Azevedo Sette
ADVOGADOS

TELECOMS SERIES

CHANGES TO THE CYBERSECURITY REGULATION APPLIED TO THE TELECOMMUNICATIONS SECTOR

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

BRAZIL

CHANGES TO THE CYBERSECURITY REGULATION APPLIED TO THE TELECOMMUNICATIONS SECTOR

By Ricardo Barretto Ferreira and Sylvia Werdmüller von Elgg Roberto

Resolution No. 767 of the National Telecommunications Agency ("Anatel"), dated August 07, 2024 ("Resolution 767/2024"), recently came into force, introducing changes to the Cybersecurity Regulation Applied to the Communications Sector ("Regulation"), which, in turn, was approved by Resolution No. 740, dated December 21, 2020, of the same Agency.

The Regulation, the application of which began on January 04, 2021, seeks to establish "conducts and procedures for promoting security in telecommunications networks and services", including Cybersecurity and the protection of Critical Telecommunications Infrastructures.

The concept of Cybersecurity is given by the text of the Regulation itself and corresponds to actions aimed at the security of operations, ensuring that information systems have the capacity to resist events in cyberspace that may compromise availability, integrity, confidentiality and authenticity of the data stored, processed or transmitted, as well as the services offered or made available by said systems.

Critical Telecommunications Infrastructures were also defined by the Regulation and are understood as facilities, services, assets and systems related to the provision of telecommunications services that, in the event of interruption or destruction, cause a relevant social, economic, political, international impact, or an impact on Brazilian security and society

Except for small-sized providers (i.e., groups holding a national market share of less than 5% in each retail market in which they operate), the Regulation is applicable to all providers of collective interest telecommunications services, which means that its provisions must be complied with by all operators providing services to any interested parties, under non-discriminatory conditions and in accordance with other applicable regulations.

It is important to note that it is expressly set forth by the Regulation that companies holding rights to operate satellites for transporting telecommunications signals, as well as other legal entities, may become subject to its provisions, or even be exempted from complying therewith, as per Anatel's decision.

Among the changes introduced by Resolution 767/2024, it was established that, regardless of their size, all providers of collective interest telecommunications services must "change the default authentication configuration of equipment provided on a loan basis to their users" (as is the case, for example, with routers). Furthermore, the same Resolution clarifies that the duty to stipulate which equipment this determination applies to, in addition to addressing the procedure related to this requirement, is the responsibility of the Technical Group of Cybersecurity and Critical Infrastructure Risk Management ("GT-Ciber").

Another important change brought by Resolution 767/2024 orders that, regardless of their size, **(i)** operators of submarine cables with international destinations (i.e., "providers responsible for data communication between countries via submarine cable, as well as a set of equipment and facilities necessary to establish such communication"), **(ii)** personal mobile service ("SMP") providers owning their own network, as well as **(iii)** network operators that offer traffic in the wholesale market and which belong to economic groups classified as holding significant market power in the High-Capacity Data Transport Market, are now required to comply with the provisions of articles 6, 7, 9, 10 and 11 of the Regulation. Therefore, we have the following scenario:

- Companies subject to the changes contained in Resolution 767/2024 must prepare, implement and maintain a Cybersecurity Policy in accordance with the terms of the Regulation, i.e., a policy of actions aimed at the security of operations, seeking to ensure that information systems have the capacity to resist events in cyberspace that may compromise availability, integrity, confidentiality and authenticity of the data stored, processed or transmitted, in addition to the services offered or accessible through said systems.

- It is now also mandatory for the aforementioned companies to use telecommunications products and equipment in their networks and services the suppliers of which implement *cybersecurity* policies aligned with the terms of the Regulation

and which carry out periodic independent audits, and the audits' results may be requested by Anatel. However, regarding this point, it is important to note that suppliers that are classified as startups were exempted from these obligations; in this case, operators themselves are responsible for cybersecurity and "for the suitability of the contracted solution to telecommunications networks and their users". According to Complementary Law No. 182, dated June 01, 2021 (legal framework for startups and innovative entrepreneurship), startups are defined as "business or corporate organizations, new or in recent operation, the performance of which is characterized by innovation applied to the business model or products or services offered".

- Relevant incidents that substantially affect the networks' security, as well as users' data, must be notified to Anatel and communicated to other operators and to users.

- Cybersecurity-related vulnerability assessment cycles must be carried out by companies.

- Providers must submit information about their Critical Telecommunications Infrastructures to Anatel.

Another requirement introduced into the text of the Regulation due to the entry into force of Resolution 767/2024 refers to the obligation for telecommunications service providers to inform Anatel about incidents that need to be reported

to the National Data Protection Authority ("ANPD"). This is a positive point, which reaffirms Brazil's commitment to protecting personal data in the most diverse spheres of economic activity.

In addition to other requirements already described in the original text of the Regulation, Resolution 767/2024 determined that the Cybersecurity Policy must cover cybersecurity aspects related to the contracting of data processing and storage and cloud computing services that are used by providers, and these assessments include **(i)** the supplier's capacity and the compatibility of its practices with the Regulation's principles and guidelines; **(ii)** risk mapping; **(iii)** procedures and controls aimed at mitigating risks that encompass critical network functions and personal data processing; and **(iv)** the complexity of incident management in cases involving data located abroad.

Finally, it should be noted that through Ordinance No. 2899, dated September 16, 2024 ("Ordinance 2899/2024"), Anatel identified the providers and operators which must comply with the cybersecurity requirements, as follows:

- Providers not considered as PPPs: Telefônica Brasil S.A., Fibrasil Infraestrutura e Fibra Ótica S.A., Telxius Cable Brasil Ltda. (Telefônica Group); Claro S.A., Embratel TVSat Telecomunicações S.A., Americel S.A., Telmex do Brasil S.A., Claro NXT Telecomunicações S.A. (Telecom Americas Group); TIM S.A., I-Systems Soluções em Infraestrutura S.A. (Telecom Italia Group); and V.Tal – Rede Neutra de Telecomunicações S.A., Oi S.A., Oi Soluções S.A. (Oi Group).

- Submarine cable operators: Globenet Cabos Submarinos S.A.; Angola Cables Brasil Ltda.; Cirion Technologies do Brasil Ltda.; China Unicom do Brasil Telecomunicações Ltda.; Cabo Brasil Europa Ltda.; and Seabras 1 Brasil Ltda.

- SMP providers with their own network: Algar Telecom S.A., Sercomtel S.A. Telecomunicações; Brisanet Serviços de Telecomunicações S.A.; Unifique Telecomunicações S.A.; and Ligga Telecomunicações S.A.

- Network operators offering traffic in the wholesale market belonging to economic groups classified as holding significant market power in the High-Capacity Data Transport Market: Algar Telecom S.A.; and Ligga Telecomunicações S.A.

At last, it should be noted that according to the text of the Regulation, from the date of publication of Ordinance 2899/2024 (which occurred on September 27, 2024), companies have a period of one year to make the necessary adjustments.

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, November 26, 2024

Autores

Ricardo Barretto Ferreira da Silva - Sócio Sênior
barretto@azevedosette.com.br

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