COMMUNICATIONS TRANSPARENCY REPORT

2025

TABLE OF CONTENTS

INTRODUCTION AND SCOPE

América Móvil, S.A.B. de C.V. (together with its subsidiaries, "AMX") remains steadfast in its commitment to the protection of the fundamental rights to privacy and freedom of expression as a means for fostering the development of a better-informed society.

We strive to safeguard our customers' rights to the protection of their personal data and the privacy of their communications. Our efforts in this regard have contributed significantly to our ability to preserve our customers' and investors' trust in our Company and to keep intact the reputation by which we have been characterized since the inception of our international operations.

Our Communications Transparency Report 2025 (this "**Report**") contains a detailed description of our policies for acknowledging, processing, reviewing and addressing the inquiries and orders received by our operating subsidiaries from Competent Authorities[1] throughout the year in each of the countries in which we operate. Our operating subsidiaries are tasked with serving as benchmarks at both the local and international levels when it comes to protecting and safeguarding the information they gather and to complying with the laws relating to government investigations and the administration of justice, among other things.

This annual update contains statistical information, by country and region, about all of the inquiries and orders that we received from Competent Authorities in 2025 in the jurisdictions in which we operate and that we processed, reviewed and either addressed or refused to address, or complied or refused to comply with, including all the inquiries received from foreign government agencies that we determined to be in compliance with the applicable requirements and, thus, warranting of action on our part in accordance with the applicable law. It should be noted, however, that the laws in effect in each of the jurisdictions in which we operate stipulate that we may not disclose the nature of any information we may provide to the Competent Authorities in response to their inquiries.

Within this context, this Report is intended to serve as a consultation and reference resource for identifying the applicable statutes and the types of inquiries and orders received by our local subsidiaries in each of the countries in which we operate.

[1] We define "Competent Authority" as any government entity upon which the laws of the relevant jurisdiction confer the power and authority to compel telecommunications carriers (whether directly or upon a court order or the satisfaction of certain other requirements) to cooperate in such entity's efforts in connection with the enforcement of security measures and the administration of justice.

OPERATIONAL TRANSPARENCY FRAMEWORK

At América Móvil, we are committed to the protection of human rights and freedom of expression. Thus, we only turn over information to the Competent Authorities where required by statute and subject to the satisfaction of the requirements set forth in the applicable laws of the relevant jurisdiction.

We have established stringent security protocols and implemented exacting strategies and procedures for complying with our disclosure obligations and ensuring that any information we provide to such effect is kept confidential.

Our comprehensive security strategy, which is based on three core values that are deeply ingrained in our operations, namely (a) **Integrity**, (b) **Availability** and (c) **Confidentiality** encompasses (i) cybersecurity, (ii) data privacy and (iii) communications privacy[2].

In addition, we use a combination of data processing platforms that trigger data retrieval and data enhancement processes in an agile and transparent manner, to ensure that all inquiries and orders are addressed in a prompt and timely fashion. We use IT tools to manage our customers' data in a systematic and structured manner, perform a number of data classification processes and combine, structure or export various types of reports in a single file, as needed.

For a breakdown of the inquiries we received, reviewed, processed and either addressed or refused to address, or complied or refused to comply with in each of the countries and regions in which we operate in Latin America, see "ORFI and SRO Statistics" below.

As a supplemental tool for assessing the inquiries and orders we receive from Competent Authorities, each such inquiry and order undergoes a comprehensive due diligence review process. This process varies depending on the laws in effect in the relevant jurisdiction, which generally stipulate that our obligation to turn over any information (e.g., any personal data pertaining to our customers or any communications-related data) or intervene in any communication (e.g., telephone tapping or geolocation) shall be enforceable solely and exclusively upon receipt of an Official Request for Information ("**ORFI**") or Service Restriction Order ("**SRO**"), as applicable, of a Competent Authority. Our local subsidiaries in member states of the European Union (i.e., Austria, Bulgaria, Croatia and Slovenia) are also subject to the applicable (supranational) laws adopted by that community.

[2] For additional information regarding our policies and procedures in Chile and Peru, see *Política de Requerimientos and Protocolo de Atención de Levantamiento del Secreto de las Telecomunicaciones*, respectively, which are available at https://www.clarochile.cl/portal/cl/recursos_contenido/pdf/1773163683379-Informe_de_Transparencia_2025_ClaroVtr.pdf and https://www.claro.com.pe/portal/pe/recursos_contenido/pdf/1771621459518-Informe_Anual_LST_2025.pdf, respectively.

Every ORFI and SRO must (i) be duly grounded in fact and law, (ii) pertain to matters within the jurisdiction of its issuer and provide assurance to the effect that private communications will be kept secret (upon verification of which our relevant subsidiary, if a telecommunications carrier (as denoted by its name), will trigger its procedure for addressing such ORFI or SRO in accordance with the laws of its home country and with our Privacy and Personal Data Protection Policy, irrespective of whether the ORFI or SRO was delivered to it by electronic means or in physical form), and (iii) have been issued by a Competent Authority. Consequently, we will never provide any information whatsoever to any person or entity through unofficial channels.

We will not fulfill any ORFI or comply with any SRO which does not meet all of the aforementioned criteria or which is in violation of the applicable law (for example, if it is unjustified or unreasonably burdensome). This means that we will not acknowledge any request for information by any person (i.e., any individual or entity, whether public or private) other than a Competent Authority. To minimize these occurrences, our subsidiaries in Peru and Colombia provide training, on a regular basis to public officials designated by the Competent Authorities, on the development of best practices guidebooks to facilitate the improvement, standardization and strengthening of our procedure for acknowledging, reviewing, processing and addressing their ORFIs and SROs[3].

We have developed a stringent set of security protocols, established specific criteria and assigned dedicated teams to ascertain the validity of each and every ORFI and SRO we receive from a Competent Authority.

We only acknowledge, process and address those ORFIs and SROs that meet the procedural requirements set forth in the laws of the relevant jurisdiction and that are delivered to us through official communication channels. Accordingly, this Report is exclusive of the instances in which the Competent Authorities accessed our systems to retrieve information directly pursuant to their statutory powers, as was the case in Brazil, Colombia, Costa Rica, Ecuador, El Salvador, Honduras and Nicaragua.

As required by law, in view of the confidential and/or secret nature of all judicial and administrative proceedings, we do not give our customers notice of our receipt of any ORFI or other inquiry about them, or of any SRO relating to them[4]. In addition, we do not publish in any of our websites or otherwise disclose the contents of any ORFI or SROs we may have received, or the nature of any information we may have provided to third parties for public record-keeping purposes in response to an ORFI. However, the contracts for our post-paid service plans and the terms and conditions for our pre-paid service plans in each of the countries in which we operate set forth the events in which the services provided thereunder may be restricted, blocked, suspended or discontinued.

[3] In 2025, our Peruvian subsidiary provided training to 210 public prosecutors and 39 police officials, which contributed to a 38.1% decrease in the number of ORFIs and SROs that we refused to fulfill or comply with as compared to 2024. Our subsidiary in Colombia held 6 training sessions that were attended by 9 judges and 452 judicial investigators assigned to the Attorney General's Office, the Directorate of Criminal Investigation and Interpol (*Dirección de Investigación Criminal e Interpol*, or DIJIN) and Unified Action Groups for Personal Liberty (*Grupos de Acción Unificada por la Libertad Personal*, or GAULA).

For further information regarding Peru, please refer to the website: https://www.claro.com.pe/portal/pe/recursos_contenido/pdf/1771621459518-Informe_Anual_LST_2025.pdf.

[4] Except in Peru, where we are required to give our customers notice of any personal information about them that we may have provided in connection with any civil, labor or family court proceedings.

The privacy of our customers' communications is one of our paramount concerns. Accordingly, we abide by the following principles:

i. No one may listen to or monitor any conversation, data transmission or other type of communication, nor disclose its existence or content, except upon a duly substantiated written order of a Competent Authority;

ii. No one may turn over personal data of others, geolocate a mobile device, block or impose service restrictions on a telephone line or keep call detail records, except where required by law and subject to the receipt of an ORFI or SRO of a Competent Authority that is duly grounded in fact and law.

iii. No one may engage in the prioritization or throttling of any traffic, application, protocol or content. All of our operations comply with the standards relating to net neutrality and zero-rating. Under no circumstance may any application traffic be given priority over other network traffic.

The Competent Authorities or competent courts in Brazil, Colombia, Chile, Ecuador, Peru, the Dominican Republic and Uruguay may require our local subsidiaries in those countries, upon the issuance of an SRO, to block or restrict the access to certain types of content, including child pornography, content whose use constitutes copyright infringement, and gambling).

The list of URLs that have been blocked or blacklisted in Chile is available at the Chilean Supreme Court's website, (https://www.pjud.cl/). Our subsidiaries in all other countries maintain their own internal lists of blocked or blacklisted websites, which, consistent with our information classification policies and with the applicable laws, are not disclosed to the public.

If you have any question in connection with the above, please contact us at privacidad@americamovil.com

PROCEDURE FOR ADDRESSING ORFIs AND SROs

This section contains a detailed description of the procedure we employ for addressing the ORFIs and SROs we receive (whether by electronic means or in physical form) from Competent Authorities[5] in view of our cooperation obligations thereto. Such procedure is substantially identical from a regulatory standpoint in all of the countries in which we operate.

We will regard as valid any ORFI or SRO which meets the procedural requirements set forth in the applicable laws of the relevant country, complies with the statutes relating to the protection of personal data and the privacy and communications, and is delivered to us in writing. For a list of the applicable statutes in effect as of the date hereof in each of the countries in which we operate, see "Regulatory Framework" below.

Upon receipt of an ORFI (which may relate to a single matter or to several matters) or SRO, the relevant area performs a review and assessment thereof in accordance with a stringent set of internal procedures that are designed to protect the rights of our customers and preserve the confidentiality of their personal data. Such procedures entail the following:

- Legal analysis[6] of the ORFI or SRO, to ascertain its validity and the subject matter jurisdiction of the issuer;
- Upon verification of the satisfaction of all the applicable legal requirements, the activation of our data gathering processes to gather the information requested by the Competent Authority;
- Preparation of a formal response to the Competent Authority, either fulfilling or complying or refusing to fulfill or comply with the ORFI or SRO, as the case may be; and
- Delivery of AMX's response to the Competent Authority by any such means as we may determine necessary and adequate to preserve the integrity and confidentiality of the information contained therein, as the case may be[7].

In Latin America, the period of time allowed by the applicable laws to fulfill an ORFI or comply with an SRO of a Competent Authority varies from one country to another and ranges from 24 hours (e.g., in Mexico and El Salvador) to 15 business days (e.g., in Brazil and Colombia)[8].

[5] For these purposes, Competent Authority includes any government entity vested with judicial or administrative powers under the laws of the relevant country. However, we employ one and the same procedure for addressing all ORFIs and SROs irrespective of the nature of the powers of their issuers.

[6] Defined as the process for determining whether an ORFI or SRO was issued by one of the government agencies identified in "Regulatory Framework" below, relates to one or more of the conducts described therein and identifies the statutes on which it is grounded.

[7] In El Salvador, only, the Competent Authorities are responsible for picking up the requested information at our office.

[8] Under the laws of Argentina, Chile, Ecuador, Guatemala, Honduras and the Dominican Republic, the period of time available for fulfilling an ORFI or complying with an SRO is determined by the Competent Authority on a case-by-case basis and stipulated in the relevant ORFI or SRO. In Nicaragua, neither the applicable laws nor the ORFIs or SROs provide for any specific period of time for responding to the latter. Lastly, in Costa Rica, although no specific statutory provision on response times exist, we have entered into an agreement with the Competent Authorities providing for response periods of between 4 hours and 3 business days, depending on the type of conduct under investigation.

In the countries in which we operate in Europe, the period of time available for fulfilling an ORFI or complying with an SRO depends on the subject matter thereof and the laws of the relevant country. Generally, ORFIs, and SROs may be enforceable either immediately upon receipt of a court order in the event of an emergency, or within a period up to several business days in the case of ordinary requests for the disclosure of data.

We will refuse to fulfill or comply with any ORFI or SRO which does not satisfy the requirements set forth in the applicable laws and will notify the Competent Authority that issued such ORFI or SRO the legal and factual basis for such refusal. We will deliver such notice to such Competent Authority within the relevant periods of time specified in the preceding paragraph. Under the applicable laws of the countries in which we operate, the validation or the refusal or rejection of an ORFI or SRO shall be deemed definitive and irrevocable.

The laws of the countries in which we operate authorize us to address ORFIs issued by foreign government agencies, provided that such ORFIs satisfy the formalities and comply with all the procedural requirements that are necessary for foreign government documents generally to be valid.

The following chart illustrates the procedure described in this section.

AMX'S PROCEDURE FOR ADDRESSING ORFIs and SROs

A Competent Authority delivers an ORFI/SRO to

By electronic means

In physical form

AMX´s Central Desk acknowledges receipt

The ORFI/SRO is forwarded to an in-house attorney

Ascertains:

Legal and factual grounds Jurisdiction

Verifies the authenticity of the seals and the satisfaction of the requisite formalities

Reviews the ORFI/SRO

Lawful

Prepares a response fulfilling/acquiescing to the ORFI/SRO

Assembles the file containing the response/report

Delivers the response by electronic means and/or in physical form

Unlawful

Prepares a response declining to fulfill the ORFI

Restricts the service

REGULATORY FRAMEWORK

Every ORFI or SRO must comply with all the formalities required by the applicable laws. We will decline to fulfill any ORFI or comply with any SRO which (i) does not specify the legal grounds and factual basis on which it is grounded; (ii) does not pertain to matters within the subject matter jurisdiction of the requesting authority; or (iii) is not issued by a Competent Authority.

The following table sets forth (i) the statutes pursuant to which we are required to cooperate with the Competent Authorities in connection with security matters and the administration of justice, (ii) the scope of our obligations under and the types of actions that we may be required to take pursuant to such statutes, and (iii) the Competent Authorities that are authorized to issue the requisite ORFIs or SROs.

MEXICO	
Applicable statutes	• Political Constitution of the United Mexican States (*Constitución Política de los Estados Unidos Mexicanos*) • Law on Telecommunications and Broadcasting (*Ley en Materia de Telecomunicaciones y Radiodifusión*) • Federal Law on the Protection of Personal Data Held by Private Persons (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) • National Criminal Procedural Code (*Código Nacional de Procedimientos Penales*) • Organic Law of the Judicial Branch of the Federation (*Ley Orgánica del Poder Judicial de la Federación*) • Federal Law Against Organized Crime (*Ley Federal Contra la Delincuencia Organizada*) • General Law on the Prevention and Punishment of Kidnapping, Enacted Under Article 73(XXI) of the Political Constitution of the United Mexican States (*Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro, Reglamentaria de la fracción XXI del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos*) • Guidelines for the Provision of Collaboration in Connection with Security and Justice Matters (*Lineamientos de Colaboración en Materia de Seguridad y Justicia*)
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Law on Telecommunications and Broadcasting, Article 183(I), (II)(a)-(h) and III • **Real-time geolocation of mobile devices:** » Law on Telecommunications and Broadcasting, Article 183(I) » National Criminal Procedural Code, Article 303 » Guidelines for the Provision of Collaboration in Connection with Security and Justice Matters, Fifteenth Guideline • **Interception of private communications:** » National Criminal Procedural Code, articles 291-294 and 301 » National Security Law (*Ley de Seguridad Nacional*), articles 34-42 » General Law on the Prevention and Punishment of Kidnapping, Enacted Under Article 73(XXI) of the Political Constitution of the United Mexican States, Article 24 » Federal Law Against Organized Crime, articles 16-21 and 26 • **Discontinuance of telecommunications services:** » Law on Telecommunications and Broadcasting, Article 120 • **Blocking of communication lines being used in connection with unlawful activities:** » Law on Telecommunications and Broadcasting, Article 121
Competent Authorities	• Heads of the security agencies and law enforcement authorities, and the public officials designated thereby

CENTRAL AMERICA[9]

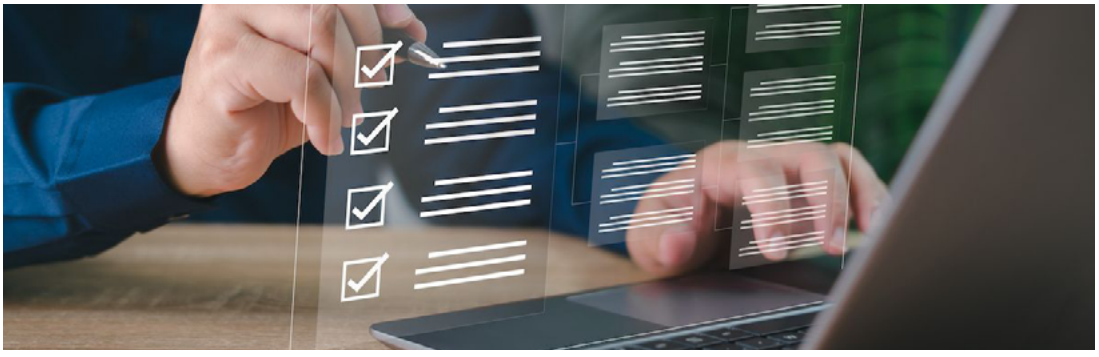
COSTA RICA	
Applicable statutes	• Law Against Organized Crime (*Ley Contra la Delincuencia Organizada*), or Law No. 8754 • General Telecommunications Law (*Ley General de Telecomunicaciones*), or Law No. 8642 • Law on the Registration, Seizure and Examination of Private Documents and the Interception of Communications (*Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones*), or Law No. 7425 • Criminal Procedural Code (*Código Procesal Penal*), or Law No. 7594
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Law Against Organized Crime, or Law No. 8754, articles 15-17 » General Telecommunications Law, or Law No. 8642, Article 18 bis • **Real-time geolocation of mobile devices:** » Law on the Registration, Seizure and Examination of Private Documents and the Interception of Communications, or Law No. 7425, articles 9, 10, 20 and 23 » Law Against Organized Crime, or Law No. 8754, Article 15 • **Interception of private communications:** » Law on the Registration, Seizure and Examination of Private Documents and the Interception of Communications, or Law No. 7425, articles 9, 10, 13, 20, 23, 26 and 28 • **Discontinuance of telecommunications services:** » Criminal Procedural Code, or Law No. 7594, articles 201, 289 and 295 » Law on the Registration, Seizure and Examination of Private Documents and the Interception of Communications, or Law No. 7425, articles 1, 2, 3, 14 and 20 • **Blocking of communication lines being used in connection with unlawful activities:** » Law on the Registration, Seizure and Examination of Private Documents and the Interception of Communications, or Law No. 7425 » General Telecommunications Law, or Law No. 8642, articles 49(4), 67(C) and 68(c) » Criminal Procedural Code, or Law No. 7594, articles 289 and 295
Competent Authorities	• Heads of the security agencies and law enforcement authorities, and the public officials designated thereby » Public prosecutors (*Ministerio Público*) » General Directorate of the Agency for Judicial Investigation (*Dirección General del Organismo de Investigación Judicial*, or OIJ) » Center for the Judicial Interception of Communications (*Centro Judicial de Intervenciones de las Comunicaciones*, or CJIC) » Costa Rican Drug Institute (*Instituto Costarricense de Drogas*, or ICD) » Judicial Branch (i.e., the judges authorized to issue SROs)

EL SALVADOR	
Applicable statutes	• Constitution of the Republic of El Salvador (*Constitución de la República de El Salvador*) • Telecommunications Law (*Ley de Telecomunicaciones*) • Special Law on the Interception of Telecommunications (*Ley Especial para la Intervención de las Telecomunicaciones*) • Cybersecurity and Information Security Law (*Ley de Ciberseguridad y Seguridad de la Información*) • Law on the Protection of Personal Data (*Ley de Protección de Datos Personales*) • Organic Law of the National Lottery for Welfare (*Ley Orgánica de la Lotería Nacional de Beneficencia*)
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Telecommunications Law, articles 42-A, 42-B and 42-E » Special Law on the Interception of Telecommunications, articles 43 and 47 • **Maintenance of a user (including pre-paid customers) registry available for inspection by the Competent Authorities:** » Telecommunications Law, Article 30 • **Geolocation of mobile devices:** » Telecommunications Law, Article 42-A » Special Law on the Interception of Telecommunications, articles 43 and 47 • **Interception of private communications:** » Constitution of the Republic of El Salvador, Article 24 » Special Law on the Interception of Telecommunications, Article 47 • **Discontinuance of telecommunications services:** » Special Law Against Extortion (*Ley Especial Contra el Delito de Extorsión*), Article 13 • **Submission of cybersecurity and data security reports upon request by the Competent Authorities:** » Cybersecurity and Information Security Law, Article 6 • **IP address, DNS or URL blocking:** » Organic Law of the National Lottery for Welfare, Article 16(I)
Competent Authorities	• Judicial Branch (judges) • Public prosecutors (*Ministerio Público*) • Governing Board (*Junta Directiva*) of the National Lottery for Welfare

[9] Includes our operations in Costa Rica, El Salvador, Guatemala, Honduras and Nicaragua.

GUATEMALA	
Applicable statutes	• Political Constitution of the Republic of Guatemala (*Constitución Política de la República de Guatemala*) • Criminal Procedural Code (*Código Procesal Penal*), or Decree No. 51-92 • Law Against Organized Crime (*Ley Contra la Delincuencia Organizada*), or Decree No. 21-2006, and the Regulations issued thereunder, or Government Resolution No. 158-2009 • Law on the Forfeiture of Assets (*Ley de Extinción de Dominio*), or Decree No. 55-2010 • Tax Code (*Código Tributario*), or Decree No. 6-91 • Law on Mobile Devices (*Ley de Equipos Terminales Móviles*), or Decree No. 8-2013
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Law Against Organized Crime, or Decree No. 21-2006, Article 48 (Interceptions) » Regulations on the Use of Special Investigative Methods (*Reglamento para la Aplicación de los Métodos Especiales de Investigación*), or Governmental Resolution No. 158-2009 » Law on the Forfeiture of Assets, or Decree No. 55-2010 » Tax Code, or Decree No. 6-91, articles 17 (Duty of collaboration, 30A (Third-party data), 98 (Revenue administration activities), 112 (Obligations of the responsible parties and taxpayers), and 112A (Other Obligations of the responsible parties and taxpayers) • **Real-time geolocation of mobile devices:** » Law Against Organized Crime, or Decree No. 21-2006 » Regulations on the Use of Special Investigative Methods, or Governmental Resolution No. 158-2009 • **Interception of private communications:** » Law Against Organized Crime, or Decree No. 21-2006, Article 48 (Interceptions) » Regulations on the Use of Special Investigative Methods, or Governmental Resolution No. 158-2009 • **Blocking of services used in a device whose IMEI is blacklisted:** » Law on Mobile Devices, or Decree No. 8-2013, Article 16 • **Blocking of communication lines being used in connection with unlawful activities:** » Law on Mobile Devices, or Decree No. 8-2013, Article 17
Competent Authorities	• Public prosecutors (*Fiscales del Ministerio Público*) • Criminal court judges • The highest tax authority

HONDURAS	
Applicable statutes	• Constitution of the Republic of Honduras (*Constitución de la República de Honduras*) • Framework Law for the Telecommunications Sector (*Ley Marco del Sector de Telecomunicaciones*) • Special Law on the Interception of Private Communications (*Ley Especial de Intervención de las Comunicaciones Privadas*) • Criminal Code (*Código Penal*) • Special Law on the Office of the Public Prosecutor (*Ley Especial del Ministerio Público*) • Criminal Procedural Code (*Código Procesal Penal*) • Civil Procedural Code (*Código Procesal Civil*) • Regulations Under the Law for the Telecommunications Sector (*Reglamento de la Ley del Sector Telecomunicaciones*)
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Constitution of the Republic of Honduras, Article 100 » Criminal Procedural Code, Article 273 • **Interception of private communications:** » Constitution of the Republic of Honduras, Article 100 » Criminal Procedural Code, articles 147, 217 and 273 » Framework Law for the Telecommunications Sector, articles 3 and 41 » Special Law on the Interception of Private Communications, articles 8, 10, 12, 37, 38, 39, 40, 41 and 43 • **Discontinuance of telecommunications services:** » Criminal Procedural Code, articles 273 and 147 • **Blocking of communication lines being used in connection with unlawful activities:** » Criminal Procedural Code, articles 273 and 147
Competent Authorities	• Heads of the security agencies and law enforcement authorities, and the public officials designated thereby: » Public prosecutors (*Ministerio Público*) » Judicial Branch » Ministry of Security (Secretaría de Seguridad), through its Directorate of Disciplinary Police Matters (*Dirección de Asuntos Disciplinarios* Policiales, or DIDADPOL) » Directorate of Police Investigations (*Dirección Policial de Investigaciones*)



NICARAGUA	
Applicable statutes	• Political Constitution of the Republic of Nicaragua (*Constitución Política de la República de Nicaragua*) • Criminal Code (*Código Penal*), or Law No. 641 • Family Code (*Código de Familia*), or Law No. 870 • Criminal Procedural Code (*Código Procesal Penal*), or Law No. 406 • Law on the Prevention, Investigation and Prosecution of Organized Crime and the Administration of Seized, Confiscated and Abandoned Property (*Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados*), or Law No. 735 • Special Law on Cybercrimes (*Ley Especial de Ciberdelitos*), or Law No. 1042 • Organic Law of the Judicial System of the Republic of Nicaragua (*Ley Orgánica del Sistema Judicial de la República de Nicaragua*), or Law No. 1244 • Rules for the Preservation of Data and Information (*Normativa para Preservación de Datos e Información*), or Administrative Resolution No. 001-2021
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Rules for the Preservation of Data and Information, or Administrative Resolution No. 001-2021, articles 1, 4 and 6 » Criminal Code, or Law No. 641, Article 462 » Criminal Procedural Code, or Law No. 406, Article 246 » Law on the Prevention, Investigation and Prosecution of Organized Crime and the Administration of Seized, Confiscated and Abandoned Property, or Law No. 735, articles 42 and 65 » Special Law on Cybercrimes, or Law No. 1042, articles 36, 37, 39, 40 and 42 » Family Code, or Law No. 870, Article 257 » Rules for the Preservation of Data and Information (*Normativa para Preservación de Datos e Información*), or Administrative Resolution No. 001-2021 • **Real-time geolocation of mobile devices:** » Law on the Prevention, Investigation and Prosecution of Organized Crime and the Administration of Seized, Confiscated and Abandoned Property, or Law No. 735, articles 42 and 65 » Special Law on Cybercrimes, or Law No. 1042, Article 39.12 • **Interception of private communications:** » Criminal Procedural Code, or Law No. 406, articles 213 and 214 » Law on the Prevention, Investigation and Prosecution of Organized Crime and the Administration of Seized, Confiscated and Abandoned Property, or Law No. 735, articles 42 and 65 » Special Law on Cybercrimes, or Law No. 1042, Article 39 • **Discontinuance of telecommunications services:** » Criminal Procedural Code, or Law No. 406, articles 246 and 230(8) and (11) » Organic Law of the Judicial Branch of the Republic of Nicaragua (*Ley Orgánica del Poder Judicial de la República de Nicaragua*), or Law No. 260, Article 12 » Special Law on Cybercrimes (*Ley Especial de Ciberdelitos*), or Law No. 1042 • **Blocking of communication lines being used in connection with unlawful activities:** » Criminal Procedural Code, or Law No. 406, articles 246 and 230(8) and (11) » Criminal Code, or Law No. 641, Article 462 » Special Law on Cybercrimes (*Ley Especial de Ciberdelitos*), or Law No. 1042
Competent Authorities	• Judicial and police authorities

ANDEAN REGION[10]

CHILE	
Applicable statutes	• Political Constitution of the Republic of Chile (*Constitución Política de la República de Chile*) • Criminal Procedural Code (*Código Procesal Penal*) • Regulations on the Interception and Recording of Telephone Conversations and Other Forms of Telecommunications (*Reglamento sobre interceptación y grabación de comunicaciones telefónicas y otras formas de telecomunicación*), or Decree No. 142 of 2005, issued by the Ministry of Transportation and Telecommunications (*Ministerio de Transporte y Telecomunicaciones*) • Decree-Law No. 211, Which Sets Forth the Rules for the Defense of Free Competition (*Decreto Ley No. 211 que Fija Normas para la Defensa de la Libre Competencia*) • Decree No. 198 of 2025, Amending Decree No. 142 of the Ministry of Transportation and Telecommunications
Scope of our cooperation obligations / required actions	• **Real-time geolocation of mobile devices:** » Criminal Procedural Code, articles 222 and 224 » Decree-Law No. 211, Which Sets Forth the Rules for the Defense of Free Competition, Article 39(n)(3) and (4) • **Interception of private communications:** » Political Constitution of the Republic of Chile, Article 19(4) and (5) » Regulations on the Interception and Recording of Telephone Conversations and Other Forms of Telecommunications, or Decree No. 142 of 2005, articles 1-8, 222 and 224 » Decree-Law No. 211, Which Sets Forth the Rules for the Defense of Free Competition, Article 39(n)(3) and (4)
Competent Authorities	• The following courts of the Judicial Branch: » Illustrious Courts of Appeals (*Ilustrísimas Cortes de Apelaciones*) » The Most Excellent Supreme Court (*Excelentísima Corte Suprema*) » Civil, labor, family and guarantee courts » Public prosecutors (*Ministerio Público*) » Office of the National Economic Prosecutor (*Fiscalía Nacional Económica*)

[10] Includes our operations in Chile, Colombia, Ecuador and Peru.

COLOMBIA	
Applicable statutes	• Political Constitution of Colombia (*Constitución Política de Colombia*) of 1991 • Criminal Procedural Code (*Código de Procedimiento Penal*), or Law 906 of 2004 • Law 1066 of 2006 • Law 1341 of 2009 • Law 1621 of 2013 • Decree 1704 of 2012 • Tax Statute (*Estatuto Tributario*)
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Political Constitution of Colombia, articles 15 and 250 » Criminal Procedural Code, or Law No. 906 of 2004, articles 235 and 236 » Law 1621 of 2013, Article 44 » Decree 1704 of 2012 » Tax Statute Law 1066 of 2006, articles 631 and 684 » Criminal Procedural Code, or Law 906 of 2004, articles 14, 244 and 246 » Code on Administrative Proceedings and Administrative Litigation (*Código de Procedimiento Administrativo y de lo Contencioso Administrativo*), or Law No. 1437 of 2011, articles 90 and 100 • **Real-time geolocation of mobile devices:** » Criminal Procedural Code, or Law 906 of 2004, Article 235 » Law 1621 of 2013, Article 44 » Decree No. 1704 of 2012, Article 5 • **Interception of private communications:** » Political Constitution of Colombia, Article 15 » Decree No. 1704 of 2012, Article 2 » Criminal Procedural Code, or Law 906 of 2004, Article 235 » Law 1621 of 2013, Article 44 » Decree 1078 of 2015, Chapter 6 "Regulations Under Article 52 of Law No. 1453 of 2011 on the Lawful Interception of Communications" • **Device and IMSI blocking:** » Decree 851 of 2024
Competent Authorities	• Attorney General of the Nation (*Fiscalía General de la Nación*), acting through the Judicial Police (*Policía Judicial*), subject to the prior authorization of a guarantees control judge (*juez de control de garantías*) • Heads of the security agencies and the public officials designated thereby • Judicial Branch • Department of Revenue and National Customs (*Dirección de Impuestos y Aduanas Nacionales*, or DIAN) • Governmental agencies authorized to collect biographical information Colombian Institute for the Families' Well-being (*Instituto Colombiano de Bienestar Familiar*, or ICBF), for purposes of the location of missing persons and the exercise of the self-enforcing powers of public entities • Administrative, disciplinary and tax authorities (such as the Office of the Comptroller General of the Republic (*Contraloría General de la República*), the internal control offices and the municipal and departmental ministries of finance)

ECUADOR	
Applicable statutes	• Constitution of the Republic of Ecuador (*Constitución de la República de Ecuador*) • Organic Telecommunications Law (*Ley Orgánica de Telecomunicaciones*) • Law on Public Security and the Security of the State (*Ley de Seguridad Pública y del Estado*) • Integrated Organic Criminal Code (*Código Orgánico Integral Penal*) • General Regulations Under the Organic Telecommunications Law (*Reglamento General a la Ley Orgánica de Telecomunicaciones*) • Concession Agreement
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Organic Telecommunications Law, articles 22(3) and (4), 24(13), (14) and (29), and 77 » General Regulations Under the Organic Telecommunications Law, articles 117,118, 119 and 120 » Concession Agreement, sections 36 and 41.9 » Integrated Organic Criminal Code, articles 230, 472, 476, 477, 477.1 and 477.2 » Organic Law on the Protection of Personal Data (*Ley Orgánica de Protección de Datos Personales*), Article 11 • **Real-time geolocation of mobile devices:** » Organic Telecommunications Law, Article 77 » General Regulations Under the Organic Telecommunications Law, articles 117,118 and 119 » Integrated Organic Criminal Code, articles 230, 472, 476, 477, 477.1 and 477.2 • **Interception of private communications:** » Organic Telecommunications Law, Article 77 » General Regulations Under the Organic Telecommunications Law, articles 118 and 119 » Concession Agreement, Section 41.9 » Regulations Relating to the Communications or Data Interception Subsystem (*Reglamento para el subsistema de Interceptación de comunicaciones o datos informáticos*), articles 4 and 5 » Integrated Organic Criminal Code, articles 230, 476, 477, 477.1 and 477.2 • **Discontinuance of telecommunications services:** » Constitution of the Republic of Ecuador, articles 164 and 165 » Concession Agreement, Section 34.7 • **Blocking of communication lines being used in connection with unlawful activities:** » Concession Agreement, Section 34.7
Competent Authorities	• Judges of competent jurisdiction • Office of the Attorney General (*Fiscalía General del Estado*) • Intelligence agencies (upon a court order) • Superintendency for the Protection of Personal Data (*Superintendencia de Protección de Datos Personales*) • Superintendency of Economic Competition (*Superintendencia de Competencia Económica*) • National Telecommunications Regulation and Control Agency (*Agencia de Regulación y Control de las Telecomunicaciones*, or ARCOTEL) • Internal Revenue Service (*Servicio de Rentas Internas*, or SRI), solely and exclusively within the limits of its jurisdiction

PERU	
Applicable statutes	• Amended and Restated Telecommunications Law (*Texto Único Ordenado de la Ley de Telecomunicaciones*), or Supreme Decree No. 013-93-TCC • Amended and Restated Regulations Under the Telecommunications Law (*Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones*), or Supreme Decree No. 020-2007-MTC • Criminal Procedural Code (*Código Procesal Penal*), or Legislative Decree No. 957 • Law that Empowers the Attorney General to Intercept and Control Private Communications and Documents Under Exceptional Circumstances (*Ley que Otorga Facultad al Fiscal para la Intervención y Control de Comunicaciones y Documentos Privados en Caso Excepcional*), or Law No. 27697 • Law That Amends Legislative Decree 1182 (*Ley que Modifica el Decreto Legislativo* 1182), or Law No. 32303 • Measures Intended to Safeguard the Right to the Inviolability and Secrecy of Telecommunications, to Protect Personal Data and to Regulate the Exercise of the Oversight and Control Powers of the Ministry of Transportation and Communications (*Norma que establece medidas destinadas a salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones y la protección de datos personales y regula las acciones de supervisión y control a cargo del Ministerio de Transportes y Comunicaciones*), or Ministerial Resolution No. 111-2009-MTC/03 • Resolution No. 000139-2025-CD/OSIPTEL • Resolution No. 134-2025-CD/OSIPTEL • Provisions Governing the Use of Telecommunications-related Data for the Identification, Location and Geolocation of Communication Devices Within the Context of the Fight Against Delinquency and Organized Crime (*Norma que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación en la lucha contra la delincuencia y el crimen organizado*), or Legislative Decree No. 1182 • Law on the Development of the Powers and Duties of the Supervisory Agency for Private Investment in Telecommunications (*Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones* - OSIPTEL), or Law No. 27336 • Legislative Decree that Amends the Provisions for the Resolution of Cases Involving Missing Vulnerable Persons Set Forth in Legislative Decree No. 1428, in Furtherance of the Search for Missing Persons (*Decreto que modifica el Decreto Legislativo No. 1428, que desarrolla medidas para atención de casos desaparición de personas en situación de vulnerabilidad, para fortalecer la búsqueda de personas desaparecidas*), or Legislative Decree No. 1603 • Legislative Decree No. 1611, otherwise known as the Legislative Decree That Sets Forth Special Measures for the Prevention and Investigation of Extortions and Other Related Crimes and Amends the Criminal Code Enacted Pursuant to Legislative Decree No. 635 and the Code of Criminal Procedure Enacted Pursuant to Legislative Decree No. 957 (*Decreto Legislativo que aprueba medidas especiales para la prevención e investigación del delito de extorsión y delitos conexos, así como la modificación del código penal, aprobado mediante Decreto Legislativo No. 635 y del Código Procesal Penal, aprobado por Decreto Legislativo No. 957*) • Article 13 of the Law for the Protection of Personal Data (*Ley de Protección de Datos Personales*), or Law No. 29733, including the Regulations issued thereunder pursuant to Supreme Decree No. 003-2013-JUS • Decree that Amends the Criminal Procedural Code Enacted Pursuant to Legislative Decree No. 957, to optimize the legal framework applicable to criminal investigations and to the intervention of the National Police and the Attorney General of Peru (*Decreto Legislativo que modifica el código procesal penal, aprobado por el decreto legislativo 957, para optimizar el marco legal que regula la investigación del delito y la intervención de la policía nacional del Perú y del Ministerio Público*), or Legislative Decree No. 1605
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Criminal Procedural Code, or Legislative Decree No. 957, articles 230 and 231 » Legislative Decree that Amends the Provisions for the Resolution of Cases Involving Missing Vulnerable Persons Set Forth in Legislative Decree No. 1428, in Furtherance of the Search for Missing Persons, or Legislative Decree No. 1603, Article 9 » Legislative Decree that Approves Special Measures for the Prevention and Investigation of Extortions and Other Related Crimes and Amends the Criminal Code Enacted Pursuant to Legislative Decree No. 635 and the Criminal Procedural Code Enacted Pursuant to Legislative Decree No. 957, or Legislative Decree No. 1611, Article 9 • **Real-time geolocation of mobile devices:** » Criminal Procedural Code, or Legislative Decree No. 957, articles 230 and 231 » Provisions Governing the Use of Telecommunications-related Data for the Identification, Location and Geolocation of Communication Devices Within the Context of the Fight Against Delinquency and Organized Crime, or Legislative Decree No. 1182, Article 4 and Second Provision of the Final Supplemental Provisions » Legislative Decree that Amends the Provisions for the Resolution of Cases Involving Missing Vulnerable Persons Set Forth in Legislative Decree No. 1428, in Furtherance of the Search for Missing Persons, or Legislative Decree No. 1603, Article 13 » Legislative Decree that Approves Special Measures for the Prevention and Investigation of Extortions and Other Related Crimes and Amends the Criminal Code Enacted Pursuant to Legislative Decree No. 635 and the Criminal Procedural Code Enacted Pursuant to Legislative Decree No. 957, or Legislative Decree No. 1611, Article 7 • **Interception of private communications:** » Political Constitution of Peru (*Constitución Política del Perú*), Article 2(10) » Amended and Restated Telecommunications Law, or Supreme Decree No. 013-93-TCC, Article 4 » Amended and Restated Regulations Under the Telecommunications Law, or Supreme Decree No. 020-2007-MTC, Article 13 » Regulations Under the Law that Provides for the Creation of the Financial Intelligence Unit - Peru (*Reglamento de la Ley que crea la Unidad de Inteligencia Financiera - Perú*), or Supreme Decree No. 020-2017-JUS, Article 4 » Criminal Procedural Code, or Legislative Decree No. 957, articles 230 and 231 » Law Against Organized Crime (*Ley Contra el Crimen Organizado*), articles 230 and 231 » Decree that Amends the Criminal Procedural Code Enacted Pursuant to Legislative Decree No. 957, to optimize the legal framework applicable to criminal investigations and to the intervention of the National Police and the Attorney General of Peru, or Legislative Decree No. 1605, Article 2 – Amendments to Articles 230 and 231 • **Preservation of the information and data collected as a result of the provision of telecommunication services:** » Legislative Decree No. 1182, Second Final Supplemental Provision • **Discontinuance of telecommunications services:** » Amended and Restated Regulations Under the Telecommunications Law, or Supreme Decree No. 020-2007-MTC, articles 18 and 19 • **Blocking of communication lines being used in connection with unlawful activities:** » Amended and Restated Regulations Under the Telecommunications Law, or Supreme Decree No. 020-2007-MTC, articles 18 and 19
Competent Authorities	• Judicial Branch (judges) • Attorneys general (at both the national and local levels) • National Police of Peru and its members • Public prosecutors • Members of the Peruvian Congress • National Prison System (*Instituto Nacional Penitenciario*) • Ministry of the Interior (*Ministerio del Interior*) • Other government agencies In each case, subject to the terms of the relevant court order

SOUTHERN CONE[11]

ARGENTINA	
Applicable statutes	• Constitution of the Argentine Nation (*Constitución de la Nación Argentina*) • National Telecommunications Law (*Ley Nacional de Telecomunicaciones*), or Law No. 19.798 • Law on the Digitalization of Argentina (*Ley Argentina Digital*), or Law 27.078 • National Intelligence Law (*Ley de Inteligencia Nacional*), or Law No. 25.520 • Decree No. 256/2015 • Supreme Court decisions Nos. 2/2016 and 30/2016 • Amended and Restated Federal Criminal Procedural Code (*Texto Ordenado del Código Procesal Penal Federal*), or Decree No. T.O. 118-2019 • National and provincial procedural codes
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Criminal Procedural Code for the Nation (*Código de Procedimiento Penal de la Nación*), Article 236 » Amended and Restated Federal Criminal Procedural Code, or Decree No. T.O. 118-2019, Article 122 • **Real-time geolocation of mobile devices:** » Criminal Procedural Code for the Nation, Article 236 » Amended and Restated Federal Criminal Procedural Code, or Decree No. T.O. 118-2019, Article 122 • **Interception of private communications:** » National Telecommunications Law, or Law No. 19.798, Article 18 » National Law on Information and Communication Technologies (*Ley Nacional de Tecnologías de la Información y las Comunicaciones*), or Law No. 27.078, Article 5 » National Intelligence Law (*Ley de Inteligencia Nacional*), or Law No. 25.520, Article 5 » Criminal Procedural Code for the Nation, Article 236 » Amended and Restated Federal Criminal Procedural Code, or Decree No. T.O. 118-2019, Article 150 • **Discontinuance of telecommunications services:** » Criminal Procedural Code for the Nation, Article 236 » Amended and Restated Federal Criminal Procedural Code, or Decree No. T.O. 118-2019, Article 122 • **Blocking of communication lines being used in connection with unlawful activities:** » Criminal Procedural Code for the Nation, Article 236 » Amended and Restated Federal Criminal Procedural Code, or Decree No. T.O. 118-2019, Article 122
Competent Authorities	• For purposes of interception requests and the maintenance of communication with carriers in connection therewith: Directorate for Legal Assistance in Connection with Complex Crimes and Organized Crime (*Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado*, or DAJUDECO) • For purposes of the issuance of ORFIs or SROs: » Judges, if relating to the Interception of private communications generally » Attorneys general, if relating to the interception of communications in connection with active investigations of kidnappings for ransom

PARAGUAY	
Applicable statutes	• National Constitution of Paraguay (*Constitución Nacional del Paraguay*) • Criminal Procedural Code of the Republic of Paraguay (*Código Procesal Penal de la República del Paraguay*) • Regulations issued by the National Telecommunications Commission (*Comisión Nacional de Telecomunicaciones*, or CONATEL) under the Telecommunications Law (*Ley de Telecomunicaciones*): » Directorate's Resolution No. 583/2020 » Directorate's Resolution No. 1350/2002 » Directorate's Resolution No. 2377/2021 • Law No. 4739/2013 that Creates the 911 Emergency Response, Dispatch, and Communications Management System (*Ley 4739/2013 que crea el Sistema 911 de atención, despacho y seguimiento de comunicaciones de emergencias*)
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Criminal Procedural Code of the Republic of Paraguay, Article 228 • **Real-time geolocation of mobile devices:** » Law No. 4739/2013 that Creates the 911 Emergency Response, Dispatch, and Communications Management System, Article 12 • **Interception of private communications:** » National Constitution of Paraguay, Article 36 • **Blocking of telephone lines:** » Public prosecutors based upon a court order, and/or courts of competent jurisdiction » CONATEL's Directorate Resolution No. 2377/2021, Article 1
Competent Authorities	• Judges • Public prosecutors (*Ministerio Público*)

[11] Includes our operations in Argentina, Paraguay and Uruguay.

URUGUAY	
Applicable statutes	• Constitution of the Oriental Republic of Uruguay (*Constitución de la República Oriental de Uruguay*) • Criminal Code (*Código Penal*) • Criminal Procedural Code (Código del Proceso Penal), or Law No. 19.293 • Decree No. 271/2021 • Decree No. 345/2022 • Decree No. 366/2017
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Law No. 19574, Article 62 » Criminal Procedural Code or Law No. 19.293, Article 45(K)(XIV) and (XV) » Decree 1/1113, enacted March 13, 2014 » General Procedural Code (*Código General del Proceso*), or Law No. 15982, Article 190 » Regulations Under Article 103 of Law No. 19889 (*Reglamentación del Artículo 103 de la Ley 19889*) • **Real-time geolocation of mobile devices:** » Law No. 19574, Article 62 » Criminal Procedural Code or Law No. 19.293, Article 45(K)(XIV) and (XV) » Decree 1/1113, enacted March 13, 2014 • **Interception of private communications:** » Law No. 19574, Article 62 » Criminal Procedural Code or Law No. 19.293, Article 45(K)(XIV) and (XV) » Decree 1/1113, enacted March 13, 2014 • **Blocking of URLs:** » Law No. 19.924 » Decree No. 345/2022 » Decree No. 366/2017
Competent Authorities	• Labor, civil and departmental courts, attorneys general and the Unit for the Regulation of Communication Services (*Unidad Reguladora de Servicios de Comunicaciones*, or URSEC), for purposes of the issuance of ORFIs relating to retained data • Criminal courts, upon request of the Office of the Public Prosecutor (*Ministerio Público*), for purposes of the issuance of SROs relating to the geolocation of devices or the interception of communications • URSEC, for purposes of the issuance of SROs relating to the blocking of URLs

CARIBBEAN[12]

PUERTO RICO	
Applicable statutes	a. Enacted by the government of the United States: • Constitution of the United States of America • Telecommunications Act of 1996 • Stored Wire Electronic Communications Act, 18 U.S.C. 2701-2713 • Foreign Intelligence Surveillance Act of 1978 • Communications Assistance for Law Enforcement Act of 1994 • Electronic Communications Privacy Act (as amended by the USA PATRIOT Act) b. Enacted by the government of the Commonwealth of Puerto Rico: • Constitution of the Commonwealth of Puerto Rico (*Constitución del Estado Libre Asociado de Puerto Rico*) • Puerto Rico Telecommunications Act of 1996 (*Ley de Telecomunicaciones de Puerto Rico de 1996*) • Civil Procedural Rules of Puerto Rico (*Reglas de Procedimiento Civil de Puerto Rico*) • Cybersecurity Act of the Commonwealth of Puerto Rico (*Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico*), or Act 40-2024 • Regulations Prescribing the Publication of the Privacy Policy Regarding the Management of Citizens' Private and Personal Data (*Reglamento para Implantar la Publicación de la Política de Privacidad en el Manejo de Datos Privados y Personales de Ciudadanos*)
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Electronic Communications Privacy Act (as amended by the USA PATRIOT Act), 18 U.S.C. §§ 2510-2523 » Stored Communications Act, 18 U.S.C. §§ 2701-2713 » Communications Act, 47 U.S.C. § 222(c) » Communications Assistance to Law Enforcement Act 47 U.S.C. §§ 1001-1010 » Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1885c » Puerto Rico Telecommunications Act, 27 L.P.R.A. § 267f (2) » Civil Procedural Rules of Puerto Rico, 27 L.P.R.A. § 40.2 • **Real-time geolocation of mobile devices:** » Other than with respect to 911 emergency calls, the disclosure of geolocation information to governmental authorities in connection with any investigation is not expressly permitted by any federal or local law. However, the United States Court of Appeals for the First Circuit (which covers Puerto Rico) has held that, under the Stored Communications Act (18 U.S.C. §§ 2701-2713), a governmental entity may require a provider to disclose real-time tracking information based upon a court order. • **Discontinuance of telecommunications services:** » Electronic Communications Privacy Act (as amended by the USA PATRIOT Act), 18 U.S.C. §§ 2510-2523 » Communications Assistance to Law Enforcement Act 47 U.S.C. §§ 1001-1010 » Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1885c
Competent Authorities	• Court officials • Government officials • Attorneys general In each case, within the limits of their powers and authority under the laws of the United States and the Commonwealth of Puerto Rico

[12] Includes our operations in Puerto Rico and the Dominican Republic.

DOMINICAN REPUBLIC	
Applicable statutes	• Constitution of the Dominican Republic (*Constitución de la República Dominicana*) • General Telecommunications Law (*Ley General de las Telecomunicaciones*), or Law No. 153-98 • Criminal Procedural Code of the Dominican Republic (*Código Procesal Penal de la República Dominicana*), or Law No. 76-02 • Law on Cybercrimes and Misdemeanors (*Ley Sobre Crímenes y Delitos de Alta Tecnología*), or Law No. 53-07 • Decision No. 2043-2003 of the Supreme Court of Justice • Decision No. 0200-13 of the Constitutional Tribunal (*Tribunal Constitucional*) on confidentiality
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Law No. 53-07 on High Technology Crimes and Misdemeanors, Article 56 • **Real-time geolocation of mobile devices:** » Law No. 53-07 on High Technology Crimes and Misdemeanors, Article 56 • **Interception of private communications:** » Criminal Procedural Code of the Dominican Republic, or Law No. 76-02, Article 192 • **Real-time interception of telecommunications:** » Criminal Procedural Code of the Dominican Republic, or Law No. 76-02, Article 192 • **Discontinuance of telecommunications services:** » General Telecommunications Law, or Law No. 153-98, Article 6 • **Blocking of communication lines being used in connection with unlawful activities:** » General Telecommunications Law, or Law No. 153-98, Article 6 » Regulations Relating to the Rights and Obligations of Users and Carriers (*Reglamento de Derechos y Obligaciones entre Usuarios y Prestadoras*), Article 14
Competent Authorities	• Public prosecutors (*Ministerio Público*) and ancillary agencies

BRAZIL	
Applicable statutes	• Constitution of the Federated Republic of Brazil (*Constituição da República Federativa do Brasil*) • General Telecommunications Law (*Lei Geral das Telecomunicações*) • Federal Law on the Protection of Data (*Lei Geral de Proteção de Dados Pessoais*), or Law No. 13.709/2018 • Brazilian Telecommunications Code (*Código Brasileiro de Telecomunicações*), or Law No. 4117/1962 • Civil Rights Framework for the Internet (*Marco Civil da Internet*), or Law No. 12.965/2014
Scope of our cooperation obligations / required actions	• **Delivery of retained data to Competent Authorities:** » Federal law against organized crime, Article 15 » Law No. 9.613/98 on money laundering and related crimes, Article 17-B » Criminal Procedural Code (*Código de Processo Penal*), Article 13-A » Civil Rights Framework for the Internet (*Marco Civil da Internet*), Article 10 • **Real-time geolocation of mobile devices:** » Law No. 13.812/19 that Creates the 911 Emergency Response, Dispatch, and Communications Management System, Article 10 » Criminal Procedural Code, Article 13-B • **Interception of private communications:** » Law No. 9.296/96, Article 1 • **Discontinuance of telecommunications services:** » Constitution of the Federated Republic of Brazil, Article 136 (which provides that, upon declaration of a state of siege, the President may impose temporary restrictions on the privacy of the communications of any person)
Competent Authorities	• Executive Branch (President of the Republic) • Judicial Branch • Public prosecutors (*Ministério Público*) upon request of the Office of the Attorney General (*Advocacia-Geral da União*) • Police authorities or Police Commissioner • Regulatory agencies

EUROPE[13]

Our operations in Europe are subject to a multinational regulatory framework that is comprised of the legislation of the European Union ("EU") and the domestic laws of the countries in which our subsidiaries are based[14]. At the supranational level, electronic communications services are primarily governed by the European Electronic Communications Code, or EECC, whose provisions aim to harmonize the EU member states' telecommunications regulatory frameworks, ensure the maintenance of a secure communications environment and promote cooperation with the regulatory authorities.

In addition to the above, our European subsidiaries are subject to various laws, regulations and directives relating to the privacy and confidentiality of communications, including (i) the EU's General Data Protection Regulation (GDPR), (ii) the European ePrivacy Directive, (iii) the regulations relating to cybersecurity and the security of communication networks, and (iv) the domestic criminal procedural laws in effect in the countries in which we operate, as they relate to the unlawful access to communications-related data and other data.

AUSTRIA	
Applicable statutes	• Security Police Act (*Sicherheitspolizeigesetz*, or SPG) • Criminal Procedural Code (*Strafprozessordnung*, or StPO) • Telecommunications Act of 2021 (T*elekommunikationsgesetz 2021*, or TKG 2021) • Financial Crimes Act (*Finanzstrafgesetz*, or FinStrG) • State Protection and Intelligence Service Act (*Staatsschutz- und Nachrichtendienst-Gesetz*, or SNG) • Stock Exchange Act 2018 (*Börsegesetz 2018*, or BörseG 2018) • Military Powers Act (*Militärbefugnisgesetz*, or MBG)
Scope of our cooperation obligations / required actions	• **Delivery of basic information about a customer:** » SPG § 53, StPO §§ 134 and 135, TKG 2021 § 181, FinStrG § 99, SNG § 11, BörseG 2018 § 99 and 153, MBG § 22 • **Delivery of stored traffic data to Competent Authorities:** » StPO §§ 134 and 135, FinStrG § 99, SNG § 11, BörseG 2018 § 99 and 153, MBG § 22 • **Interception of private communications:** » StPO §§ 134 and 135, SNG § 11 • **Real-time geolocation of mobile devices:** » SPG § 53, SNG § 11
Competent Authorities	• Police • Attorneys general and public prosecutors • Jurisdictional authorities • Administrative authorities • Financial crimes enforcement authorities • Financial Market Authority • Directorate State Protection and Intelligence Service • Military authorities

[13] Includes our operations in Austria, Belarus, Bulgaria, Croatia, Slovenia, North Macedonia and Serbia.

[14] Austria, Bulgaria, Croatia and Slovenia, who are member states of the EU, have incorporated these provisions into their own legal frameworks. North Macedonia and Serbia, who are candidate countries for EU membership, are in the process of incorporating the EU's legal framework into their own national legislation.

BELARUS	
Applicable statutes	• Constitution of the Republic of Belarus (*Конституция Республики Беларусь*) • Telecommunications Act of the Republic of Belarus (*Закон Республики Беларусь «Об электросвязи»*) (provisions relating to the obligations of network operators) • Operative Search and Investigation Act (*Закон Республики Беларусь «Об оперативно-розыскной деятельности»*), or Act No. 307-3 of July 15, 2015 (provisions relating to interceptions) • Criminal Procedural Code of the Republic of Belarus (*Уголовно-процессуальный кодекс Республики Беларусь*) • Personal Data Protection Act (*Закон Республики Беларусь «О защите персональных данных»*), or Act No. 99-3 of May 7, 2021 (exceptions for national security purposes) • Information, Informatization and Information Protection Act (*Закон Республики Беларусь «Об информации, информатизации и защите информации»*), or Act No. 455-3 of November 10, 2008 (provisions relating to lawful interceptions) • Resolution No. 476 of the Council of Ministers, dated September 2, 2025, restricting access to Internet resources and allowing the disconnection of subscribers from services (*Постановление Совета Министров РеспублиБеларуськи Беларусь*)
Scope of our cooperation obligations / required actions	• **Delivery of user data:** » Telecommunications Act of the Republic of Belarus, § 43 • **Cooperation in connection with investigations:** » Telecommunications Act of the Republic of Belarus, § 43 • **Protection of methods-related data:** » Telecommunications Act of the Republic of Belarus, § 43 • **Provision of access to databases:** » Telecommunications Act of the Republic of Belarus, § 43
Competent Authorities	• Office of the Attorney General (*Генеральный прокурор*) through its authorized officials • Investigative Committee (*Председатель Следственного комитета*) through its authorized officials • State Security Committee (*Председатель КГБ*), or KGB, through its authorized officials • Ministry of Internal Affairs (*Министр внутренних дел*), through its authorized officials • Operations and Analysis Center Under the President of the Republic (*Оперативно-аналитический центр при Президенте Республики Беларусь*), or OAC, as with respect to the oversight and surveillance of the telecommunications sector • National State Inspectorate for Telecommunications (*Государственная инспекция по электросвязи*) • State Control Committed (*Комитет государственного контроля*) • Ministry of Information (*Министерство информации*)

BULGARIA	
Applicable statutes	• Electronic Communications Act (*Закон за електронните съобщения*) • National Criminal Code (*Наказателен кодекс*) • Personal Data Protection Act (*Закон за защита на личните данни*) • National Cybersecurity Act (NIS2) (*Закон за киберсигурност*) • Electronic Communications Networks and Physical Infrastructure Act (*Закон за електронните съобщителни мрежи и физическа инфраструктура*) • Special Intelligence Means Act (*Закон за специалните разузнавателни средства*) • Communications Regulation Commission (*Комисия за регулиране на съобщенията*, or KPC) • Insurance Code (*Кодекс за застраховането*) • Credit Institutions Act (*Закон за кредитните институции*)
Scope of our cooperation obligations / required actions	• **Delivery of stored traffic data to Competent Authorities:** » Electronic Communications Act, § 251 et seq. » Criminal Procedural Code, § 150 • **Interception of private communications:** » Electronic Communications Act, § 304 et seq., as they related to the Special Intelligence Means Act • **Identification of customers:** » Electronic Communications Networks and Physical Infrastructure Act, § 310
Competent Authorities	• Attorneys general, for purposes of criminal procedures/investigations • Criminal and, in certain instances, civil courts, upon the issuance of an order • Ministry of Interior/police, which are the entities vested with the power and authority to conduct criminal investigations and perform public security duties • State Agency for National Security and other intelligence and/or security agencies, for purposes of the performance of any national security and counterintelligence duties under the Special Intelligence Means Act • Communications Regulation Commission, for purposes of the exercise of its oversight powers and the enforcement of the applicable regulation • Commission for Personal Data Protection, for purposes of the exercise of its oversight powers • Emergency services such as the operators of the 112 system, to facilitate the response to emergency calls and the location of individuals who are in danger (frequently, in limited circumstances and subject to specific laws and regulations) • Tax and customs authorities such as the National Revenue Agency, where expressly permitted by the applicable laws, for purposes of the conduction of tax- or customs-related investigations (generally, in certain specific circumstances and upon a court order) • Other governmental entities vested with jurisdiction over specific sectors (e.g., anticorruption, financial intelligence), but solely and exclusively where permitted by law and subject to certain procedural guarantees • The authorities responsible for the regulation and oversight of financial and credit institutions

CROATIA	
Applicable statutes	• Constitution of the Republic of Croatia (*Ustav Republike Hrvatske*) (Official Gazette Nos. 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10 and 05/14) • Electronic Communications Act (*Zakon o elektroničkim komunikacijama*) (Official Gazette No. 76/2022) • Regulation on national security requirements of the Republic of Croatia for individuals and legal entities in telecommunications (*Pravilnik o zahtjevima nacionalne sigurnosti Republike Hrvatske za fizičke i pravne osobe u telekomunikacijama*) (Official Gazette Nos. 64/2008 and 76/2013) • Criminal Procedural Act (*Zakon o kaznenom postupku*) (Official Gazette Nos. 152/08, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/2017, 126/19, 130/20 and 80/22) • Office for the Suppression of Corruption and Organised Crime Act (*Zakon o Uredu za suzbijanje korupcije i organiziranog kriminaliteta*) (Official Gazette Nos. 76/09, 116/10, 145/10, 57/11, 136/12, 148/13, 70/17, 136/25)
Scope of our cooperation obligations / required actions	• **Delivery of retained data:** » Criminal Procedural Act, §§ 261 and 263 • **Preservation of retained data:** » Criminal Procedural Act, § 263, fourth paragraph • **Interception (telephone tapping and surveillance):** » Electronic Communications Act, §§ 52-54 » Security and Intelligence System Act, §§18, 19 and 33 » Criminal Procedural Act, §§ 207, 257, 332, 334, 335, 227 and 229 » Regulation on national security requirements of the Republic of Croatia for individuals and legal entities in telecommunications
Competent Authorities	• Operational and Technical Centre for Telecommunications Surveillance, or OTC • Judicial Branch (criminal courts) • Office of the Attorney General • Office for the Suppression of Corruption and Organised Crime • Police • Secret Service

SLOVENIA	
Applicable statutes	• Criminal Procedural Act Penal (*Zakon o kazenskem postopku*) • Police Tasks and Powers Act (*Zakon o nalogah in pooblastilih policije*) • Electronic Communications Act (*Zakon o elektronskih komunikacijah*) • Financial Administration Act (*Zakon o finančni upravi*) • Inspection Act (*Zakon o inšpekcijskem nadzoru*) • Criminal Code (*Kazenski zakonik*)
Scope of our cooperation obligations / required actions	• **Delivery of data and cooperation with Competent Authorities in connection with criminal procedures:** » Criminal Procedural Act, §§ 148, 149/b, 149/c, 149/č, 149/e, 156 and 161 » Criminal Code, § 43 • **Compliance and cooperation with police authorities' ORFIs and law enforcement activities:** » Police Tasks and Powers Act, §§ 43 and 115 • **Mandatory disclosure of electronic communications data:** » Electronic Communications Act, §§ 11 and 287 • **Delivery of data to financial authority for official purposes:** » Financial Administration Act, §§ 17 and 46 • **Delivery of documentation and data in connection with inspections:** » Inspection Act, § 19
Competent Authorities	• Police (*Policija*) • Financial Administration (*Finančna uprava*) • Agency for Communication Networks and Services (*Agencija za komunikacijska omrežja in storitve*, or AKOS) • Market Inspectorate (*Tržni inšpektorat*) • District State Prosecutor's Office (*Okrožno državno tožilstvo*) • Courts (*Sodišče*)

NORTH MACEDONIA	
Applicable statutes	• Constitution of the Republic of North Macedonia (*Устав на Република Северна Македонија*) • Law on Criminal Procedure (*Закон за кривична постапка*) • Law on Electronic Communications (*Закон за електронски комуникации*) • Law on Interception of Communications (*Закон за законито следење на комуникациите*) • Law on Police (*Закон за полиција*) • Law on the Public Prosecution Office (*Устав на Република Северна Македонија*)
Scope of our cooperation obligations / required actions	• **Delivery of metadata, including:** » Tracking and identification of the origin of a communication » Identification of the destination of a communication » Identification of the date, time and duration of a communication » Identification of the type of communication » Identification of the type of equipment used by the customer or presumably owned thereby » Identification of the location of mobile communication devices In each case, pursuant to Article 207 of the Law on Electronic Communications, articles 258 and 287 of the Law on Criminal Procedure, articles 32 and 33 of the Law on Interception of Communications, Article 3 of the Law on Police, and articles 1, 2 and 5 of the Law on the Public Prosecution Office. • **Interception:** » Law on Electronic Communications, Article 115
Competent Authorities	• Judicial Branch (courts) • Ministry of Interior • Offices of the attorneys general and public prosecutors • Intelligence agencies • Operational and Technical Agency • Agency for National Security • Financial Police Office • Customs Administration

SERBIA	
Applicable statutes	• Constitution of the Republic of Serbia (*Ustav Republike Srbije*) • Electronic Communications Act (*Zakon o elektronskim komunikacijama*) • Criminal Procedure Code (*Zakonik o krivičnom postupku*) • Security Information Agency Act (*Zakon o Bezbednosno-informativnoj agenciji*) • Military Security Agency and Military Intelligence Agency Act (*Zakon o Vojno-bezbednosnoj agenciji i Vojno-obaveštajnoj agenciji*) • Rulebook on the Requirements for Devices and Software Support for Lawful Interception of Electronic Communications and Technical Requirements for Fulfilling the Obligation of Data Retention on Electronic Communications (*Pravilnik o uslovima koje moraju da ispunjavaju uređaji i softverska podrška za zakonito presretanje elektronskih komunikacija i tehničkim uslovima za ispunjavanje obaveze zadržavanja podataka o elektronskim komunikacijama*)
Scope of our cooperation obligations / required actions	• **Retention of communications data, including:** » Tracking and identification of the origin of a communication » Identification of the destination of a communication » Determination of the beginning, duration and end of a communication » Identification of the type of communication » Identification of the customers' equipment » Identification of the location of the customers' mobile devices In each case, pursuant to §§ 126-130 • **Interception of electronic communications:** » Rulebook
Competent Authorities	• Criminal courts • Ministry of the Interior (Police) • Office of the Attorney General • Security and Intelligence Agency, or BIA • Military Security Agency, or VBA • Military Intelligence Agency

ORFI AND SRO STATISTICS

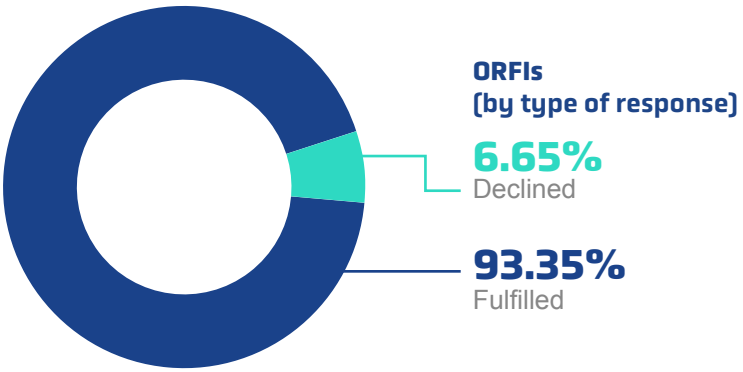
EUROPE

The laws and regulations currently in effect in the countries in which we operate in Europe impose certain restrictions on the disclosure of the type of operating data covered by this Report, which are aimed at protecting the integrity of investigations and the rights of data subjects. In compliance with such restrictions and with the EU General Data Protection Regulation, this section does not include statistical information about the inquiries addressed by our European affiliates[15].

LATIN AMERICA

In 2025, our subsidiaries in Latin America received a total of 909,867 ORFIs and SROs. This represented an increase of 45,089 ORFIs and SROs or 5.21%, in the total number of ORFIs and SROs received by our subsidiaries, over 2024.

We addressed 849,346 ORFIs and SROs or 93.35% of the total number of ORFIs and SROs received, and rejected for various reasons 60,521 ORFIs and SROs or 6.65% of the total number of ORFIs and SROs received by our subsidiaries.



As required by the applicable laws relating to national security, the protection of the data held by telecommunications operators, the secrecy of telecommunications and other related matters in the countries in which we operate, we do not perform any type of analysis or assessment of the aforementioned information. The above is intended primarily to preserve the confidentiality of the personal data of those of our customers whose individual accounts or lines have been the subject matter of an ORFI or SRO, and of the communications carried over such lines[16].

[15] In Austria, the Federal Ministry of the Interior publishes an annual report on the actions taken against all operators in response to requests for access to information of public importance, which is available at: https://www.bmi.gv.at/508/start.aspx.
The statistical information pertaining to the ORFIs and SROs received and processed in Serbia is available at: https://www.poverenik.rs/en/o-nama/annual-reports.html

[16] However, our Colombian subsidiary reports to the Ministry of Information and Communication Technologies (*Ministerio de Tecnologías de la Información y las Comunicaciones*, or MinTIC), on a monthly basis, the impact on its customers of the blocking orders issued thereby with respect to certain URLs, based on the demands, claims and complaints submitted by them through our customer service channels.

The following table contains a breakdown of the total number of ORFIs and SROs received by our operating subsidiaries, by country.

MEXICO	
Total	100,948
Addressed	97,881
Rejected	3,067

CENTRAL AMERICA

	COSTA RICA	EL SALVADOR	GUATEMALA	HONDURAS[17]	NICARAGUA
Total	19,599	8,907	12,229	9,969	547
Addressed	19,404	7,923	9,639	9,969	519
Rejected	195	984	2,590	0	28

ANDEAN REGION

	CHILE	COLOMBIA	ECUADOR	PERU
Total	38,003	29,342	16,175	18,597
Addressed	36,212	22,158	8,359	17,081
Rejected	1,791	7,184	7,816	1,516

SOUTHERN CONE

	ARGENTINA	PARAGUAY	URUGUAY
Total	116,350	5,858	13,958
Addressed	116,005	5,858	13,958
Rejected	345	0	0

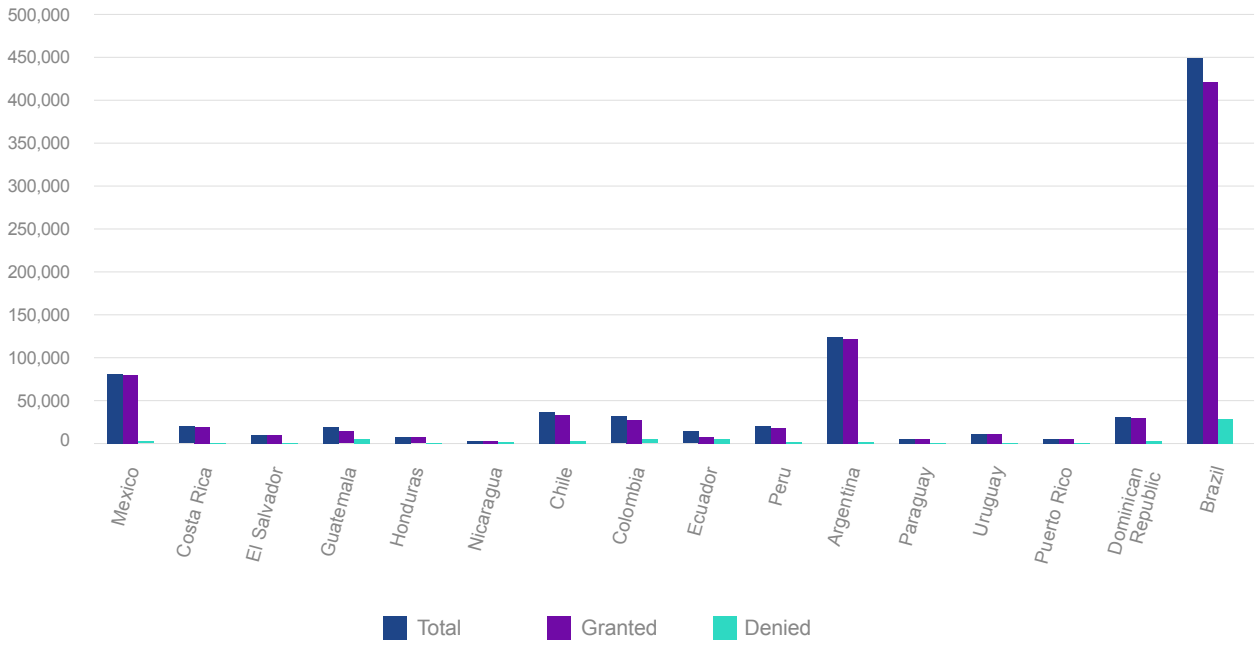
CARIBBEAN

	PUERTO RICO	DOMINICAN REPUBLIC
Total	4,925	34,556
Addressed	4,925	34,556
Rejected	0	0

BRAZIL	
Total	479,904
Addressed	444,899
Rejected	35,005

[17] In Honduras, the Competent Authorities did not pick up from our offices the information that we gathered in response to 242 ORFIs, or 2.43% of the total number of ORFIs we received from such authorities.

ORFIs BY COUNTRY



PROCESSED REQUESTS BREAKDOWN

Of the aggregate number of ORFIs and SROs we addressed[18], (i) 41.8% pertained to Retained Data[19] and (ii) 58.2% involved accessing or providing access to communications (e.g., interception of telephone calls, discontinuance of services, real-time geolocation, and blocking). The following table contains a breakdown of such ORFIs and SROs by country.

MEXICO	
Retained Data	85,074
Access to communications	12,807

CENTRAL AMERICA

	COSTA RICA	EL SALVADOR	GUATEMALA	HONDURAS	NICARAGUA
Retained Data	19,395	7,923	7,697	9,969	519
Access to communications	9	0	1,942	0	0

[18] Upon determination that such ORFIs or SROs were valid.

[19] Defined as files and records pertaining to customer accounts or which contain personal data of our customers.

ANDEAN REGION

	CHILE	COLOMBIA	ECUADOR	PERU
Retained Data	30,498	22,158	8,359	15,840
Access to communications	5,714	0	0	1,241

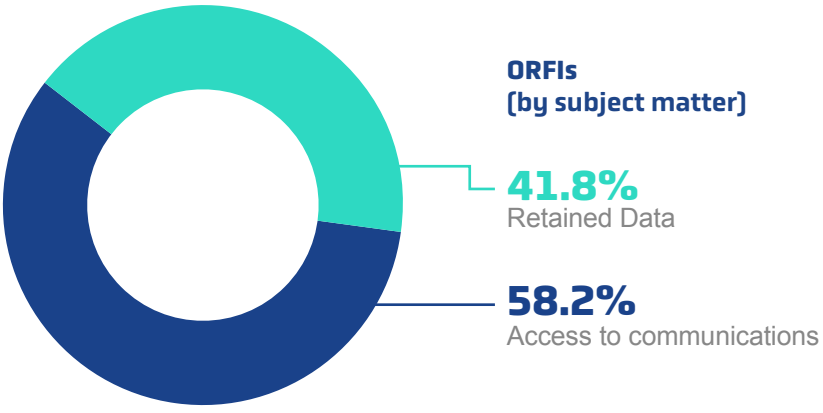
SOUTHERN CONE

	ARGENTINA	PARAGUAY	URUGUAY
Retained Data	103,493	5,776	10,577
Access to communications	12,512	82	3,381

CARIBBEAN

	PUERTO RICO	DOMINICAN REPUBLIC
Retained Data	4,871	22,910
Access to communications	54	11,646

BRAZIL	
Retained Data	4
Access to communications	444,895



In 2025, our subsidiaries in Latin America received a total of 2,224 SROs[20] requiring access to communications and addressed/complied with 2,217 or 99.69% of such SROs. The following table contains a breakdown of such SROs by country.

COUNTRY	SROs RECEIVED	SROs ADDRESSED	ISSUERS/COMPETENT AUTHORITIES
Mexico	1,882	1,882	State attorneys general
Costa Rica	72	65	Public prosecutors (*Ministerio Público*)
El Salvador	0	0	Office of the Attorney General of the Republic (*Fiscalía General de la República*) Criminal courts (in connection with criminal investigations)
Guatemala	83	83	Attorneys general Ministry of Government (*Ministerio de Gobernación*)
Honduras	0	0	Judicial Branch
Nicaragua	0	0	Judicial Branch
Colombia	0	0	Judicial Branch
Ecuador	0	0	Executive Branch, through the National Telecommunications Regulation and Control Agency (*Agencia de Regulación y Control de las Telecomunicaciones*, or ARCOTEL)
Peru	118	118	Executive Branch, through the Supervisory Agency for Private Investment in Telecommunications (*Organismo Supervisor de Inversión Privada en Telecomunicaciones*, or OSIPTEL)
Argentina	69	69	Attorneys general Judicial Branch (judges)
Dominican Republic	0	0	Judicial Branch
Brazil	0	0	Judicial Branch

[20] The applicable laws in effect in Chile, Paraguay, Puerto Rico and Uruguay do not provide for this type of actions. Accordingly, the table does not include information for those countries.

In 2025, our subsidiaries in Latin America received 54,256 SROs requiring the interception of communications (i.e. real-time interventions). Brazil, Argentina and the Dominican Republic together accounted for 68.47% of such SROs.

COUNTRY	SROS RECEIVED	ISSUERS/COMPETENT AUTHORITIES
Mexico	4,922	Executive Branch, through the Ministry of the Interior (*Secretaría de Gobernación*) Security agencies/National Guard Federal and state attorneys general
Costa Rica	9	Public prosecutors (*Ministerio Público*)
El Salvador[21]		Office of the Attorney General of the Republic (*Fiscalía General de la República*)
Guatemala	1,571	Special Investigative Methods Unit (*Unidad de Métodos Especiales de Investigación*)
Honduras[22]		Office of the Public Prosecutor, through the Communications Intervention Unit (*Unidad de Intervención de Comunicaciones*)
Nicaragua	0	Judicial Branch
Chile	5,962	Public prosecutors (*Ministerio Público*) Office of the National Economic Prosecutor Judicial Branch (Courts of Appeals)
Colombia[23]		Office of the Attorney General of the Republic (*Fiscalía General de la República*)
Ecuador	0	Office of the Attorney General
Peru	1,123	Judicial Branch
Argentina	12,512	Judicial Branch, through the Directorate for Legal Assistance in Connection with Complex Crimes and Organized Crime
Paraguay	82	Judicial Branch
Uruguay	3,381	Judicial Branch
Puerto Rico	54	Judicial Branch of the U.S. government Executive Branch of the U.S. government » United States Drug Enforcement Administration » Federal Bureau of Investigations » United States Department of Homeland Security/U.S. Immigration and Customs Enforcement » Bureau of Alcohol, Tobacco, Firearms and Explosives
Dominican Republic	11,646	Public prosecutors (*Ministerio Público*) Judicial Branch
Brazil	12,994	Judicial Branch

Of the total number of ORFIs and SROs received by our subsidiaries from Competent Authorities[24] in Latin America, 53.4% were issued by security agencies (primarily, police authorities), 24.7% by members of the judiciary and 21.4% by attorneys general[25].

[21] The Office of the Attorney General has the power and authority to access our systems to intervene directly in any communication. Accordingly, there is no information available on the number of interventions carried out thereby.

[22] The Communications Intervention Unit, which is part of the National Directorate for Intelligence and Investigation (*Dirección Nacional de Inteligencia e Investigación*), has the power and authority to access our systems to intervene directly in any communication.

[23] The Office of the Attorney General of the Nation has the power and authority to access our systems to intervene directly in any communication. Accordingly, there is no information available on the number of interventions carried out thereby.

[24] For ease of reference, we have classified the Competent Authorities according to the branch of government to which they belong. However, our data bases contain detailed information about the Competent Authority that issued each ORFI or SRO, including the name thereof and the number of the official communication by means of which we were given notice thereof.

[25] Includes the ORFIs received from public prosecutors in each of the countries in which we operate.

We fulfilled or complied with 94.8% of the ORFIs and/or SROs that we received from attorneys general, 94.7% of the ORFIs and/or SROs we received from judicial authorities (including judges, Courts and Supreme Court), 92.4% of the ORFIs and/or SROs we received from security agencies, 66.3% of the ORFIs and/or SROs we received from executive authorities and 63.7% of the ORFIs and/or SROs we received from "Other Authorities" (primarily, independent agencies or entities which are not executive, legislative or judicial authorities) constituted valid and lawful ORFIs or SROs.

The following table contains a breakdown of the total number of ORFIs and SROs that we received and either addressed or rejected in each of the countries in which we operate, by type of Competent Authority.

MEXICO		
TOTAL ORFIs & SROs BY TYPE OF AUTHORITY	Judicial Branch	4,757
	Executive Branch	0
	Security agencies	9,843
	Attorneys general	84,375
	Other Authorities	1,973
	Total	**100,948**
ADDRESSED	Judicial Branch	3,900
	Executive Branch	0
	Security agencies	9,489
	Attorneys general	83,386
	Other Authorities	1,106
	Total	**97,881**
REJECTED	Judicial Branch	857
	Executive Branch	0
	Security agencies	354
	Attorneys general	989
	Other Authorities	867
	Total	**3,067**

CENTRAL AMERICA

		COSTA RICA	EL SALVADOR	GUATEMALA	HONDURAS	NICARAGUA
TOTAL ORFIs & SROs BY TYPE OF AUTHORITY	Judicial Branch	691	943	72[26]	2,057	522
	Executive Branch	0	0	18	0	0
	Security agencies	0	1	0	7,000	23
	Attorneys general	18,908	7,962	12,098	912	2
	Other Authorities	0	1	41	0	0
	Total	**19,599**	**8,907**	**12,229**	**9,969**	**547**
ADDRESSED	Judicial Branch	691	373	54	2,057	497
	Executive Branch	0	0	18	0	0
	Security agencies	0	1	0	7,000	22
	Attorneys general	18,713	7,548	9,567	912	0
	Other Authorities	0	1	0	0	0
	Total	**19,404**	**7,923**	**9,639**	**9,969**	**519**
REJECTED	Judicial Branch	0	570	18	0	25
	Executive Branch	0	0	0	0	0
	Security agencies	0	0	0	0	1
	Attorneys general	195	414	2,531	0	2
	Other Authorities	0	0	41	0	0
	Total	**195**	**984**	**2,590**	**0**	**28**

[26] In some instances, notwithstanding that an ORFI may have been issued by a judicial authority, we may be required to submit our reply to the prosecutor in charge of the investigation.

ANDEAN REGION

		CHILE	COLOMBIA	ECUADOR	PERU
TOTAL ORFIs & SROs BY TYPE OF AUTHORITY	Judicial Branch	1,201	3,910	13,970	3,376
	Executive Branch	11	540	32	118
	Security agencies	0	14,939	0	2,155
	Attorneys general	36,791	7,901	2,118	12,866
	Other Authorities	0	2,052	55	82
	Total	**38,003**	**29,342**	**16,175**	**18,597**
ADDRESSED	Judicial Branch	1,142	1,991	7,511	3,376
	Executive Branch	11	298	32	118
	Security agencies	0	12,454	0	1,658
	Attorneys general	35,059	5,906	816	11,929
	Other Authorities	0	1,509	0	0
	Total	**36,212**	**22,158**	**8,359**	**17,081**
REJECTED	Judicial Branch	59	1,919	6,459	0
	Executive Branch	0	242	0	0
	Security agencies	0	2,485	0	497
	Attorneys general	1,732	1,995	1,302	937
	Other Authorities	0	543	55	82
	Total	**1,791**	**7,184**	**7,816**	**1,516**

SOUTHERN CONE

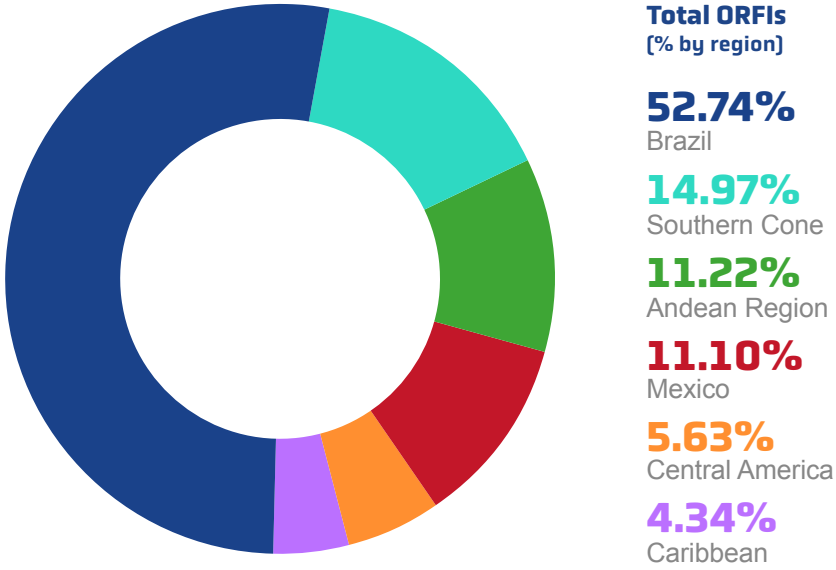
		ARGENTINA	PARAGUAY	URUGUAY
TOTAL ORFIs & SROs BY TYPE OF AUTHORITY	Judicial Branch	116,350	288	13,911
	Executive Branch	0	0	0
	Security agencies	0	0	0
	Attorneys general	0	5,570	0
	Other Authorities	0	0	47
	Total	**116,350**	**5,858**	**13,958**
ADDRESSED	Judicial Branch	116,005	288	13,911
	Executive Branch	0	0	0
	Security agencies	0	0	0
	Attorneys general	0	5,570	0
	Other Authorities	0	0	47
	Total	**116,005**	**5,858**	**13,958**
REJECTED	Judicial Branch	345	0	0
	Executive Branch	0	0	0
	Security agencies	0	0	0
	Attorneys general	0	0	0
	Other Authorities	0	0	0
	Total	**345**	**0**	**0**

CARIBBEAN

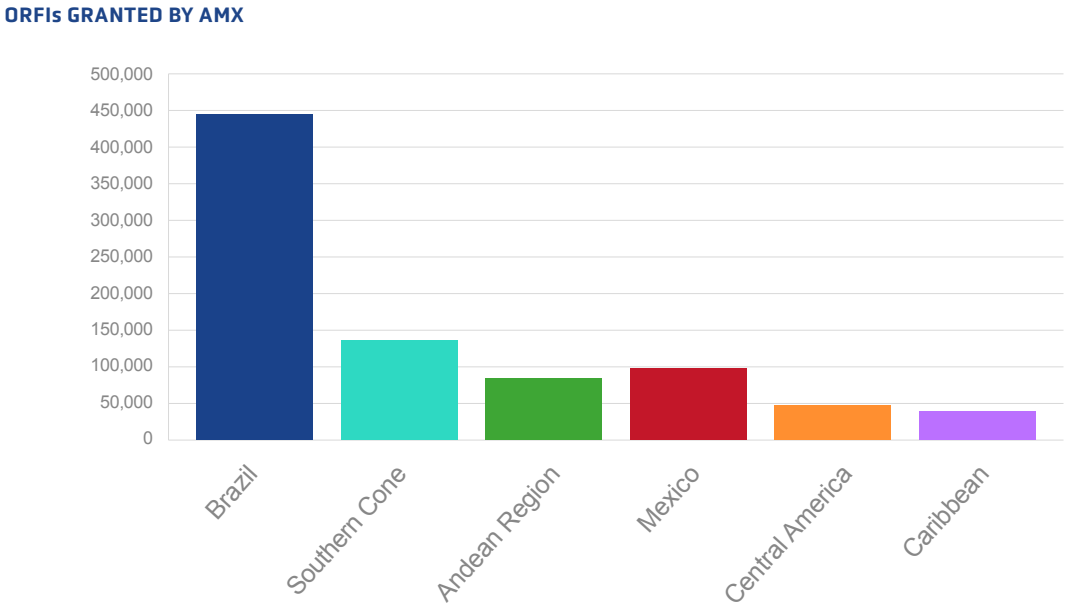
		PUERTO RICO	DOMINICAN REPUBLIC
TOTAL ORFIs & SROs BY TYPE OF AUTHORITY	Judicial Branch	234	141
	Executive Branch	0	0
	Security agencies	3,594	30,403
	Attorneys general	984	4,007
	Other Authorities	113	5
	Total	**4,925**	**34,556**
ADDRESSED	Judicial Branch	234	141
	Executive Branch	0	0
	Security agencies	3,594	30,403
	Attorneys general	984	4,007
	Other Authorities	113	5
	Total	**4,925**	**34,556**
REJECTED	Judicial Branch	0	0
	Executive Branch	0	0
	Security agencies	0	0
	Attorneys general	0	0
	Other Authorities	0	0
	Total	**0**	**0**

BRAZIL		
TOTAL ORFIs & SROs BY TYPE OF AUTHORITY	Judicial Branch	61,997
	Executive Branch	0
	Security agencies	417,907
	Attorneys general	0
	Other Authorities	0
	Total	**479,904**
ADDRESSED	Judicial Branch	60,424
	Executive Branch	0
	Security agencies	384,475
	Attorneys general	0
	Other Authorities	0
	Total	**444,899**
REJECTED	Judicial Branch	1,573
	Executive Branch	0
	Security agencies	33,432
	Attorneys general	0
	Other Authorities	0
	Total	**35,005**

On a regional basis in Latin America, Brazil accounted for the largest number of ORFIs and SROs reported by our subsidiaries in 2025, with 479,904 ORFIs and SROs or 52.74% of the total number of ORFIs and SROs we received in all of the countries in which we operate, followed by the Southern Cone with 14.97%, the Andean Region with 11.22% and Mexico with 11.10%.



The Caribbean accounted for the largest percentage of fulfilled ORFIs and SROs among all the regions in which we operate in Latin America, with 100% of the total number of ORFIs and SROs received by our subsidiaries in that region, followed by the Southern Cone with 99.75%, Mexico with 96.96% and the Andean Region with 82.07%.



STATUTORY POWERS OF COMPETENT AUTHORITIES

The following table shows the statutory powers of the Competent Authorities in each of the countries in which we operate.

	LATIN AMERICA																EUROPE						
	ARGENTINA	BRAZIL	COLOMBIA	COSTA RICA	CHILE	ECUADOR	EL SALVADOR	GUATEMALA	HONDURAS	MEXICO	NICARAGUA	PERU	PUERTO RICO	PARAGUAY	DOMINICAN REPUBLIC	URUGUAY	AUSTRIA	BELARUS	BULGARIA	CROATIA[F]	SLOVENIA	NORTH MACEDONIA[F]	SERBIA
Confidentiality	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES	YES
Service Restriction Orders	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	NO	YES	YES	YES	NO
Requisition	YES	NO	NO	NO	NO	YES	NO	YES	YES	YES	YES	YES	NO	YES	YES	NO	YES	YES	NO	NO	YES	NO	NO
Repossession of frequencies	YES	NO	YES	NO	NO	YES	YES	NO	YES	YES	YES	YES	NO	YES	YES	YES	YES	YES	NO	NO	YES	NO	YES
Restriction of network access in prisons	NO	YES	YES	YES	NO[A]	NO[C]	YES	NO	YES	YES	NO	YES	NO	NO	NO	YES	NO	NO	NO	NO	NO	YES	NO
Discontinuance of services as a result of tampering with the normal operation of a telecommunications network	NO	NO	NO	YES	NO	YES[D]	YES	NO	NO	YES	NO	YES	YES	NO	YES	NO	YES	NO	NO	NO	YES	NO	YES
Reassignment of frequencies and public telecommunication networks	NO	NO	YES	YES	NO	YES	YES	NO	NO	YES	NO	NO	YES	NO	YES	NO	YES	NO	NO	NO	YES	NO	NO
Limitation of unrestricted-use rights	NO	NO	YES	NO	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO
Domain blocking	YES	YES	YES	NO	YES[B]	YES	NO	YES[E]	NO	NO	NO	YES	NO	NO	NO	YES	YES	YES	YES	YES	YES	YES	YES
Intervention of the IT and communication sectors	YES	NO	YES	YES	NO	NO[C]	NO	NO	YES	NO	NO	YES	NO	NO	NO	YES	YES	NO	NO	NO	YES	NO	NO
Emergencies, commotions or calamities	YES	NO	YES	NO	NO	YES	NO	YES	NO	YES	NO	YES	NO	YES	YES	YES	YES	YES	NO	NO	YES	NO	YES
Content blocking	NO	NO	YES	NO	YES	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES	YES	YES	NO	NO	YES	YES	YES
Revocation of concessions	NO	NO	NO	NO	NO	YES[C]	NO	NO	YES	YES	NO	YES	NO	NO	YES	YES	YES	YES	NO	NO	YES	NO	YES

[A] Pursuant to the Supreme Court's decisions requiring carriers to block the access to unlicensed gambling websites
[B] Pursuant to a decision of the Supreme Court
[C] Pursuant to the Concession Agreement
[D] Pursuant to the Concession Agreement and the fraud prevention agreements entered into with the regulatory authorities
[E] Upon receipt of a court order
[F] Upon receipt of an order issued by a public prosecutor

FOR THE AVOIDANCE OF DOUBT, BELOW IS A GLOSSARY OF THE TERMS INCLUDED IN THE PRECEDING TABLE.

Confidentiality

Obligation to protect our customers' data and refrain from disclosing any such data (except as required by law). Under the applicable laws, legal entities are required to safeguard their customers' data and to regard such data as strictly private and confidential.

We are permitted to retain anonymized personal data, that is, personal data which has been processed to make it unidentifiable and ensure that is cannot be traced back to a specific individual. Any such information is outside the scope of the laws and regulations relating to the protection of personal data. However, such information shall remain confidential and be safeguarded in accordance with our own policies.

Service Restriction Orders

Directives (commonly known as "SROs") that constitute lawful demands of the Competent Authorities requiring us to take action to prevent or restrict the access to our networks or to the services provided by third parties over such networks, or to block certain specified services, content, URLs or domains.

Telecommunications carriers, either directly or through industry organizations such as the GSMA, have been encouraging government authorities to become more transparent about their role in the discontinuance or restriction of access to telecommunications networks and services, and about their legal arguments in support of the adoption of such measures, in an effort to ensure that any limitation on the right to freedom of expression imposed by the laws of their home countries is based solely and exclusively on security concerns, and that any intervention by such authorities is limited in scope and is carried out in compliance with the international laws and principles on the respect of human rights.

We decry the issuance of SROs which are in violation of the human rights recognized by the International Bill of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and the Ten Principles of the United Nations Global Compact. However, as a telecommunications carrier we are required to comply with the SROs of the Competent Authorities, including those relating to the imposition of service restrictions.

Government Seizure and Control (Requisition)[27]

The laws of the countries in which we operate authorize the federal governments thereof to effect the requisition of general means of communication, and of the assets, rights and elements required for their operation, in the event of (i) natural disasters, (ii) war, (iii) material disruption of the public order or (iv) imminent danger to the national security, the internal peace of the country or the domestic economy, or to ensure the continuity of service.

Under the aforementioned laws, upon any requisition the personnel assigned to the operation of the relevant network must be made available for the duration of the contingency to an administrator appointed by the federal government. Such administrator would be responsible for ensuring the achievement of the objectives stipulated in the relevant requisition order.

[27] Administrative act pursuant to which the federal government assumes temporary control over all or part of a public telecommunications network operated by a private carrier, thereby limiting the ownership rights of such carrier.

Repossession of Frequencies[28]

Under the laws of the countries in which we operate, the federal government may reclaim the radio frequencies that we use under our spectrum concessions (i) for public interest reasons, (ii) for national security reasons at the request of the President, (iii) for purposes of the deployment of new technologies, (iv) to address interference issues, (v) to comply with the international treaties to which the relevant country is a party, (vi) to reconfigure the radioelectric spectrum or (vii) to ensure the continuity of a public service.

In the event of cancellation of a concession following a repossession, the federal government shall provide for the adoption of any and all such measures as may be necessary to ensure the continuity of the services.

Restriction of network access in prisons

Obligation of a telecommunications carrier to restrict the access to its networks and services from within prison facilities in order to preclude the use of mobile devices in furtherance of criminal activities, in the interest of national security.

The Competent Authorities may require telecommunications carriers and other providers of telecommunication services to implement any such procedures and solutions as may be necessary to render commercial wireless services unavailable within the prison system.

Discontinuance of services as a result of tampering with the normal operation of a telecommunications network

Power and authority of a government entity to require a telecommunications carrier to discontinue the provision of services to one or more customers upon the detection of unusual traffic volumes that may impair the operation of a mobile network.

This may occur as a result of the use of non-homologated telecommunication devices that generate abnormal traffic volumes which cannot be controlled by their users.

Reassignment of frequencies and public telecommunication networks

Power and authority of the federal government or the agencies responsible for managing the radioelectric spectrum to require a telecommunications carrier to switch its operations to a different frequency.

Limitation of unrestricted-use rights

Power and authority of the Competent Authorities to establish unrestricted frequency bands in accordance with the recommendations issued by the International Telecommunication Union (ITU).

In such event, the regulatory agency responsible for managing the radioelectric spectrum in the relevant country will determine which of the frequencies included in such country's Frequency Allocation Chart will constitute unrestricted frequencies. In addition, such agency may determine that the users of certain frequencies will be exempted from the payment of contributions to the social programs established by the government to foster the expansion of network coverage in rural areas.

[28] Power and authority of the federal government to reclaim any or all of the radio frequencies used by a carrier under spectrum concessions in the events set forth in the applicable laws.

Domain blocking

Statutory power and authority of the Competent Authorities to require telecommunications operators to block certain specified URLs or domains if such authorities have reason to believe that such URLs or domains are being used in connection with unlawful activities such as the violation of intellectual property rights, the sexual abuse of minors or other activities proscribed by the laws of the relevant country.

Intervention of the IT and communication sectors

Power and authority of the federal government to implement regulations, public policies and actions intended to control the development of the relevant country's IT and communications sectors.

Such powers and authority, which vary from one country to another, may include the establishment of public policy objectives (e.g., the protection of users at large and of children and teenagers), the enactment of regulations governing the provision of specific types of services, the performance of audits and the implementation of actions intended to control the provision, quality, connectivity and other aspects of IT and communication services.

Emergencies, commotions or calamities

Circumstances involving the occurrence of natural disasters at the national, local or regional level in a given country, including earthquakes, floods and other events of force majeure, or events which may pose a risk to the national security of the country in which a telecommunications carrier operates, including wars, armed conflicts and internal turmoil.

Under the laws of the countries in which we operate and the terms of the concessions granted to the telecommunications carriers operating therein, upon the occurrence of a natural disaster or other event of force majeure the Competent Authorities may seek to compel such carriers to devote their attention to the restoration of communication services, to prioritize certain actions or to broadcast information intended to protect human life.

In addition, under the laws of the countries in which we operate, upon the occurrence of an event involving national security concerns the Competent Authorities may seek to compel the cooperation of telecommunications carriers in connection therewith or may take over their operations.

Content blocking

We are permitted to block the access to certain types of content, applications or services in the interest of our customers' privacy and the security of our networks. We may also block the access to specific types of content, applications and online services at the request of a customer, pursuant to an order of a Competent Authority or if the relevant content, application or service is in violation of the applicable laws.

Revocation of concessions

Power and authority of the telecommunications regulators or other Competent Authorities to terminate the concession, license or other similarly-titled agreement with a given telecommunications carrier in the event of violation of the terms of such agreement or upon the occurrence of certain events.

2025