Azevedo Sette
ADVOGADOS

TELECOMS SERIES

TELECOMMUNICATIONS CYBERSECURITY - RECENT DEVELOPMENTS

BRAZIL

São Paulo | Belo Horizonte | Brasília | Rio de Janeiro | Goiânia | Recife
www.azevedosette.com.br

Telecommunications Cybersecurity Recent Developments

By Ricardo Barretto Ferreira and Sylvia Werdmüller von Elgg Roberto

As it has occurred with government authorities in different countries worldwide, the issue of cybersecurity in telecommunications has also been the subject of attention by the Brazilian authorities.

In fact, in Brazil, there are already several regulations dealing with the matter, among which we might mention Decree No. 9637, dated December 26, 2018, which instituted the National Policy for Information Security, Decree No. 10222, dated February 05, 2020, which approved the National Cybersecurity Strategy, and Normative Instruction No. 4, dated March 26, 2020, of the Institutional Security Office of the Presidency of the Republic, which provides for the minimum cybersecurity requirements that must be adopted in establishments of the 5th generation (5G) mobile telephony networks (see the Telecoms Series article entitled "Cybersecurity on Telecommunications Network").

Due to the relevance of the matter, the National Telecommunications Agency ("ANATEL"), the body that regulates telecommunications in Brazil, by means of Resolution No. 740, dated December 21, 2020, recently approved the **Cybersecurity Regulation Applied to the Telecommunications Sector** ("Regulation"), which entered into force on January 4, 2021.

The purpose of the Regulation is to establish conducts and procedures to promote security in telecommunications networks and services, including Cybersecurity and the protection of Critical Telecommunications Infrastructures (art. 1). According to ANATEL, the measure is necessary to reduce the susceptibility to attacks and frauds.

The concept of **Cybersecurity** is given by the Regulation and corresponds to "actions aimed at the security of operations, in order to ensure that information systems are capable of resisting events in cyberspace which might compromise the availability, integrity, confidentiality and authenticity of data stored, processed or transmitted and the services that these systems offer or make accessible" (art. 3, X). **Critical Telecommunications Infrastructures**, in turn, are "facilities, services, goods and systems related to the provision of telecommunications services which, if interrupted or distributed, will cause serious

social, economic, political, international impacts or impact to State security and society" (art. 3, VI).

The Regulation is applicable to all telecommunications service providers of collective interest, except for small-sized providers ("PPP", "Prestadoras de Pequeno Porte" in Portuguese) (art. 2, head provision of the Regulation). The definition of PPP was not covered by the normative; however, it is conferred by ANATEL Resolution No. 694, dated July 17, 2018, which, among other topics, amended the General Competition Goals Plan ("PGMC", "Plano Geral de Metas de Competição" in Portuguese, approved by ANATEL Resolution No. 600/2012). Thus, according to the applicable wording of the PGMC, PPP is the "group holding a national market share of less than 5% (five percent) in each retail market in which it operates."

Still with regard to the definition of PPPs, it is also relevant to note that in Act No. 6539, dated October 18, 2019, ANATEL's Board of Directors specified that providers belonging to Telefônica Group, Telecom Americas Group, Telecom Italia Group, Oi Group and Sky/AT&T Group are not considered PPPs (art. 1). Furthermore, such Act clarifies that, by exclusion, telecommunications service providers not encompassed in the previously mentioned groups are deemed PPPs (art. 2). However, it should be emphasized that the regulation is subject to periodic reviews every two (2) years from its publication, except in exceptional and justified cases; thus, such Act might be reviewed in 2021.

Notwithstanding the above, the Board of Directors might include or dismiss telecommunications service providers of collective or restricted interest, regardless of size, as well as companies holding satellite exploration rights to transport telecommunications and other signals, from the incidence of the Regulation provisions (art. 2, Paragraph 1). However, even though applicability of the regulation might be dismissed, this fact does not exempt the company from complying with other legal and regulatory provisions (art. 2, Paragraph 3).

The Regulation also lists other relevant definitions regarding the regulated matter. Thus, for example, **cyberspace** is the "virtual space composed of a set of internet communication channels and other communication networks which ensure the interconnection of ICT devices and encompasses all forms of digital network activities, including storage, processing and sharing of content in addition to all actions, human or automated, conducted by means of this environment" (art. 3, IV).

Furthermore, in contrast to the aforementioned definition of cybersecurity, **cyber risk** should be understood as the "combination of the consequences of an event associated with a future incident holding the potential to cause compromise or disruption of one or more information technology systems, resulting from failures or breaches in the cybersecurity system, and of the probability of associated occurrence" (art. 3, IX).

According to the Regulation, providers must proceed with the preparation, implementation and maintenance of a Cybersecurity Policy (art. 6), as well as use, in their networks and services, telecommunications products and equipment from suppliers having a cybersecurity policy compatible with the principles and guidelines of the Regulation (art. 7). In addition, among other obligations, providers should also (i) change the standard authentication configuration of equipment made available to users in loan for use (art. 8, caput); (ii) carry out vulnerability assessment cycles (art. 10), by means of an appraising entity or a qualified and independent company, the results of which should be forwarded to ANATEL for confidential treatment (art. 19); and (iii) submit to ANATEL information regarding their Critical Telecommunications Infrastructures (art. 11), which must include, at least, network data and geographic mapping of physical structures and routes (art. 20).

The Regulation establishes certain specific aspects of the Cybersecurity Policy. Thus, among other requirements, such Policy, when providing for conducts and procedures promoting Cybersecurity and the mitigation of risks of Critical Telecommunications Infrastructures, must also (i) be consistent with the customer base, the nature and complexity of products, services, activities, processes and systems; (ii) be disclosed to professionals and collaborators in the applicable areas, with limitations regarding the sharing of sensitive information; (iii) establish the internal structure responsible for the Policy, identifying the competent people and areas, as well as the focal point of contact for emergencies; and (iv) be updated and revised from time to time. Another very important point is that the aforementioned Policy, its complementary documents and respective proof of internal approval thereof should be available to ANATEL whenever requested (arts. 12 and 13).

According to the Regulation, the Cybersecurity Policy should be published on the provider's website according to the terms of Article 15, and must cover several aspects, including norms, standards and references of good cybersecurity practices; procedures relating to the safe storage of user data; procedures and controls adopted regarding the identification and analysis of vulnerabilities, threats and risks related to Cybersecurity, Critical Telecommunications Infrastructures and the continuity of telecommunications services; mapping of possible risks of incidents and events affecting the security of user data storage; and procedures and controls adopted to mitigate vulnerabilities. In addition, it should also provide for the incident response plan, with the definition of actions, resources and responsibilities and, in addition, the procedures relevant to the sharing of information about relevant incidents and other information related to Cybersecurity (art. 14). Annually or upon request, the company should submit to ANATEL a report

regarding the Policy's execution (art. 16.)

Relevant incidents, substantially affecting the security of telecommunications networks and the security of user data, should be notified by the provider to ANATEL, as well as communicated to other providers and users (art. 9 and 17), notwithstanding other legal communication obligations, as occurs, for example, under the General Data Protection Law (Law No. 13709/2018), which came into force in Brazil on September 18, 2020.

At this point, it is worth mentioning that, according to the Regulation, an **incident** is defined as the "action or omission, which has allowed, or which might allow, unauthorized access, interruption or change in operations (including by taking control), destruction, damage, deletion or change of protected information, removal or limitation of the use of protected information or also the appropriation, dissemination and improper publication of protected information of any critical information asset or of any critical activity for a period of time shorter than the objective recovery time "(art. 3, V).

The notification of incidents to be forwarded to ANATEL should include the analysis of its cause and of its impact, in addition to the mitigation actions adopted, as applicable (art. 17, Paragraph 1). The Regulation also determines that telecommunications service providers should adopt a procedure for sharing information on relevant incidents and others related to Cybersecurity, in a confidential and non-discriminatory manner (art. 18).

In addition, according to the regulations, ANATEL (i) will monitor providers' cybersecurity policy (art. 21); (ii) will consider cybersecurity in the conformity assessment and homologation of telecommunications products and equipment (art. 22); and (iii) might determine compliance with technical requirements and adoption of specific cybersecurity measures in the implementation, operation and maintenance of telecommunications networks (art. 23).

Another important aspect of the Regulation is the establishment of the Technical Group on Cybersecurity and Critical Infrastructure Risk Management ("GT-Ciber"), which is responsible for assisting ANATEL in monitoring the implementation of the Cybersecurity Policy and the management of Critical Infrastructures by providers; monitoring the emergence of new technologies and threats, assessing their impact on telecommunications networks and services; preparing studies and proposing improvements in the regulation and administrative decisions related to Cybersecurity, among other attributions listed in article 24. In addition, it is important to note that the GT-Ciber might propose the inclusion or exemption of providers of telecommunications services and others, from the incidence of the terms

of the Regulation.

Adaptation of providers to the Regulation's provisions must occur within 180 (one hundred and eighty) days from its entry into force (art. 27), subjecting violators to the application of administrative sanctions (art. 26).

To receive the main legislative news and positioning on this and other topics related to telecommunications, follow the Technology, Media and Telecommunication (TMT) team of Azevedo Sette Advogados.

São Paulo, February 08, 2021.

Authors

Ricardo Barretto Ferreira da Silva - Senior Partner
barretto@azevedosette.com.br

Sylvia Werdmüller von Elgg Roberto - Associate
selgg@azevedosette.com.br