Telefónica

Report on Transparency in Communications 2024

Contents

Introduction and scope of the report

Telefónica, like any other telecommunications company, is required by law, in the jurisdictions in which it operates, to cooperate and respond to requests for information [see glossary] made by competent authorities [see glossary], including State security forces, bodies, government agencies and/or courts.

For this reason, and as part of our commitment to **human rights** in general, and to **privacy and freedom of expression** in particular, we publish a yearly Transparency Report. This report contains detailed information on requests made by competent authorities. These requests are related to: lawful interceptions of communications, access to metadata, content blocking and restriction and geographical or temporary suspensions of the service.

In line with our general human rights approach as well as our due diligence process, we follow the provisions set out in our **Regulation on Requests from competent authorities,** which aims to ensure a balance between legal compliance and respect for the fundamental rights of people in the countries where we operate.

At Telefónica we **do not respond to private requests.** We only deal with *requests* that come from a competent authority in the country in question. Any request must comply with the judicial and/or legal processes applicable in the corresponding country.

This report covers the annual period from 1 January to 31 December 2024 and includes information on all OBs that are part of Telefónica as of the publication date. It provides details on:

- Local legislative context that grants legal power to the competent authorities to make *requests;*
- Names of the local competent authorities legally empowered to submit *requests;*
- Total number of *requests* received and rejected during the year;
- Total number of accesses affected.

.

Reported indicators

In this document we report the number of *requests* we receive from the competent authorities in the countries in which we operate.

The **indicators** we offer in this report are:

1. Lawful interceptions of communications:

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.

2. Access to metadata:

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

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

3. Content blocking and restriction:

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

4. Geographical or temporary suspensions of the service:

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

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

- ***Requests* rejected or partially deal with:** number of times we have rejected a request or provided only partial or no information in response to a request for any 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.
- **Affected accesses:** number of accesses affected by each request. For content blocking and restriction, affected URLs are counted.

There may be significant variations in the data for each of the indicators mentioned below, both with respect to previous years and between countries, which are usually due to technical, methodological, seasonal or legislative reasons. While all reasonable care has been taken to ensure the accuracy of the data the information contained in this report has not been audited. Neither Telefónica Group, nor any of the members of its senior management, its directors or its employees, either explicitly or implicitly, guarantees that these contents are exact, accurate, comprehensive or complete.

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

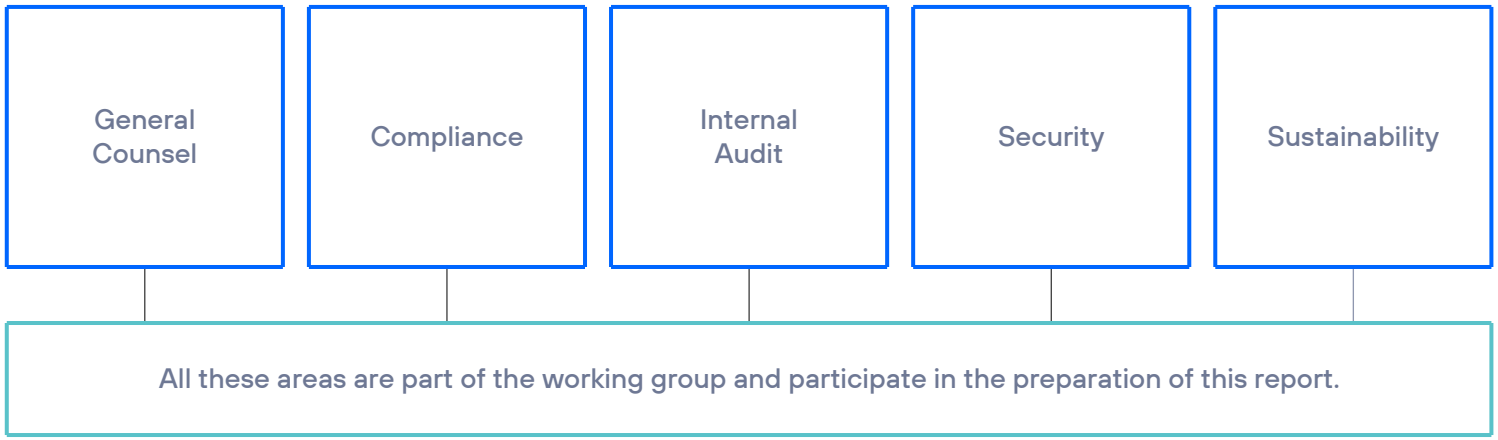
In this respect, we must highlight the situation of Venezuela, in which Telefónica must prioritise compliance with current legislation, the maintenance of connectivity in the country and the well-being of our employees.

Governance of the report

The following corporate areas are involved in the governance and management of this report: **General Counsel, Compliance, Internal Audit, Security and Sustainability,** as well as the corresponding local General Counsel teams in the OBs.

For the preparation of this report, an analytical review of the locally reported data is carried out and the participating areas may make any observations they deem pertinent, either generally or specifically, in relation to the information provided by the operators. The objective is to ensure at all times the quality of the information, in compliance with the regulations in force, the protection of the fundamental rights of individuals and based on the procedures performed.

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



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

- certain *requests* by authorities;
- certain legislations.

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

Finally, Telefónica has a public website where a list of the latest reports is published.

Report by country

Brazil

Lawful interceptions of communications

Legal framework

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

Competent authorities

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

Requests

Interceptions	2024
N° of requests received	270,516
N° of rejected *requests*	62,203
N° of accesses affected *	208,313

* Considering the same number of applications received (1:1), excluding those rejected.

Access to metadata

Legal framework

- Law No. 9,296, 24/07/1996.
- Law No. 9,472, Article 3, 16/07/1997.
- Law 9,613/98.
- Law No. 12,830, Article 2, 20/07/2013.
- Law No. 12,850, Article 15, 20/08/2013.
- Law No. 12,965, Articles 7, 10 and 19, 23/04/2014.
- Law No. 13,812, Article 10, 05/2019.
- Resolution No. 73 of 25 November 1998 / Regulation of Telecommunications Service - Article 65 - K.
- Resolution No. 765 of 2023.
- Decree-Law 3.689/1941.

Competent authorities

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

- Judges in any sphere: data to identify the origin and destination of a communication (e.g., telephone numbers, internet service user names), date, time and duration of a communication and the location of the device.

Requests

Metadata Requests	2024
N° of request received	4,656,502
N° of rejected requests	129,757
N° of accesses affected *	4,526,745

* Considering the same number of applications received (1:1), excluding those rejected.

Content blocking and restriction

Legal framework

- Administrative Ruling No. 1.475 of 16 September 2024, Article 2, paragraph 3. Provides the conditions and adaptation deadlines for legal entities that operate the lottery modality of fixed-odd betting.
- Action Plan to combat the use of clandestine decoders in the conditional access service, approved by Anatel Resolution No. 189 of 7 February 2023.
- Law 12.965/14.

Competent authorities

- Exclusively Judges.

Requests

Blocking Requests	2024
N° of requests received	31,655
N° of rejected requests	128
N° of urls affected *	31,527
Breakdown of petitions according to local legislation (e.g. for child pornography, intellectual property, etc...).	
Website/domain blocking: Copyright Piracy National operation - piracy Image rights Compensation for material damage Other	

* Considering the same number of applications received (1:1), excluding those rejected.

Geographical or temporary suspension of the service

Legal framework

- Resolution No.73 of 25 November 1998 / Regulation of Telecommunications Service - Article 65-K.
- Internal Resolution No. 189/2023 of ANATEL.
- Law 12.965/14.

Competent authorities

- Exclusively Judges.

Requests

Suspensions Requests	2024
N° of requests received	14,941
N° of rejected requests	924
N° of accesses affected *	14,017

* Considering the same number of applications received (1:1), excluding those rejected.

Chile

Lawful interceptions of communications

Legal framework

- No. 5 of Article 19 of the Political Constitution. Inviolability of Communications.
- Criminal Procedure Code, Articles 9, 219, 222, 223 and 224.
- Law 20,000. Traffic and control of narcotics, Article 24.
- Law 19,913 on money laundering.
- Law 18,314 that determines terrorist conduct. No.3, Article 14.
- Decree Law 211, Article 39 letter n).
- Law 19,974. National Intelligence System Law. Letters a), b), c) and d) of Article 24, in relation to Articles 23 and 28 of the same legal body.
- Criminal Procedure Code, Articles 177, 113 bis and 113 ter.
- Decree 142 of 2005 of the Ministry of Transport and Telecommunications, Regulation on the interception and recording of telephone communications and other forms of telecommunication, modified by Decree 198-2024, published in the Official Gazette on January 31, 2025.

Competent authorities

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

Requests

Interceptions	2024
N° of requests received	5,865
N° of rejected request	175
N° of accesses affected*	5,690

* Considering the same number of applications received (1:1), excluding those rejected.

Access to metadata

Legal framework

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

Competent authorities

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

Requests

Metadata Requests	2024
N° of request received	30,705
N° of rejected requests	5,039
N° of accesses affected	18,501

Content blocking and restriction

Legal framework

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

Competent authorities

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

Requests

Blocking Requests	2024
N° of requests received	0
N° of rejected requests	0
N° of urls affected	0

- *There is no record of requests received associated with content blocking or filtering.*

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

Suspensions Requests	2024
N° of requests received	N.A.
N° of rejected request	N.A.
N° of accesses affected	N.A.

Colombia

Lawful interceptions of communications

Legal framework

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

Competent authorities

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

Requests

Interceptions	2024
N° of requests received	N.A.
N° of rejected request	N.A.
N° of accesses affected	N.A.

Access to metadata

Legal framework

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

Competent authorities

- Guarantee Control Judge.

Grants judicial authorization for communications interceptions.

- Office of the Attorney General (*Fiscalía General de la Nación*)

Requests interception authorization from the judge.

Coordinates, directs, and oversees the execution of the measure.

May authorize temporary interceptions in urgent cases (must be legalized within 36 hours).

- Judicial Police Units

Technically carry out interceptions under judicial order and the supervision of the Attorney General's Office.

- CTI (Technical Investigation Corps) of the Attorney General's Office.

- DIJIN (Criminal Investigation and INTERPOL Directorate) of the National Police.

Requests

Metadata Requests	2024
N° of request received	14,963
N° of rejected requests	3,302
N° of accesses affected	31,770

Content blocking and restriction

Legal framework

- Law 1098 of 2006 (Code on Children and Adolescents) and Law 1453 of 2011 reforming the Code on Children and Adolescents.
- Law 679 of 2001, which issued legislation to prevent and counter child exploitation, child pornography and child sexual tourism, pursuant to Article 44 of the Constitution (Articles 7 and 8).
- Decree 1524 of 2002, implementing Article 5 of Law 679 of 2001, in order to establish the technical and administrative measures intended to prevent access by children to any type of pornographic information on the Internet or on the different types of computer networks which can be accessed through global information networks (Articles 5 and 6).
- Law 1450 of 2011, which issued the 2010-2014 National Development Plan, Article 56.
- Law 1273 of 2009, amending the Criminal Code, creating a new protected legal right - known as "data protection" - and integrally preserving the systems which use information and communication technology, among other provisions, Article 269G, Article 269F.

Competent authorities

- Judicial police with a court order from a supervisory judge.
- Supervisory judge.
- Judicial authorities, with intelligence and counter intelligence units (National Police; military forces; UIAF (Information and Financial Analysis Unit).
- CRC (Communications Regulatory Commission) Ruling 3502 of 2011.

Requests

Blocking Requests	2024
N° of requests received	25
N° of rejected requests	0
N° of urls affected	15,780

Breakdown of petitions according to local legislation (e.g. for child pornography, intellectual property, etc...).

The list of URLs corresponds to the new URLs included in the blocking lists sent by the relevant authorities:
i) Blocking related to children and adolescents
ii) Coljuegos
iii) Judicial orders

Geographical or temporary suspension of the service

Legal framework

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

Competent authorities

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

Requests

Suspensions Requests	2024
N° of requests received	0
N° of rejected request	0
N° of accesses affected	0

Ecuador

Lawful interceptions of communications

Legal framework

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

Competent authorities

- Competent prosecutor within an investigation.
- In Ecuador, the Company does not manage these type of requests. The Attorney General's Office of Ecuador, as the competent authority in accordance with the law, carries out the interceptions directly.

Requests

Interceptions	2024
N° of requests received	N.A
N° of rejected request	N.A.
N° of accesses affected	N.A.

Access to metadata

Legal framework

- Organic Integral Penal Code, Article 499.

Competent authorities

- Judges of Criminal Guarantees.

Requests

Metadata Requests	2024
N° of request received	11,241
N° of rejected requests *	0
N° of accesses affected	11,241

* *All request received complied with the applicable legality.*

Content blocking and restriction

Legal framework

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

Competent authorities

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

Requests

Blocking Requests	2024
N° of requests received	6
N° of rejected requests *	0
N° of urls affected	6

Breakdown of petitions according to local legislation (e.g. for child pornography, intellectual property, etc...).

The requests were for unauthorised broadcasting of national and international football matches.

* *All request received complied with the applicable legality.*

Geographical or temporary suspension of the service

Legal framework

Constitution of Ecuador, Articles 164 and 165.

Competent authorities

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

Requests

Suspensions Requests	2024
N° of requests received	0
N° of rejected request	0
N° of accesses affected	0

- *There have been no requests in 2024.*

Germany

Lawful interceptions of communications

Legal framework

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

Competent authorities

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

Requests

Interceptions	2024
N° of requests received	32,049
N° of rejected request *	0
N° of accesses affected	67,749

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

Access to metadata

Legal framework

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

Competent authorities

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

Requests

Metadata Requests	2024
N° of request received	63,654
N° of rejected requests *	0
N° of accesses affected	511,043

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

Content blocking and restriction

Legal framework

- Telecommunications Act, Section 165 Technical and organisational protective measures and blocking requested (Telekommunikationsgesetz - TKG).
- State Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and Telemedia, Section 14 (Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien).

Competent authorities

- Clearing Body for Copyright on the Internet (CUII)
- Bavarian regulatory authority for new media (BLM).

Requests

Blocking Requests	2024
N° of requests received	199
N° of rejected requests *	0
N° of urls affected	750
Breakdown of petitions according to local legislation (e.g. for child pornography, intellectual property, etc...).	
Telefonica:e.g. phishing Intellectual property (Clearing Body for Copyright on the Internet [CUII]) European Council Regulation (EU) 2022/350 Bavarian regulatory authority for new media (BLM)	

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

Geographical or temporary suspension of the service

Legal framework

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

Competent authorities

- Not applicable.

Requests

Suspensions Requests	2024
N° of requests received	N.A.
N° of rejected request	N.A.
N° of accesses affected	N.A.

Mexico

Lawful interceptions of communications

Legal framework

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

Competent authorities

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

Requests

Interceptions	2024
N° of requests received	387
N° of rejected request	0
N° of accesses affected	461

Access to metadata

Legal framework

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

Competent authorities

- The heads of the security and justice procurement authorities shall designate the public servants responsible for managing the requests made to the concession holders and receiving the corresponding information, by means of agreements published in the Official Gazette of the Federation. This delegation is published whenever there is a change in the designated public servants and/or new appointments.

Requests

Metadata Requests	2024
N° of request received	12,172
N° of rejected requests	686
N° of accesses affected	23,000

Content blocking and restriction

Legal framework

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

Competent authorities

- Not applicable.

Requests

Blocking Requests	2024
N° of requests received	N.A.
N° of rejected requests	N.A.
N° of urls affected	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

Suspensions Requests	2024
N° of requests received	N.A.
N° of rejected request	N.A.
N° of accesses affected	N.A.

Spain

Lawful interceptions of communications

Legal framework

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

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

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

    In the latter case, it will be necessary that the public administration has jurisdiction as regards security issues or for the provision of the public services affected by the abnormal functioning of the service or the network of electronic communications. In the event that the procedure is initiated at the request of an administration other than that of the State, the latter shall be deemed an interested party and may prepare a report prior to the final resolution."

  - Article 81(1): "Prior to the beginning of the sanctioning procedure, the cessation of the alleged infringing activity may be ordered by the competent body of the Ministry of Economy and Enterprise, by resolution without prior hearing, where there are reasons of overriding urgency based on any of the following assumptions:

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

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

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

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

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

Competent authorities

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

Requests

Interceptions	2024
N° of requests received	26,704
N° of rejected request	3,103
N° of accesses affected	9,146

Access to metadata

Legal framework

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

Competent authorities

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

Requests

Metadata Requests	2024
N° of request received	199,003
N° of rejected requests	8,906
N° of accesses affected *	0

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

Content blocking and restriction

Legal framework

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

Competent authorities

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

Requests

Blocking Requests	2024
N° of requests received	320
N° of rejected requests	8
N° of urls affected	16,127
16027 URL blocked, 100 URL unblocked	
Breakdown of petitions according to local legislation (e.g. for child pornography, intellectual property, etc...).	
Intellectual Property Crimes Medication Illegal Gambling	

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

Suspensions Requests	2024
N° of requests received	N.A.
N° of rejected request	N.A.
N° of accesses affected	N.A.

Uruguay

Lawful interceptions of communications

Legal framework

- Constitution of the Republic, Article 28.
- Law 19574, Article 62.
- Decree 1/1113 of 13 March 2014.
- Decree 359/021 of 26 October 2021.

Competent authorities

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

Requests

Interceptions	2024
N° of requests received *	4,124
N° of rejected request **	48
N° of accesses affected	4,076

* This total includes interventions, extensions of interventions, measures that were rejected and canceled (it is an order issued by the Judge requesting the cancellation of an extension that is in progress).

** The rejected measures correspond to the extensions that were requested after the deadline of the original intervention had expired.

Access to metadata

Legal framework

- Constitution of the Republic, Article 28.
- Law 19574, Article 62.
- Decree 1/1113 of 13 March 2014.
- Decree 359/021 of 26 October 2021.

Competent authorities

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

Requests

Metadata Requests	2024
N° of request received	9,251
N° of rejected requests *	0
N° of accesses affected	9,251

* *All request received complied with the applicable legality.*

Content blocking and restriction

Legal framework

- Law 19,535 of 25 September 2017.
- Decree 306/2017 regulated the provisions of Articles 244 and 245 of Law 19,535, 21/12/2017.
- Law 19,924 article 712.- Decree 345/2022.

Competent authorities

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

The dissemination of television services for subscribers through the Internet or similar network, for commercial purposes. by a natural or legal person who is not authorized to offer said signals, in violation of the provisions of Laws No. 9,739, of 17 December 1937 (Copyright Law) and No. 17,616. of 10 January 2003, and its amendments. may be administratively sanctioned. For these purposes, the Communications Services Regulatory Unit (URSEC) is empowered to adopt sanctioning and preventive measures in accordance with the provisions below and the regulations issued from time to time by the Executive Branch (Article 712 — Law 19,924).

Requests

Blocking Requests	2024
N° of requests received	50
N° of rejected requests	0
N° of urls affected	307
Breakdown of petitions according to local legislation (e.g. for child pornography, intellectual property, etc...).	
Intellectual property (sports events) and online gambling.	

Geographical or temporary suspension of the service

Legal framework

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

Competent authorities

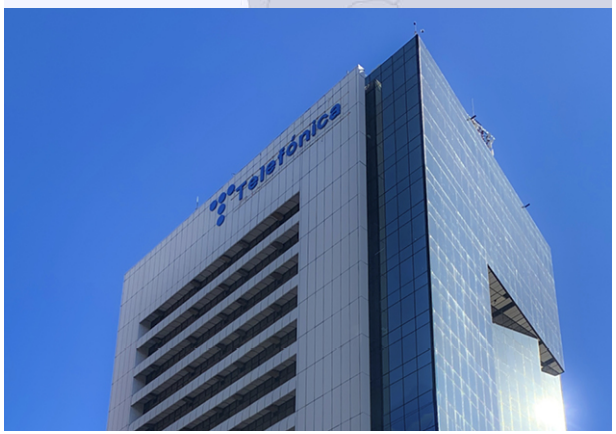
- Ministry of the Interior (Executive Branch).

It is clarified that it is not a blocking required of the operator or carried out by it (the blocking is carried out by the Ministry of the Interior itself). The Ministry of the Interior simply informs the operator that the Ministry itself has blocked the service to certain mobile phones (preventing traffic from entering its central office) so that we can inform customers in case of query.

Requests

Suspensions Requests	2024
N° of requests received	15
N° of rejected request	0
N° of accesses affected	984

Venezuela



Lawful interceptions of communications

Legal framework

- Organic Criminal Procedure Code, Article 205, 206 and 207.
- Decree with Rank, Value and Force of 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, prior authorization of the competent judge.
- Police corps duly empowered to exercise powers in criminal investigations (upon the request to the Public Prosecutor and the authorisation of the corresponding judge).
- The Scientific and Criminal Investigation Service Corps (CICPC) in the cases established by the laws.

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.
- State security bodies that have been granted investigative powers in a criminal investigation.

Content blocking and restriction

Legal framework

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

Competent authorities

- National Telecommunications Commission (CONATEL).

Geographical or temporary suspension of the service

Legal framework

- Organic Law on Telecommunications, Article 5.

Competent authorities

- National Telecommunications Commission (CONATEL).

Glossary

Concept	Explanation
Competent Authority	Judges and courts, state security forces and bodies and other administrations or governmental bodies that are empowered by the law to make the requests relevant to this report. The competent Authorities may vary according to the type of request and the applicable legislation in each of the countries.
Personal Data	Personal data means any information which refers to an identified or identifiable person, such as his or her name and address, the recipients of his or her communications, the location, the content of the communications, the traffic data (days, time, recipients of the communications, etc.).
Location Data	The location data may refer to the latitude, longitude and altitude of the user's terminal equipment, the direction of travel, the level of accuracy of the location information, the identification of the network cell in which the terminal equipment is located at a certain moment or the time at which the location information has been recorded.
Traffic Data	Any data processed for the purposes of conducting communication through an electronic communications network or for invoicing purposes.
IMEI	These initials stand for International Mobile Equipment Identity. It has a serial number which physically identifies the terminal. The IMEI enables the operator to identify terminals which are valid and, therefore, can connect to the network.
IMSI	These are the initials which stand for International Mobile Subscriber Identity. It is the identifier of the line or service. This number is used to route calls and to obtain the country or network to which it belongs.

Concept	Explanation
Major Events	There are certain situations of force majeure which may lead to the following actions: **1. Service restriction or denial** (including SMS, voice, email, voicemail, internet and other services) entailing limitation of freedom of expression. Examples: • Restricting or denying services on a national scale. • Restriction or denial of access to a website/ websites for political reasons (such as Facebook pages, news websites such as bbc.co.uk, the opposition party's websites prior to elections or human rights groups' websites). • Specific shutdown of any kind of telecommunications services, resulting from political causes (e.g., concerning a small number of cells). • Denying certain clients access to specific services or networks in order to limit said individuals' legitimate freedom of expression. **2. Network shutdown/access control.** Examples: • Total shutdown of a national network. • Access control involving a specific area or region, motivated by political reasons. **3. Legally unfounded interceptions.** • Situations in which the authorities intercept communications without any legal grounds for reasons of *force majeure*. **4. Communications imposed by the authorities.** Examples: • Sending politically motivated messages/communications to our customers on behalf of governments or government agencies. **5. Substantial operational changes.** Examples: • Substantial operational or technical changes or change proposals concerning surveillance services (such as data access, retention or interception) aimed at reducing the operator's control in terms of supervising such activities (e.g., procedural changes allowing direct access on the part of a governmental agency/ government). • A procedural change to establish widespread surveillance. **6. Substantial legal changes.** (substantial changes, or proposed changes, to laws providing governmental authorities with more power to impose requests on operators). Example: • Changes in the communication interception laws.

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

Telefónica