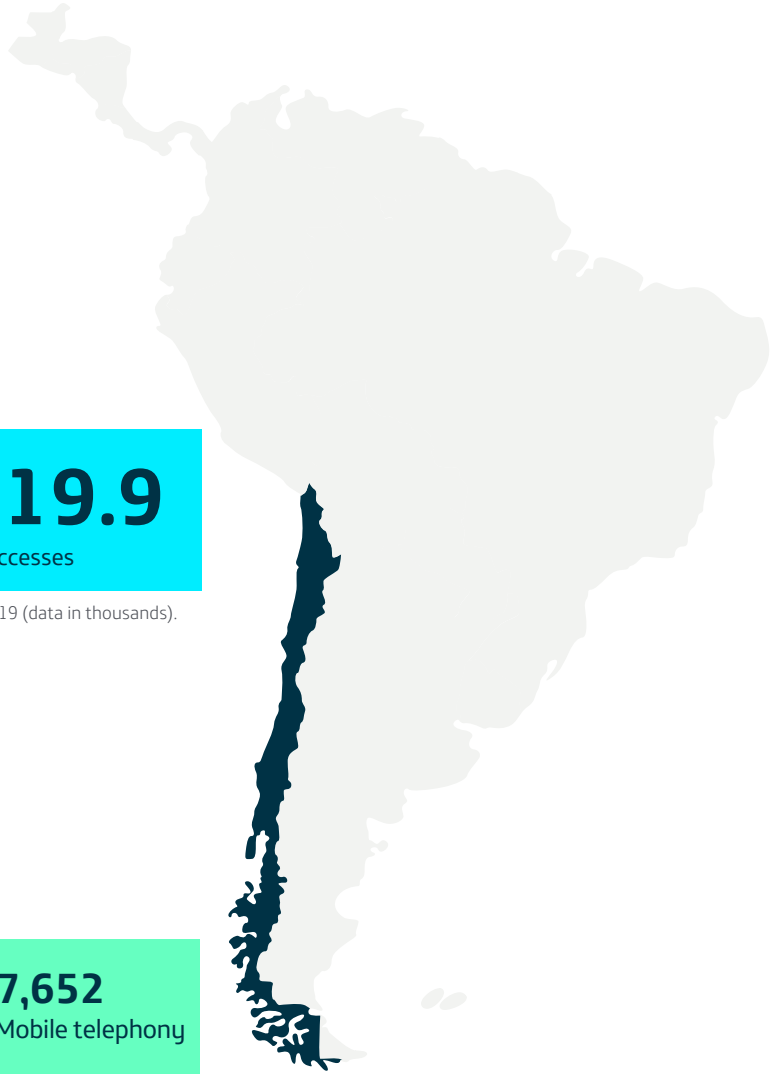
Chile

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 2019, Telefónica Chile had more than 10.3 million accesses. With regard to the financial figures, Telefónica's revenue in Chile stood at 1,914 million euros and the OIBDA was 669 million euros.



10,319.9
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

1,072.9 Fixed telephony	**7,652** Mobile telephony
1,065.6 Broadband	**523.3** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

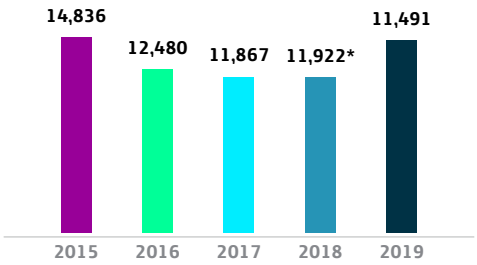
Legal framework

- 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



* The total of 11,922 requests for lawful interception includes a total of 714 requests for extensions of lawful interception.

Breakdown of Interceptions (2019)

Registrations	**11,020**
Extensions	**471**
Cancellations	**440***

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

Accesses affected	**5,590**	Requests rejected	**163**

ACCESS TO METADATA

Legal framework

- The Political Constitution of the Republic of Chile. Based on the provisions of the sole article of Law 21.096 that modified Article 19 number 4 of the Constitution, all persons are guaranteed: "... the protection of their personal data. The treatment and protection of this data will be carried out in the form and conditions determined by law".
- The Code of Criminal Procedure: Articles 219 and 222 of the Code of Criminal Procedure authorise the provision of information by order of the Judge of Guarantee, with a warning of contempt in the event of non-compliance, that is to say, with a warning of disobedience of a judicial decision, in accordance with Article 180 of the Code of Criminal Procedure and Article 240 of the Code of Civil Procedure.
- The Public Prosecutor´s Office (Ministerio Público) is the authority that directs the criminal investigation and issues investigative orders that may contain requests for information on telecommunications companies, in accordance with the provisions of Articles 19 and 180 of the Code of Criminal Procedure. In addition, and in accordance with the provisions of Article 182 of the Code of Criminal Procedure, which stipulates the secrecy of investigative actions, the Public Prosecutor´s Office may request background

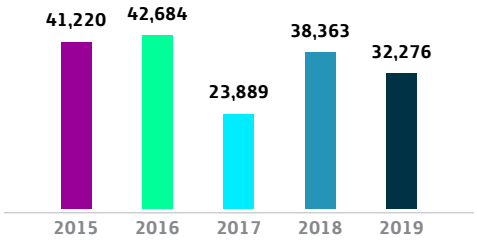
information on the subscription of services contracted by a particular person, sending jointly the identification data of the owner or user in the respective order to investigate, in order to determine the degree of participation of the persons involved. It also requests information on the activity of IMEI number records for certain devices that are the object of investigation, information that is sent without delivering the personal data of subscribers or users associated with that IMEI number.

- Constitutional Organic Law of the Public Prosecutor´s Office N°19.640.
- Inquisitorial Criminal Procedure: Articles 120bis and 171 of the Criminal Procedure Code.

Competent authorities

- Public Criminal Prosecutor: The Public Prosecutor's Office.
- 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 Inteligencie.
- Agencies with prior judicial authorisation.

Requests



Accesses affected	10,357	Requests rejected	675

BLOCKING AND FILTERING OF CERTAIN CONTENTS

Legal framework

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

Competent authorities

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

Requests

1. For violation of copyright (Law 17,336 of Intellectual Property).

URLs affected	0	Requests rejected	0

GEOGRAPHICAL OR TEMPORARY SUSPENSION OF THE SERVICE

Legal framework

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

Competent authorities

Not applicable.

Requests

N/A	N/A	N/A	N/A	N/A
2015	2016	2017	2018	2019

Accesses affected	N/A	Requests rejected	N/A

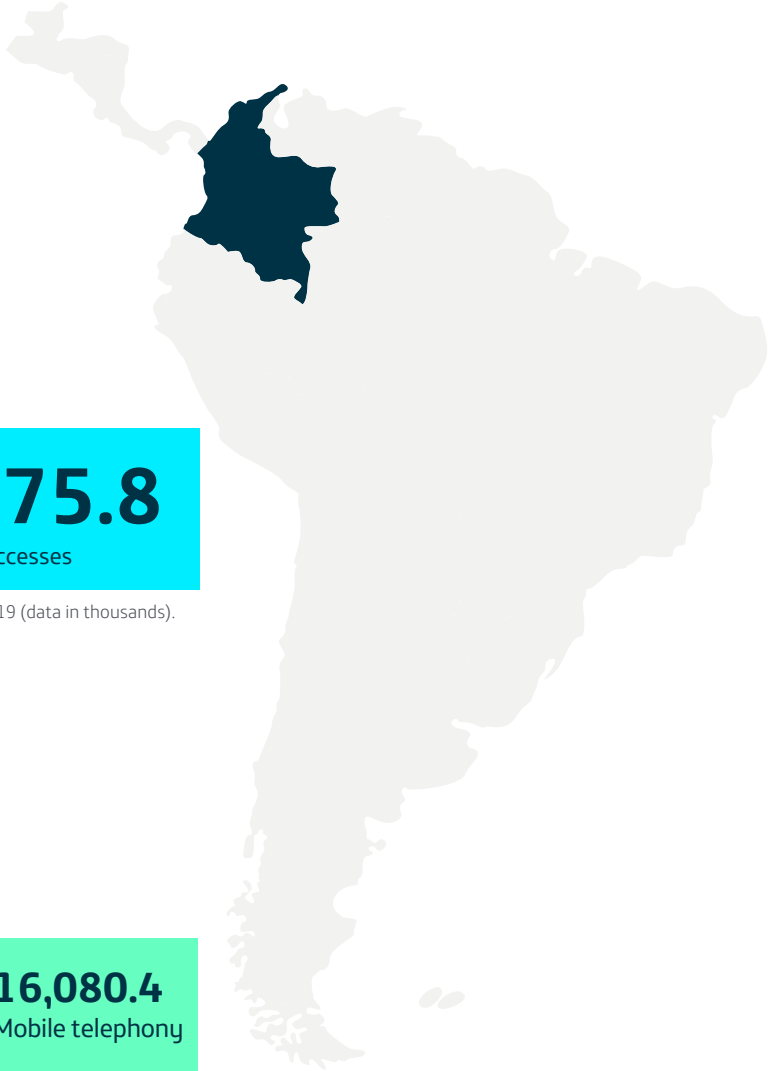
Colombia

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 19.2 million accesses at December of 2019.

Telefónica's revenue in Colombia reached 1,410 million euros and the OIBDA stood at 558 million euros by the end of 2019.



19,275.8
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

1,487.7 Fixed telephony	**16,080.4** Mobile telephony
1,179.2 Broadband	**528.1** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

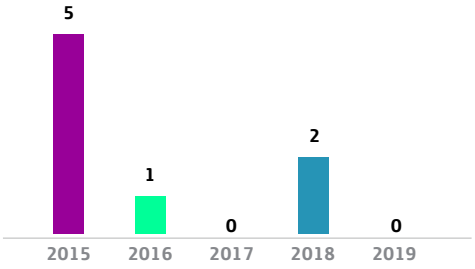
Legal framework

- 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	0	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, Articles 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:

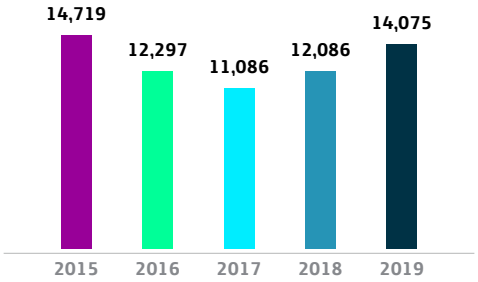
- Prosecutor General of the Nation and all the public servants who perform judicial functions (Article 249 CN and articles 112, 113 CPC).
- Judicial Police: C.T.I., National Police and D.A.S., authorised by the competent judicial authority and by legal mandate (Articles 311 to 320 CPC).
- "Anti-kidnapping 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 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	42,225	Requests rejected	140

BLOCKING AND FILTERING OF CERTAIN CONTENTS

TOTAL URL AFFECTED

URL's affected	10,561	Requests rejected	N/A*

*Because of the blocking system established by the law.

Child sexual abuse material

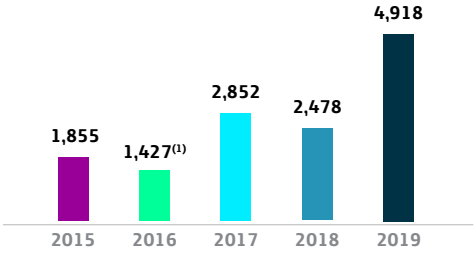
Legal framework

- 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*



(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.

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

Illegal Games

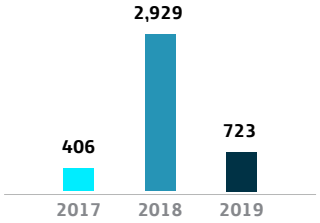
Legal framework

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

Competent 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 URL



Court Order

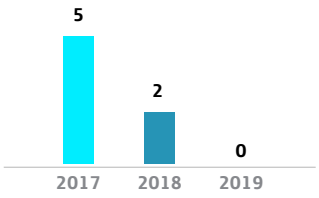
Legal framework

- 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 URL



GEOGRAPHICAL OR TEMPORARY SUSPENSION OF THE SERVICE

Legal framework

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

Decree 2434 of 2015, Resolution CRC 4972 2016 - Obliges prioritization of calls between authorities to deal with emergencies. This prioritization involves terminating user calls that are not on the list of numbers.

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

Accesses affected	0	Requests rejected	0

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 4,393 millones accesess in Telefonica Ecuador at December 2019.

Telefónica's revenue in Ecuador stood at 484 million euros and the OIBDA was 193 million euros in 2019.

4,393
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

0.0 Fixed telephony	**4,393** Mobile telephony
0.0 Broadband	**0.0** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

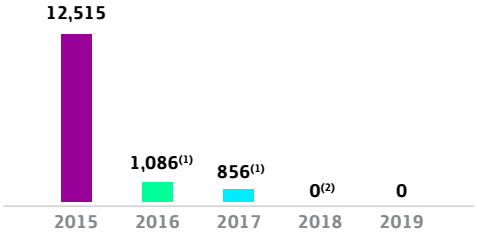
Legal framework

- 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

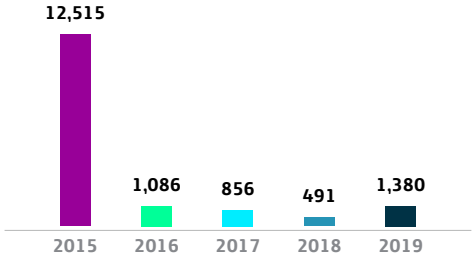
Legal framework

- Integral Organic Criminal Code. Section 499.

Competent authorities

- Judges of Criminal Guarantees.

Requests



Accesses affected	1,320	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

2015	2016	2017	2018	2019
0	0	0	1*	0

*For violating Copyright.

URLs affected	0
Requests rejected	0

GEOGRAPHICAL OR TEMPORARY SUSPENSION OF THE SERVICE

Legal framework

Constitution of Ecuador. Articles 164 and 165.

Competent authorities

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

Requests

2015	2016	2017	2018	2019
0	0	0	0	0

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 48.2 million accesses in Germany.

Telefónica's revenue in Germany reached € 7,399 million and OIBDA was 2,326 million euros.

48,258
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

2,129 Fixed telephony	**43,827** Mobile telephony
2,302 Broadband	**0.0** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

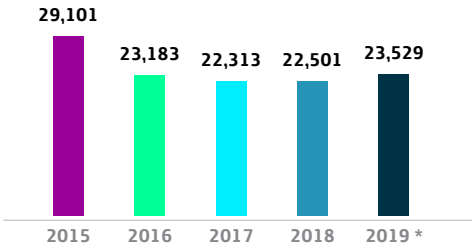
Legal framework

- 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 - G10).
- 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 includes new, extended and cancelled interceptions.

Accesses affected	55,772	Requests rejected	0

ACCESS TO METADATA

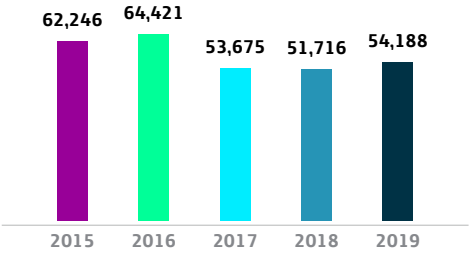
Legal framework

- 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	458,872	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

N/A	N/A	N/A	N/A	N/A
2015	2016	2017	2018	2019

URLs affected	N/A	Requests rejected	N/A

GEOGRAPHICAL OR 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

N/A	N/A	N/A	N/A	N/A
2015	2016	2017	2018	2019

Accesses affected	N/A	Requests rejected	N/A

Mexico

www.telefonica.com.mx

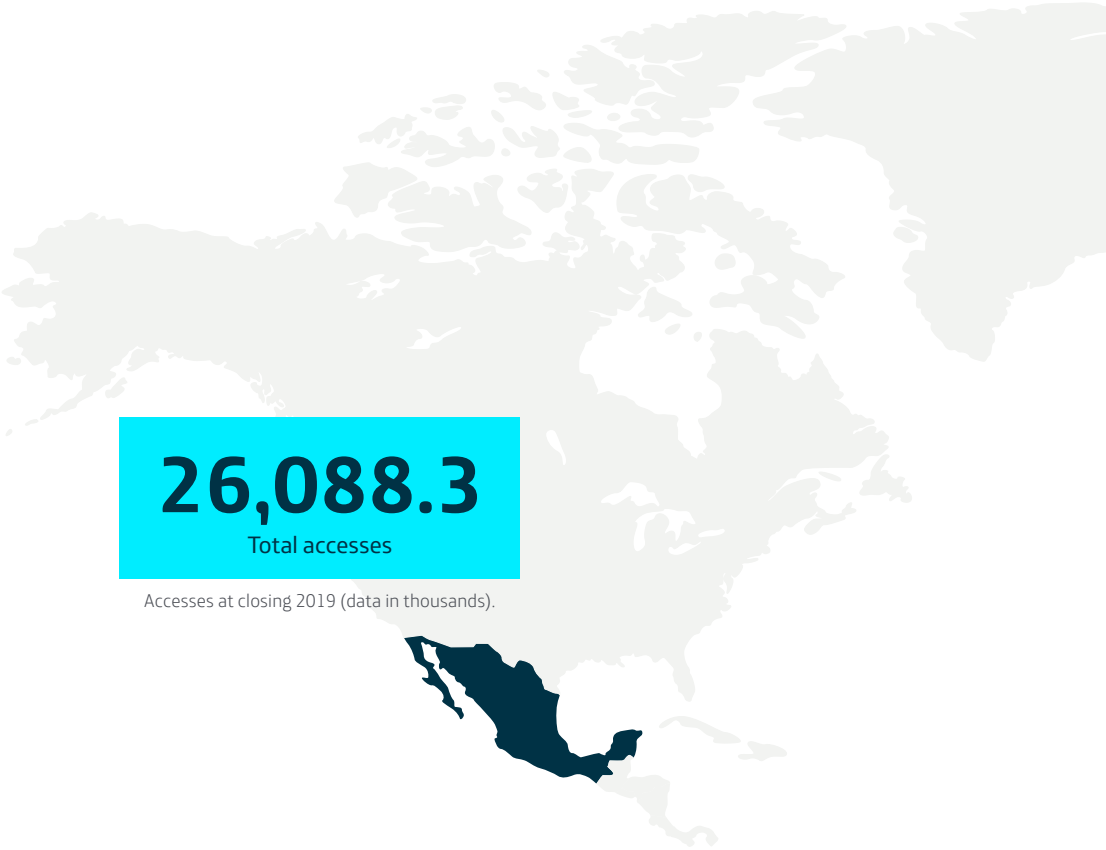
Telefónica Mexico has participated and competed in the mobile telecommunications market since 2001 and promotes the development of telecommunications in the country.

The commercial offers are available in 231Customer Service Centers (CAC), 36 Movistar Stores as well as n 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 26.6 million accesses in December 2019.

With regard to the financial figures, in 2019 Telefónica's revenue in Mexico stood at 1,244 million euros and the OIBDA was 147 million euros.

(1) Includes the impact of -239M euros (October-December 2019) as a result of the transformation of T. Mexico's operational model following the agreement reached with AT&T.



26,088.3
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

0.0 Fixed telephony	**26,088.3** Mobile telephony
0.0 Broadband	**0.0** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

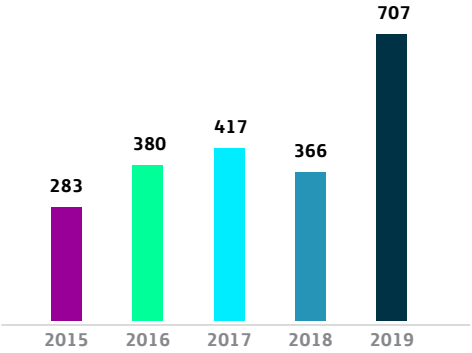
Legal framework

- 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



Breakdown of Interceptions (2019)

Registrations	368
Extensions	10
Cancellations	329
Accesses affected	460
Requests rejected	2

ACCESS TO METADATA

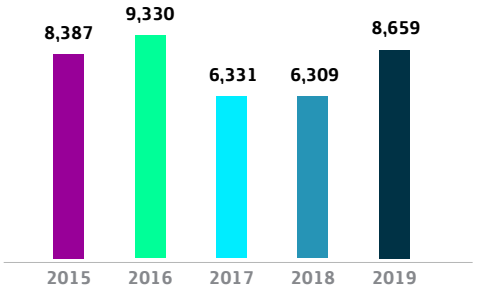
Legal framework

- 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



Accesses affected	18,331
Requests rejected	149

BLOCKING AND FILTERING OF CERTAIN CONTENTS

Legal framework

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

Competent authorities

Not applicable.

Requests

N/A	N/A	N/A	N/A	N/A
2015	2016	2017	2018	2019

URL's affected	N/A	Requests rejected	N/A

GEOGRAPHICAL OR TEMPORARY SUSPENSION OF THE SERVICE

Legal framework

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

Competent authorities

Not applicable.

Requests

N/A	N/A	N/A	N/A	N/A
2015	2016	2017	2018	2019

Accesses affected	N/A	Requests rejected	N/A

Peru

www.telefonica.com.pe

Telefónica began to operate in the Peruvian market in the middle of the 1990s. The company managed more than 17.6 million accesses at the end of third quarter 2019.

Regarding financial figures, Telefónica's revenue in Peru stood at 2,102 million euros and the OIBDA was 354 millon euros.

17,640.6
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

2,247 Fixed telephony	**11,897.4** Mobile telephony
1,991.5 Broadband	**1,505.0** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

Legal framework

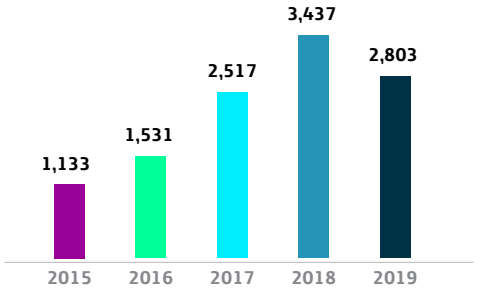
- Political Constitution of Peru, Art. 2, paragraph 10.
- Telecommunications Law (Supreme Decree No. 013-93-TCC - Article 4) and its Regulations (Supreme Decree No. 0202007-MTC - Article 13).
- Law No. 27697: Law which grants power to the public prosecutor for the intervention and control of communications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

Requests*



*Includes registrations, extensions and cancellation of interceptions.

Accesses affected	4,257	Requests rejected	298

ACCESS TO METADATA

Legal framework

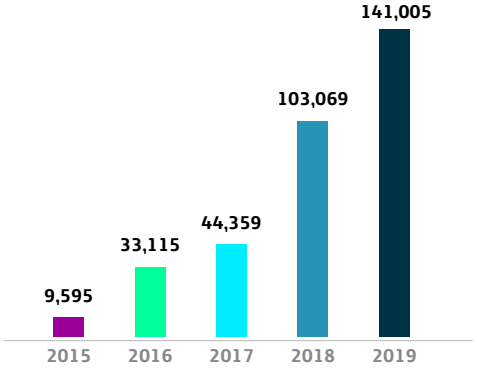
- Political Constitution of Peru, Art. 2, paragraph 10.
- Telecommunications Law (Supreme Decree No. 013-93-TCC - Article 4) and its Regulations (Supreme Decree No. 020-2007MTC - Article 13).
- Law No. 27697: Law which grants power to the public prosecutor for the intervention and control of communications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

The heads of the security and law enforcement agencies will designate the public servants responsible for managing the requests made to the operators and receive the corresponding information, by means of agreements published in the Federal Official Gazette.

Requests



Accesses affected	45,473	Requests rejected	969

BLOCKING AND FILTERING OF CERTAIN CONTENTS

Legal framework

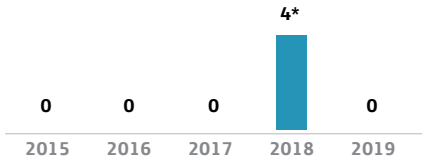
Copyright Law.

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



*Requerimientos de INDECOPI (medidas cautelares en casos por propiedad intelectual).

URL's affected	0	Requests rejected	0

GEOGRAPHICAL OR 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

Accesses affected	0	Requests rejected	0

Spain

www.telefonica.es

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 41.8 million accesses at the end of December 2019.

Revenue from operations amounts to 12,767 millones de euros and its OIBDA reached 3,687 million euros in 2019.

41,837.7
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

9,024.1 Fixed telephony	**18,916.9** Mobile telephony
6,034.8 Broadband	**4,073.8** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

Legal framework

- Spanish Constitution, Art. 18.
- Law of criminal prosecution, Art. 588.
- Law 9/2014, General of Telecommunications (Art. 39 and 42). What is more, this law has been amended in accordance with the provisions of Royal Decree Law 14/2019 of 31 October, adopting urgent measures for public security reasons in the field of e-government, public sector procurement and telecommunications Thus, there is a new wording to Articles 4(6) and 81(1).
  - Article 4(6), "The Government may, exceptionally and temporarily, agree to the direct management or intervention by the General State Administration of electronic communications networks and services in certain exceptional cases which could affect public policy, public security and national security. In particular, this exceptional and transitional power of direct management or intervention may affect any infrastructure, associated resource or element or level of the network or service that is necessary to preserve or restore public policy, public security and national security.

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

    The agreements to take over the direct management of the service and the intervention or those of intervening or operating the networks referred to in the preceding paragraphs shall be adopted by the Government on its own initiative or at the request of any competent public administration. In the latter case, it will be necessary that the public administration has security clearance or for the provision of the public services affected by the abnormal functioning of the service or the network of electronic communications. In the event of that the procedure be initiated at the request of a different administration from that of the State, the latter shall be deemed to be interested and may conduct a report with character prior to final resolution."
  - Article 81(1), "Prior to the beginning of the sanctioning procedure, may be ordered by the competent body of the Ministry of Economy and Enterprise, by resolution without prior hearing, the cessation of the alleged infringing activity where there are reasons of overriding urgency based on any of the following assumptions:

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

    b) Where there is an immediate threat and serious for public health.

    c) When the alleged infringing activity may result in serious damage to the operation law enforcement public, civil and emergency protection.

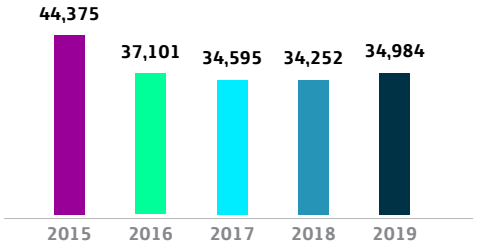
    d) Where serious interference is made with others communication services or networks electronics.

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

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.
- The Government, on an exceptional basis and may agree to assume responsibility for the General State Administration of the direct management or intervention of networks and electronic communications services in certain exceptional cases that may affect public order, the public safety and national security.

Requests



Breakdown of Interceptions (2019)

Registrations	12,944
Extensions	15,700
Cancellations	6,340
Accesses affected	14,215
Requests rejected	5,374

ACCESS TO METADATA

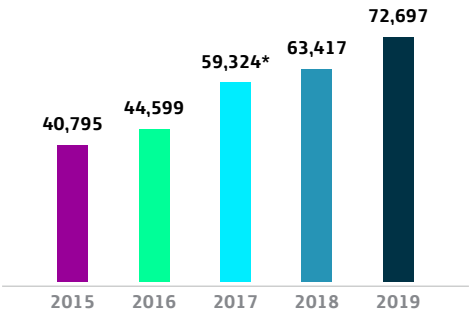
Legal framework

- 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



* 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*	Requests rejected	12,397

* 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

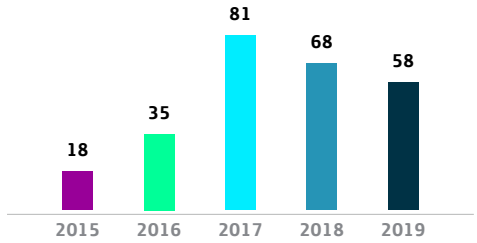
Legal framework

- 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/AccountingAdministrative/ Criminal Courts.
- National Intellectual Property Commission.
- General Gambling Directorate.
- Agency for Medicine/Doping/Health/Sport.

Requests



Copyright

Nº solitudes	29	Nº of URL's affected	770

Crimes

Nº solitudes	24	Nº of URL's affected	131

Medications

Nº solitudes	2	Nº of URL's affected	2

Illegal gambling

Nº solitudes	3	Nº of URL's affected	1,385

URL's affected	2,288*	Requests rejected	0

*Includes URLs and IP addresses

GEOGRAPHICAL OR TEMPORARY SUSPENSION OF THE SERVICE

Legal framework

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

Competent authorities

Not applicable.

Requests

2015	2016	2017	2018	2019
N/A	N/A	N/A	N/A	N/A

Accesses affected	N/A	Requests rejected	N/A

United Kingdom

www.telefonica.com/en

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 34.8 million accesses at the end of 2019 in the UK.

With regard to the financial figures, in 2019 Telefónica's reveneu in UK stood at €7,109 million and OIBDA amounts up to €2,144 million.

34,860.2
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

313.3 Fixed telephony	**25,803.3** Mobile telephony
28.9 Broadband	**0.0** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

Legal framework

Lawful intercept is governed by the Investigatory Powers Act 2016 (IPA). The Investigatory Powers Commissioner (IPC) and the Investigatory Powers Commission's Office (IPCO) are now fully established. IPCO is overseeing implementation and compliance with the lawful intercept requests made pursuant to the IPA.

Competent authorities

Under the IPA, the Secretary of State for a relevant Government department can issue an intercept warrant where he/she believes it is necessary in the interests of national security, for the purpose of preventing or detecting serious 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 authorised 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 must be authorised by the Secretary of State (or their deputy) in the form of a warrant and a judge. The judge will consider the same factors as the Secretary of State (i.e. whether there are grounds for the issuing of the warrant and whether the conduct is proportionate to the objective).

Requests*

N/D	N/D	N/D	N/D	N/D
2015	2016	2017	2018	2019

*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. Please see: https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202017%20Web%20Accessible%20Version%2020190321.pdf

Accesses affected	N/D

Requests rejected	N/D

ACCESS TO METADATA

Legal framework

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

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

Competent authorities

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 offices 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.

IPA regime

- 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*

N/D	N/D	N/D	N/D	N/D
2015	2016	2017	2018	2019

*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	N/D	Requests rejected	N/D

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. This is legal content. e.g. legal adult sites (unlike IWF sites which are child abuse sites).

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

The code of practice can be viewed here: http://www.mobilebroadbandgroup.com/documents/mbg_content_code_v2_100609.pdf

TUK also seeks to block access to sites which are linked to "phishing" and "smishing" i.e. the fraudulent practice of sending emails and text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers in accordance with its legal rights.

Competent authorities

- Internet Watch Foundation.

- Courts.

Requests*

N/D	N/D	N/D	N/D	N/D
2015	2016	2017	2018	2019

*Only IWF, no stats available.

URL's affected	N/D	Requests rejected	N/D

GEOGRAPHICAL OR TEMPORARY SUSPENSION OF THE SERVICE

Legal framework

Telefónica UK has obligations to be able to provide service limitations in network overload situations – e.g. major disaster, etc– to provide priority service to emergency responders. The Mobile Telecommunications Privileged Access Scheme (MTPAS) was created under the Civil Contingencies Act 2004 (CCA). Eligibility is restricted to organisations that have a part to play in responding to, or recovering from, an emergency as defined in the CCA . At the onset of an emergency response, the relevant Police commander will use an agreed protocol to notify all mobile network operators that a major incident has been declared and request that call traffic levels are monitored. If networks become congested, the network operators are asked to consider invoking MTPAS to give emergency responders a much higher likelihood of being able to make a call than other customers.

Competent authorities

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

Requests*

2015	2016	2017	2018	2019
0	0	0	0	0

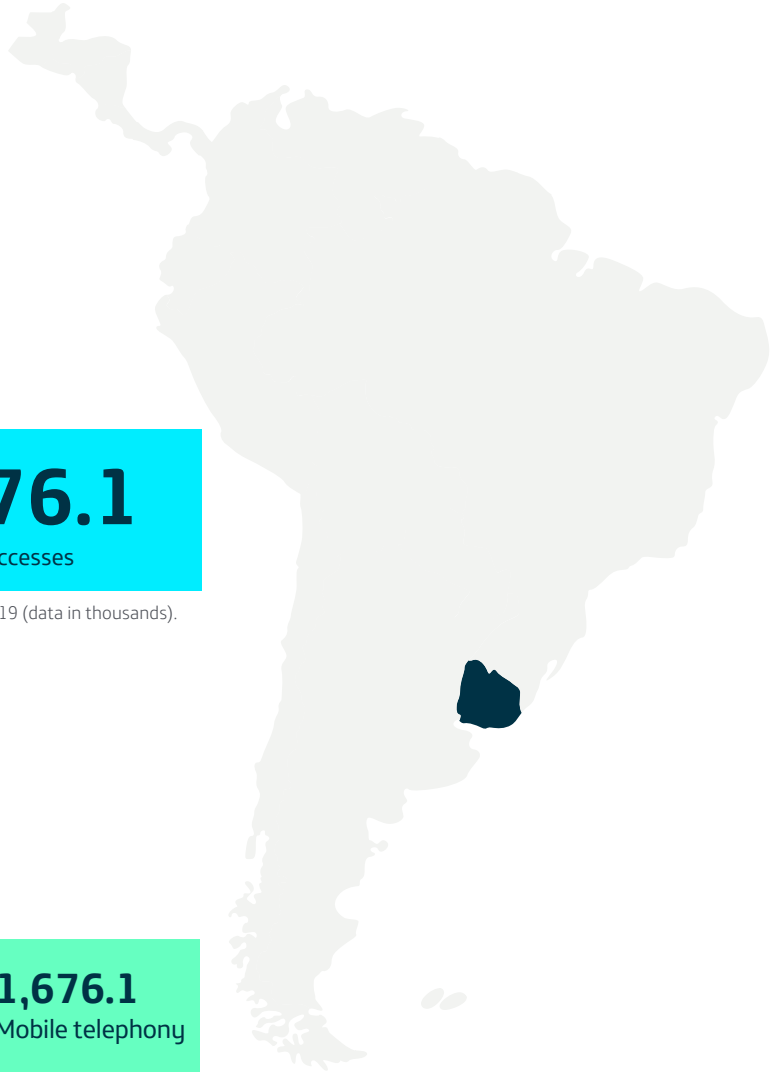
Accesses affected	0	Requests rejected	0

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 2019, Telefónica's revenue in Uruguay reached 219 million euros and the OIBDA was 83 million euros.



1,676.1
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

0.0 Fixed telephony	**1,676.1** Mobile telephony
0.0 Broadband	**0.0** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

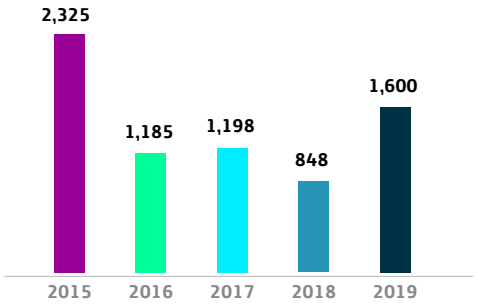
Legal framework

- 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



Breakdown of Interceptions (2019)

Registrations	867
Extensions	489
Cancellations	244

Accesses affected	867	Requests rejected	22

ACCESS TO METADATA

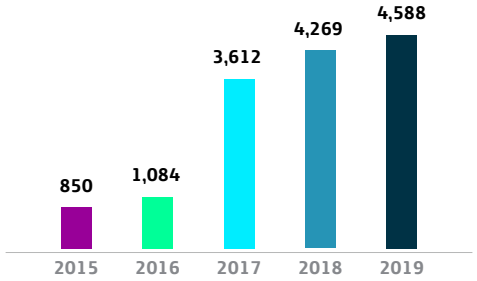
Legal framework

- 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*



* 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	4,588	Requests rejected	36

BLOCKING AND FILTERING OF CERTAIN CONTENTS

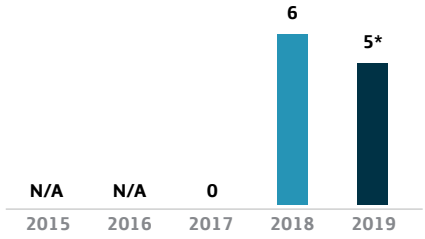
Legal framework

- 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



*Games and sports betting online.

URL's affected	19
Requests rejected	3

GEOGRAPHICAL OR TEMPORARY SUSPENSION OF THE SERVICE

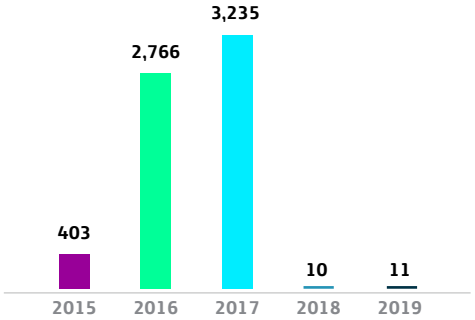
Legal framework

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 suspension for a period of 3 to 6 months.

Accesses affected	1,422
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 2019, Telefónica's income in Venezuela was 79 million euros and the OIBDA stood at 19 million euros.

9,474
Total accesses

Accesses at closing 2019 (data in thousands).

Accesses

344 Fixed telephony	**8,818** Mobile telephony
6 Broadband	**306** Pay TV

Accesses at closing 2019 (data in thousands).

LAWFUL INTERCEPTIONS

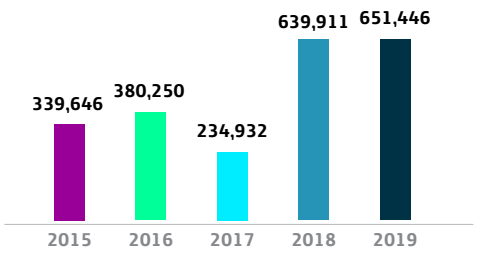
Legal framework

- 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*



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

Accesses affected	1,212,732	Requests rejected	6,617

ACCESS TO METADATA

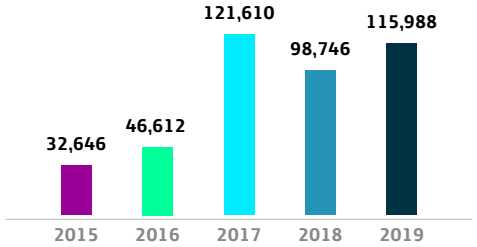
Legal framework

- 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	1,013,531	Requests rejected	916

BLOCKING AND FILTERING OF CERTAIN CONTENTS

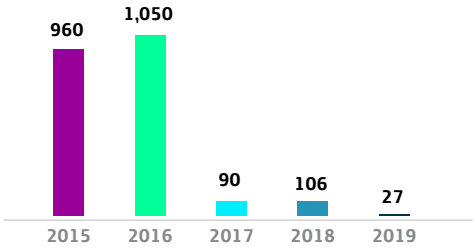
Legal framework

- 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



URL's affected	27
Requests rejected	0

GEOGRAPHICAL OR TEMPORARY SUSPENSION OF THE SERVICE

Legal framework

Organic Law on Telecommunications, Article 5.

Competent authorities

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

Requests

Accesses affected	0
Requests rejected	0

Glossary

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

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

CONCEPT	EXPLANATION
MAJOR EVENTS (cont.)	> Specific shutdown of any kind of telecommunications services, resulting from political causes. (e.g. concerning a small number of cells). > Denying certain clients access to specific services or networks in order to limit said individuals' legitimate freedom of expression. **2. Network shutdow Not applicableccess 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.

CONCEPT	EXPLANATION
Request	A Petition is a requirement related to the provision of a service, in the exercise of the duty of cooperation with the Competent Authorities. A Petition may contain one or more individualized requests, called Requests. Types of Requests: > Lawful interception of communications > Metadata associated with communications > Content blocking and restriction > Suspension of service
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.