



ANTI-PIRACY WHITE PAPER

HISTORY, INTERNATIONAL BENCHMARK, RESULTS OBTAINED AND CHALLENGES FACED

National Telecommunications Agency

SAUS Quadra 06, Blocos C, E, F e H

CEP 70.070-940 - Brasília/DF

Phone: (61) 2312-2000 – www.gov.br/anatel

President

Carlos Manuel Baigorri

Board of Directors

Vicente Bandeira de Aquino Neto

Alexandre Reis Siqueira Freire

Octavio Penna Pieranti

Edson Holanda

Superintendencies

Daniel Martins D'Albuquerque – Superintendent of Administration and Finance (SAF)

José Borges da Silva Neto – Superintendent of Competition (SCP)

Suzana Silva Rodrigues – Superintendent of Obligations Control (SCO)

Gesilêa Fonseca Teles – Superintendent of Inspection (SFI)

Gustavo Nery e Silva – Superintendent of Internal Information Management (SGI)

Vinícius Oliveira Caram Guimarães – Superintendent of Granting and Provision of Resources (SOR)

Nilo Pasquali – Superintendent of Planning and Regulation (SPR)

Cristiana Camarate Silveira Martins Leão Quinalia – Superintendent of Consumer Relations (SRC)

Gustavo Santana Borges – Executive Superintendent (SUE)

Advisory and related entities

Daniel Leite Santos França – Head of the Parliamentary and Social Communication Advisory

Andrea Mamprim Grippa – Head of International Advisory (AIN)

Maria Lúcia Valadares e Silva – Head of the User Relations Office (ARU)

Dagma Sebastiana Caixeta de Macedo – Head of the Institutional Relations Office (ARI)

João Marcelo Azevedo Marques Mello da Silva – Head of Technical Advisory (ATC)

André Garcia Pena – Head of Internal Audit (AUD)

Silvio Andrade dos Santos – Internal Affairs Officer (CRG)

Felipe Augusto Esmeraldo de Oliveira – Ombudsman



NATIONAL TELECOMMUNICATIONS AGENCY

Anti-Piracy White Paper: HISTORY, INTERNATIONAL BENCHMARK, RESULTS OBTAINED AND CHALLENGES FACED

Coordinator

Alexandre Reis Siqueira Freire

BRASÍLIA-DF
2025



Research Team

Coordination

Alexandre Reis Siqueira Freire

Authors

Office of Chief Executive Officer Alexandre Freire

Alexandre Reis Siqueira Freire

Ailfran Moraes Martins

Leonardo Albuquerque Marques

Superintendence of Inspection

Gesilêa Fonseca Teles

Marcus Vinicius Galletti Arrais

Jamilson Ramos Evangelista

Eric Magalhães Delgado

Marcel Fleury Pinto

Sérgio Campos

Paulo Aurélio Pereira da Silva

Ana Paula Mendonça Abrão

Eduardo Lustosa Rege

Eduardo Hiroshi Murakami

José Afonso Cosmo Júnior

Marcello Vieira Mascarenhas

Allan Robson Cruz

Superintendence of Inspection

Gesilêa Fonseca Teles

Superintendence of Granting and Provision of Resources

Geraldo Magela Benício Junior

Cataloguing at the source – Anatel Library

W582 Anti-piracy White Paper: history, international benchmark, results obtained and challenges faced [electronic resource] / coordinator: Alexandre Reis Siqueira Freire – Brasília : Anatel, 2025.

1 online resource [106 p.] : il.

Access mode: World Wide Web.

Digital publication (e-book) in PDF format.

Various authors.

1. Piracy. 2. Telecommunications product. 3. Products certification. 4. Product approval. 5. Telecommunications sector. 6. Government regulation. I. National Telecommunications Agency (Brazil). II. Freire, Alexandre Reis Siqueira (coord.). III. Title.

CDD 343.099

Catalogue sheet prepared by Carolina Pereira Marinho – CRB1/2275

How to quote this book:

FREIRE, Alexandre Reis Siqueira (coord.). **White paper combate à pirataria**: histórico, benchmark internacional, resultados obtidos e desafios enfrentados. Brasília: Anatel, 2025. e-Book. (1 recurso online (106 p.)), il.

National Telecommunications Agency
SAUS, Quadra 6, Bloco C, E, F e H
CEP: 70.070-940 – Brasília/DF
Phone: (61) 2312-2000
Website: www.gov.br/anatel

TABLE OF CONTENTS

PRESENTATION	5
1. OVERVIEW OF PIRACY IN THE TELECOMMUNICATIONS SECTOR IN BRAZIL	10
1.1. Conformity assessment system	11
1.2. Conformity Assessment (Regulatory Basis)	12
1.3. Anatel's certification model	16
1.4. Anatel's inspecting practices	23
1.5. Market growth and piracy in the context of telecommunications.....	24
1.6. Physical and Digital Risks to Users	25
2. ACTIONS TO COMBAT PIRACY AND THEIR REACTIONS	36
2.1. PACP – Action Plan to Combat Piracy	36
2.2. Combating Piracy in Marketplaces.....	42
2.3. Partnerships with public administration entities	46
2.4. Evolution of legal understanding (marketplace, social media and distribution chain).....	51
2.4.1. <i>MARKETPLACE LIABILITY</i>	52
2.4.2. <i>ACCOUNTABILITY OF SOCIAL MEDIA (YOUTUBE AND FACEBOOK)</i>	59
2.4.3. <i>ACCOUNTABILITY OF THE PRODUCT SUPPLY CHAIN</i>	59
2.5. Plan to Combat the Use of Clandestine Decoders.....	67
3. OTHER ADMINISTRATIONS ACTIONS TO COMBAT PIRACY	74
3.1. Combating piracy in e-commerce	74
3.3. Combating the connection of non-approved equipment and access to content.....	81
3.4. Multilateral Partnerships and Global Forum.....	88
4. FUTURES CHALLENGES AND OPPORTUNITIES	90
4.1. Key Challenges	90
4.2. Future Opportunities.....	91
REFERENCES	93

PRESENTATION

Telecommunications services are one of the pillars of Brazil's economic and social development. Its use, whether in the daily experience of consumers or in the provision by the companies that make up the sector, must ensure the protection of the fundamental rights of users, the balance of competition and strict compliance with the legislation. In this sense, the fight against piracy of telecommunications products and services undertakes a strategic position in Anatel's acting, not only as a measure to repress illicit acts, but as an essential action to preserve the quality, security and integrity of national networks.

This White Paper presents, in a comprehensive and grounded manner, the set of initiatives undertaken by the Agency to address this challenge. The document gathers technical data, legal analysis, updated statistics and detailed descriptions of operational strategies, while highlighting the results already achieved through inspection operations, seizures of irregular devices, technological blockades and regulatory measures that reinforce the protection of the sector. It is, therefore, an institutional report that combines technical rigor with a strategic vision of the future.

Piracy, more than a one-off problem, is a systemic threat. Its impacts range from the degradation of the quality of services to the compromise of free competition, harming companies that operate within the law and discouraging new investments. In addition, irregular products and services expose users to increasing cybersecurity risks, opening space for sophisticated criminal practices and putting trust in the digital ecosystem in check. Combating such practices, therefore, is an indispensable condition for building a competitive, innovative, and safe environment.

To fulfill this mission effectively, Anatel has acted in an articulated manner with government agencies, private sector entities and civil society, recognizing that only the coordinated action of all actors will allow lasting results. This cooperation strengthens both prevention mechanisms and instruments of repression, increases the population's awareness and fosters joint solutions of a structural nature.

The advances already achieved demonstrate the relevance of this strategy. The operations carried out show not only the effectiveness of the inspection instruments, but also the Agency's ability to innovate in the application of regulatory measures that raise the level of reliability in the sector. However, market dynamics and the speed of technological transformation impose new challenges, such as the exponential growth of the Internet of Things, the sophistication of cybercrime practices, and the need to intensify international cooperation to contain a phenomenon that crosses borders.

Thus, this White Paper is not limited to presenting actions already carried out, but seeks to reaffirm Anatel's commitment to transparency, institutional responsibility and the defense of the public interest. By inviting readers to explore its content, the Agency reinforces its determination to lead the construction of integrated and sustainable solutions to effectively combat piracy. More than a technical document, it is a manifestation of commitment to the future of telecommunications in Brazil: a future that must be marked by quality, safety, innovation and mutual trust between society, the productive sector and public authorities.



Carlos Baigorri
Presidente da Anatel



Alexandre Freire
Conselheiro Diretor da Anatel

INTRODUCTION

Telecommunications networks are composed of a set of equipment that enables the providing of distance communication services, such as transceivers (radio communication, such as mobile phones, for consumer use, and Radio Transceiver Stations - RTSs, used by providers) and their peripherals (antennas, chargers, batteries, etc.), which use scarce public resources (radio frequency spectrum and orbit), and devices that allow information to travel through physical media (copper cables, coaxial cables, fiber optic cables, etc.).

The concept of telecommunication can be extracted from Article 60, § 1, of Law No. 9,472, of July 19, 1997 - General Telecommunications Law - GTL:

Article 60. (...)

Paragraph 1 - Telecommunication is the transmission, emission or reception, by wire, radioelectricity, optical means or any other electromagnetic process, symbols, characters, signs, writings, images, sounds or information of any nature.

This equipment must support the providing of telecommunications services under minimum quality and safety standards, ensuring consumer protection, both physical and cybernetic, and observing the applicable Brazilian and international legislation, especially regarding the regular use of the radio frequency spectrum.

This entire set of obligations, which derive from the provisions of the GTL, is ensured by regulatory rules, of which those on certification/approval of equipment stand out, representing an instrument for the management of telecommunications networks, based on the establishment of basic parameters for the use and connection of telecommunications. No desempenho de sua missão institucional, a Anatel vem adotando uma série de medidas

equipment to the networks, in addition to the guarantee of origin, technical support and legal liability of manufacturers.

In performing its institutional mission, Anatel has been adopting a series of measures aimed at identifying, preventing and repressing illegal practices associated with the use of non-approved products and the misuse of telecommunications networks. Such actions include inspection operations aimed at removing irregular products from the market and blocking clandestine devices, public awareness campaigns, and coordination with other public agencies, such as the Brazilian Internal Revenue Service and the Ministry of Justice and Public Security, as well as partnerships with the private sector.



Anatel's action in the fight against piracy is based on the current legal and regulatory framework, which requires the certification of telecommunications products, curbs the misuse of spectrum and the unauthorized use of services. However, technological advances, globalization — especially e-commerce — and the complexity of illicit distribution chains and network use impose the need for a more strategic, cooperative, and evidence-based approach.

This White Paper presents the technical, administrative and legal bases for the certification

against piracy. It offers a broad view of the problem, the mechanisms of action, the results obtained and the ways to improve public policies in the sector.

Gathering data, case studies, practical experiences and normative foundations, this document seeks to support decision-makers, regulated agents, researchers and other stakeholders in the fight against piracy, in favor of a safer, more reliable and fairer digital ecosystem for all Brazilians.

1. OVERVIEW OF PIRACY IN THE TELECOMMUNICATIONS SECTOR IN BRAZIL

Anatel, according to Articles 19, XII and XIII, and 162, paragraph 2, of the GTL, has the competence to certify or recognize telecommunications products, and the use of radio frequency emitting equipment without this certification is prohibited. Under the terms of Article 1st, sole paragraph, of the GTL, its activities include the discipline and inspection of networks, the radio frequency spectrum and orbit resources.

Without the rules for assessing the conformity and approval of these products, there is no guarantee of safety, quality, or compatibility of equipment – enabling potential interference in services, electrical risks, battery explosions, excessive exposure to non-ionizing radiation, and cybersecurity vulnerabilities.

The conformity assessment and approval of telecommunications products ensure legal certainty and consumer protection, ensuring the accountability of suppliers and the protection of the most vulnerable party – the Brazilian consumer. Anatel evaluates these conditions before the release of the products to the market, prohibiting the sale of equipment that does not meet the safety requirements.

Before dealing with illegal trade, it is necessary to understand the Brazilian System for Conformity Assessment of Telecommunications Products.



1.1. Conformity assessment system

The conformity assessment system is a standardized process, with pre-established rules, duly monitored and evaluated, in order to provide an adequate degree of confidence that a product, process or service, or even a professional, meets pre-established requirements in accordance with standards or regulations. According to the International Organization for Standardization, ISO/IEC 17000 standard, it is the activity that allows demonstrations that specific requirements related to products, processes, services, systems, people or organizations are met.

The conformity assessment models by certification, provided for in the Regulation on Conformity Assessment and Approval of Products for Telecommunications, are based on the types of certification schemes described in ISO/IEC 17067 standard, which presents the fundamentals for product, process or service certification, and provides guidelines for certification programs/schemes.

The management systems of telecommunications product certification entities must be based on the ISO/IEC 17065 standard, which defines the requirements for certification entities for products, processes and services, as well as testing and calibration laboratories.

Finally, the technical requirements, defined by Anatel regulations, follow normative references established by international standardization entities, such as ITU, 3GPP, IEEE, IEC, among others.

Thus, the conformity assessment process of telecommunications products is developed based on international standards, ensuring alignment with the standards adopted worldwide, so that the level of reliability appropriate to its results is ensured.

1.2. Conformity Assessment (Regulatory Basis)

The legal discipline to curb the sale of products not approved by Anatel is based, essentially, on the following precepts of the GTL:

Article 19. The Agency is responsible for (...)

XIII – issue or recognize the certification of products, in compliance with standards and norms established by it;

Article 156. (...)

Paragraph 2 – certification is the recognition of compatibility of specifications of a given product with the technical characteristics of the service for which it is intended.

Article 162. (...)

Paragraph 2 – the use of radio frequency emitting equipment without certification issued or accepted by the Agency is prohibited.

The Regulation for Conformity Assessment and Approval of Telecommunications Products, approved by Anatel Resolution No. 715, of October 23, 2019, and updated by Anatel Resolution No. 780, of August 1, 2025, details these precepts:

Article 55. Approval is a mandatory prerequisite for the use

and commercialization, in the country, of products covered by this Regulation.

Article 63. Approved products must contain the identification of the approval, according to the operational procedure.

Articles 83. The following conducts are subject to sanctions, subject to specific legislation and regulations:

I – use or utilization of non-approved product; (...)

IV – commercialization of non-approved products; (...)

IX – disclosure of an invalid approval code or belonging to another equipment in an advertisement for a non-approved product;

X – importing of non-approved product.

Additionally, it is important to highlight the logic of the Agency's action in the face of the commercialization of non-approved products.

The GTL and the infra-legal normative design formulated by the regulatory entity for assessing the conformity of telecommunications products is a product of the new model of state action in the infrastructure sector established in Brazil in the 1990s, in which the State went from being a producer to a regulator.

Under this new model of state action, which in the telecommunications sector was driven by the Constitutional Amendment No. 8/1995, broke the state monopoly on telecommunications services and provided for the creation of a sectoral regulatory entity gifted with technical capacity and infra-legal normative powers, framing a legal structure with the contours given by the GTL, a legal structure that defined the arrangement of exploration of telecommunications services in Brazil.

Among the rules that determine the implementation and operation of networks, Article 156

of the GTL provided for the certification of products as an instrument for the management of telecommunications networks, determining that the connection¹ may be prohibited for equipment without certification issued or accepted by the Agency. The second paragraph of this article defines certification as the recognition of the compatibility of the specifications of a given product with the technical characteristics of the telecommunications service for which it is intended.

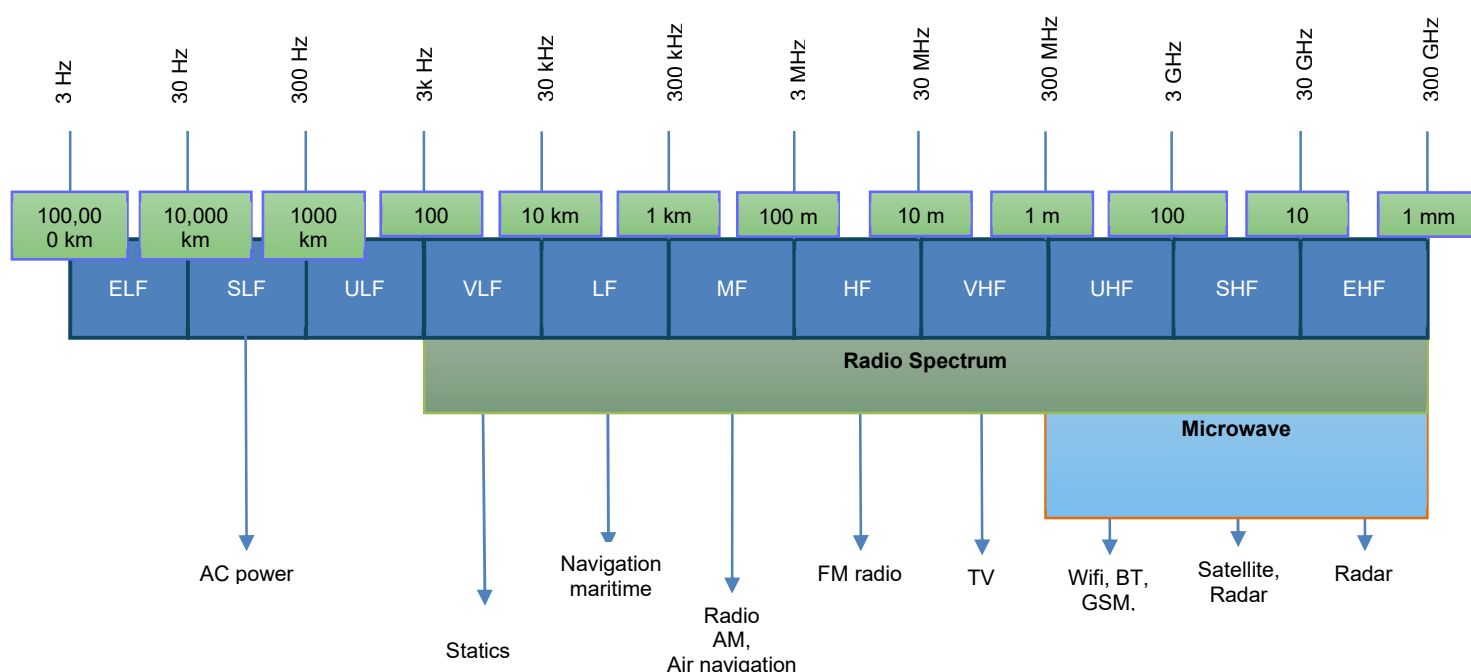
Telecommunications networks must be organized as integrated routes of free circulation, in which the interconnection between the networks of the various providers is mandatory, as well as the integrated operation at the national and international levels, and the right of ownership over the networks is conditioned by the duty to fulfill their social function.

Certification requirements, as extracted from their own definition, are responsible for determining the operating parameters of equipment used in telecommunications networks. This process has a double function: first, to define parameters of reliability of the equipment used in national telecommunications networks, enabling the fruition of information with quality and safety, according to the state of the art of technological development worldwide; and second, protection of the local consumer regarding the safety and reliability of the equipment.

The certification is especially important for the management of the radio frequency spectrum, a finite public good, managed by Anatel. At the current stage of telecommunications development, it is noted that the massification of services is offered through wireless networks and it is through compliance with the requirements of product

¹ In technical vocabulary, a connection or interconnection is the linking of a user's terminal or network to public telecommunications networks. Available at: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2018/1142-resolucao-693>. Accessed on: Jul 7, 2025.

certification (also of the licenses to operate stations) that the rules for the use of the spectrum and, as a consequence, for the traffic of information in telecommunications networks are respected.



Thus, a product, in order to be approved by Anatel and consequently be compatible with the telecommunications service for which it is intended, must be safe for the consumer (according to the state of the art of technological development), current (operate according to the appropriate technology at the time of approval) and comply with Brazilian telecommunications regulations (such as the conditions of use of the radio frequency spectrum).

If, for the operation of the networks, the Law determines that connections of terminal equipment without certification may be prohibited (Article 156, caput, of the GTL), when it

comes to the use of the radio spectrum, certification is mandatory and a sine qua non condition for the use of the product. Thus, Article 162, § 2, of the GTL prohibits the use of radio frequency emitting equipment without certification issued or accepted by the Agency.

For no other reason, the GTL, recognizing certification as an important instrument for network management, attributed to Anatel the competence to issue norms and standards to be complied with by telecommunications service providers regarding the equipment used.

From the legal competence determined by Article 19, XIII, of the GTL, Anatel issued its resolutions establishing the Brazilian model for conformity assessment of telecommunications products, forming an exception to the competence of the National Institute of Metrology, Quality and Technology - Inmetro, as a metrology body for the various branches of the national economy.

1.3. Anatel's certification model

Initially, it is important to note that the process of certifying equipment in Brazil began with the State at the end of the 1940s. Since that time, the central concern has been to ensure the monitoring and control of the equipment used in the country, as well as their submission to tests and evaluations. Such rigor intended at proving compliance with the technical specifications of the services to be made available.

In the following years, with the evolution of telecommunications systems, the equipment certification process improved. It is relevant to note that, before the creation of Anatel, the General Telecommunications Norm No. 004/91 (GTN 004/91), approved Ordinance No. 173, of August 21, 1991, by the Ministry of Infrastructure, was the first to establish systematized rules and procedures regarding the certification of telecommunications products in Brazil. The scenario was very different, where the state was the telecommunications service

provider, limited to fixed telephony. Throughout the evolution of telecommunications, the state goes from being a provider to a regulator with the growing increase in products that can be certified in an open and competitive market.

Period	Predominant Technology	Types of Devices	Relative Volume	Regulatory Impact
1980s	Landline telephone	Telephones	Low	State Monopoly
1990s	Dial-up internet	PCs, modems	Average	Certification of analog terminals
2000s	Broadband	Modems, routers, STBs	High	Multiprotocol certification
2010s	3G/4G	Smartphones, tablets	Very high	Expansion of RF certification
2020s	5G / IoT	Smart devices, automation	Massive	Regulatory update and digital security

The certification model currently in force, considering Anatel's duties and competencies related to the subject, was initially implemented by Resolutions No. 242, of November 30, 2000, and No. 323, of November 7, 2002, which were succeeded by Resolution No. 715, of October 23, 2019 and Resolution No. 780, of August 1, 2025 (which updated and complemented them), approving the Regulation for Conformity Assessment and Approval of Telecommunications Products. This Regulation standardizes the entire certification process within Anatel and is supported by secondary technical rules, named operational procedures and technical requirements, which detail the form and technical parameters necessary for the approval of a product.

This Regulation (approved by Resolution No. 715/2019) identifies a two-phase process that results in the approval of a product.

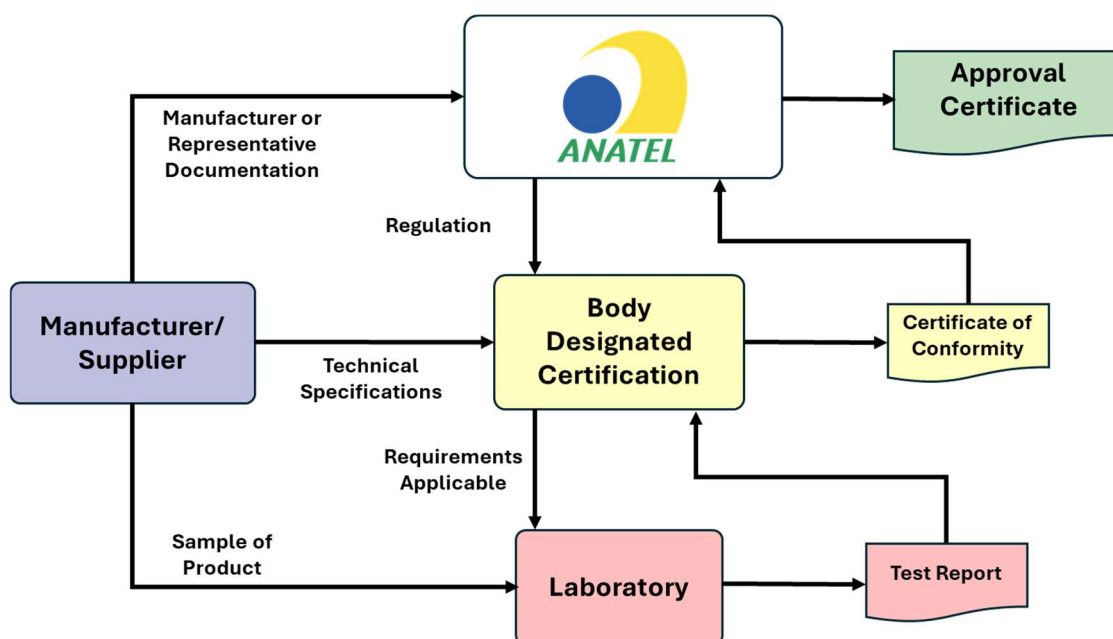
The first phase is the evaluation of the product's conformity, in which agents external to Anatel act. Or the conformity assessment is conducted by declaration of conformity (DC,

provided for in Article 29, I and II, of the Regulation), in which the interested party itself attests to the conformity of the product, an exceptional situation for the Brazilian model (generally applicable to artisanal products or products imported for personal use, see Article 33 of the Regulation), or the conformity assessment is done by certification of technical conformity (CCT, provided for in Article 29, III to V, of the Regulation), in which the entire operation is done through a service provision contract involving a Designated Certification Entity - OCD (responsible for conducting the certification process, see Article 36), a qualified test laboratory (chosen by the applicant for approval, see Article 18) and the interested party in the homologation. It should be noted that both OCDs and qualified laboratories are legal entities governed by private law that generally act in the certification of products for various branches of the economy (many of them accredited by Inmetro). The certification of technical conformity is applicable to products intended for commercialization, such as mobile phones (see Article 32 of the Regulation). Therefore, this stage generally involves technical and laboratory analyses, done by OCD and a qualified testing laboratory, with technical capacity recognized by Anatel, to analyze the scope of the product. The result of this step is the issuance of the Certificate of Technical Conformity (CCT), an indispensable condition for the approval of the product.

The second phase consists of the analysis conducted by Anatel, which takes place within the Agency, on compliance with the objective criteria (adequacy of the issuance of the CCT to the rules previously issued by Anatel) and the subjective criteria (which refer to the legitimacy of the approval request and the ability of the interested party to be responsible for the product in the country), which results in the state seal for the use and commercialization of the product for telecommunications in Brazil. The result of this step is the Homologation Certificate.

The approval of the CCT is a prerequisite for the use and commercialization of telecommunications products in the country. The extent of rights arising from this approval

(meaning the right to use the product or right to use and market it) depends on the type of conformity assessment that was employed, according to Articles 55 and 64 of the Regulation approved by Resolution No. 715/2019.



Articles 32 and 33 of the aforementioned Regulation define under what condition the conformity assessment should preferably be done (by certification of conformity or by declaration of conformity). And by virtue of Article 31, the definition of the models available for the conformity assessment of telecommunications products must consider the application, the complexity of the equipment and the potential risk of its use for the user.

For each family of telecommunications products (e.g. access terminal stations, optical cables, antennas, etc.), Anatel establishes a set of technical requirements and defines a manner of conformity assessment, which can be more or less interventional, depending on the relevance of the product in the telecommunications scenario (for the user, for telecommunications services, for the network, for the national telecommunications policy, etc.).

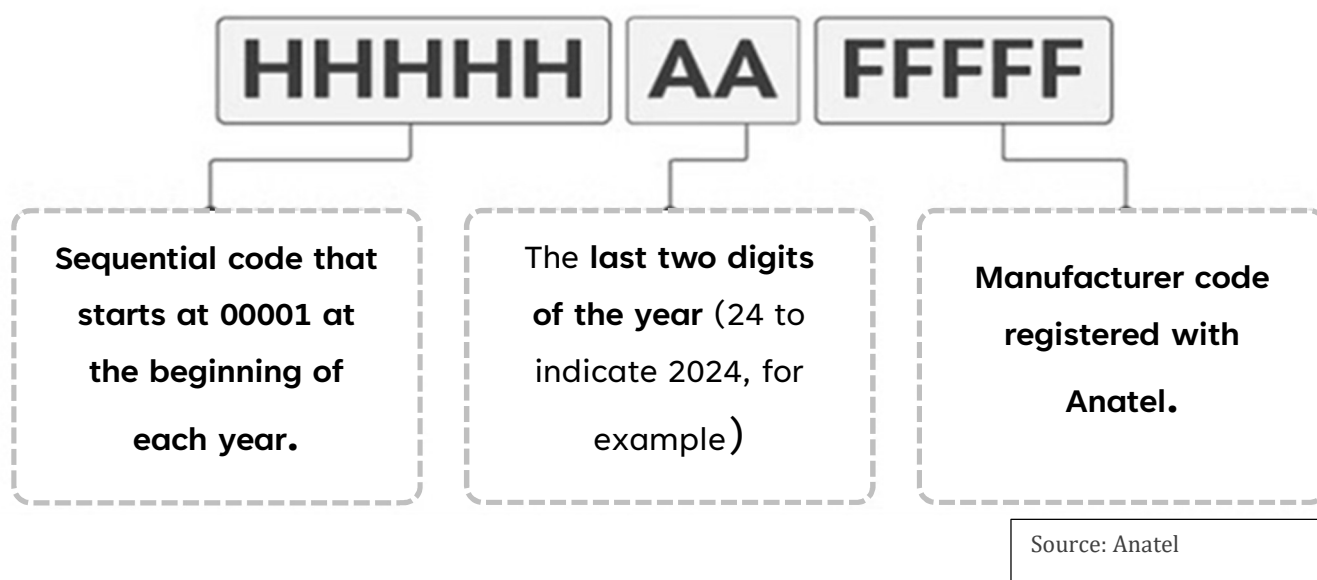
Still within the scope of its competences, and considering the provisions of Article 55, paragraph 1, updated by Resolution No. 780/2025, Anatel had already issued Act No. 4,521, of June 21, 2021, approving the operational procedure for importing telecommunications products. This procedure establishes conditions for the importation of compulsory approval products, whether these products are for personal use, commercialization, evaluation of the conformity of samples or demonstration.

From the consumer's perspective, the rules on the identification of approval are also important. Approved products must bear the identification of approval as set out in the corresponding operating procedure. There are two types of marking required by the sectoral regulation: the first concerns the identification of Anatel's homologation, and the second concerns the homologation security seal for lithium batteries and chargers.

Regarding the identification of the homologation, Act No. 4,088, of July 31, 2020, was published, approving the operational procedure for marking the identification of the Anatel homologation in telecommunications products, and defining the Homologation Code (12 (twelve) digits combination that identifies each approved product), the Anatel Logo, the Anatel Signature (expression "National Telecommunications Agency") and the Anatel Seal (formed by the Anatel Logo and the numerical code of approval, accompanied or not by the Anatel Signature). The responsibility for identification lies with the national manufacturer of the telecommunications product, regardless of the location of the manufacturing units; the manufacturer's legal representative, in the case of an imported product; and the user, in cases of products imported directly for personal use, or of non-commercial artisanal products, for example.

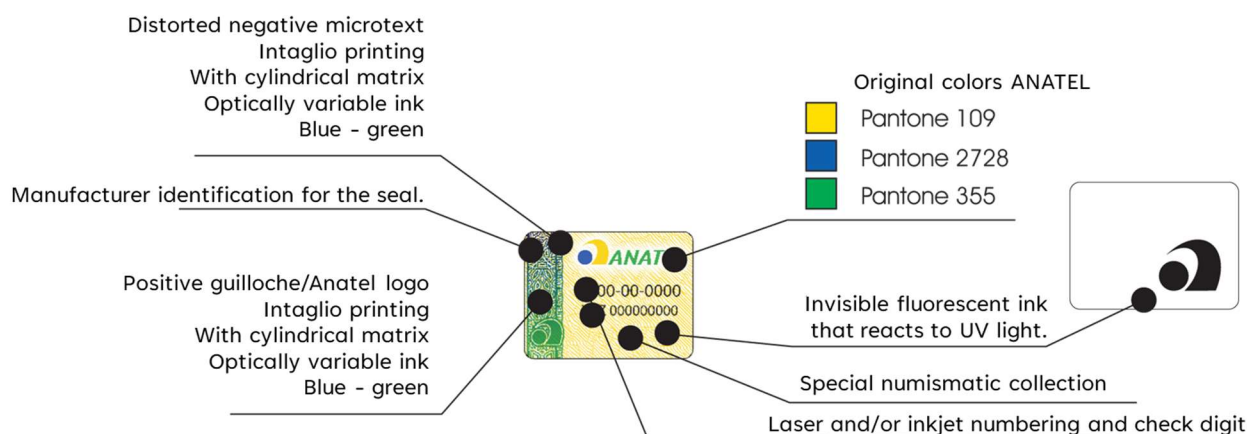


EXAMPLES OF ANATEL SEAL



The security seal consists of the form of identification of approval for specific products defined by the Agency, which have a production control and tracking system, allowing for protection against counterfeiting, diversion, smuggling, undue alterations or duplications of the Anatel Seal from the monitoring of the production chain. This matter is governed by the operating procedure approved by Act No. 14,010, of October 4, 2022, and applies to those interested in the sale of lithium batteries and chargers for mobile phones, as well as to

printing companies, duly qualified to supply security seals, in the exercise of their functions as agents in the conformity assessment process of telecommunications products.



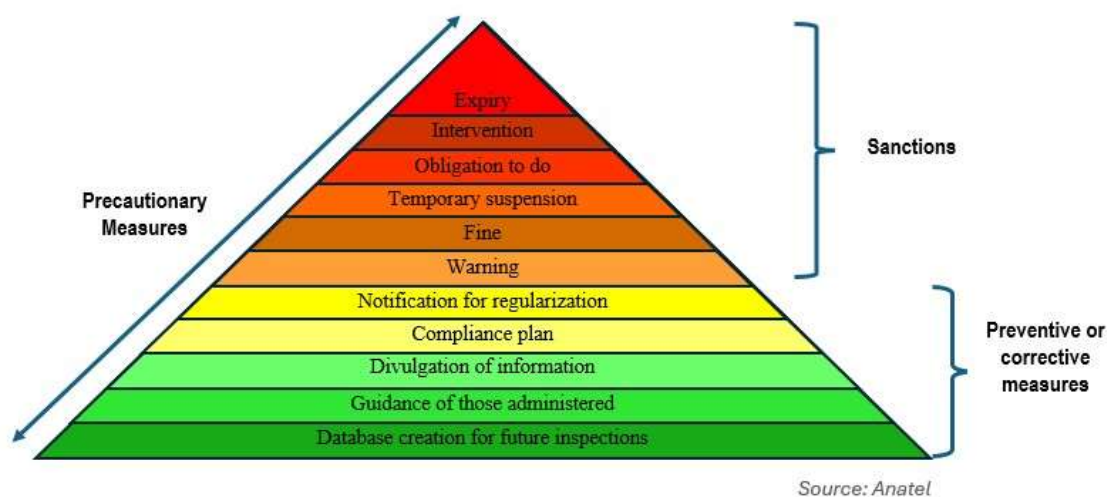
Given its complexity, the structure that leads to the approval of a telecommunications product is not accessible to the common consumer, which requires the regulatory body to make an extra effort to raise awareness of its importance. This fact is reflected in the market and in economic agents in general.

1.4. Anatel's inspecting practices

Anatel's actions in the sector have evolved significantly towards a more modern, efficient and responsive regulatory model. In this context, Resolution No. 746/2021, which establishes the Regulatory Oversight Regulation, introduces an approach based on prevention, incitement to voluntary compliance, and prioritization of risks, while Resolution No. 589/2012, which deals with the Administrative Sanctions Regulation, maintains the necessary legal framework for accountability and punishment of infringing conduct. The interaction between these two normative instruments translates into an integrated strategy that balances regulatory education and application of sanctions, promoting both spontaneous compliance with the rules and effective accountability when necessary.

Resolution No. 746/2021 recognizes that inspection must go beyond simple repression, adopting practices that encourage regular behavior through guiding actions, educational campaigns, and warnings. This approach seeks to dialogue with the regulated, identify weaknesses and encourage corrections before adopting punitive measures. Resolution No. 589/2012, on the other hand, comes into play when there is resistance, recurrence or seriousness of infractions, guiding the proportional and motivated application of sanctions, such as formal warning, fine, suspension or revocation of the grant.

The correlation between the two regulations allows Anatel to act gradually and responsively, adjusting its response according to the profile of the regulated agent and the nature of the infraction. Agents who demonstrate good faith and willingness to correct their conduct can be treated as a priority with educational measures. On the other hand, repeated, intentionally damaging conduct or conduct that causes harm to public order, consumers or the integrity of the sector requires a firm and exemplary sanctioning response.



This integration strengthens the pedagogical function of regulation, promotes an environment of greater legal certainty, reduces litigation, and encourages the construction of a regulatory culture based on dialogue, transparency, and accountability. By strategically combining education and sanctions, Anatel positions itself as a modern agency, focused not only on control, but also on the formation of a more conscious, ethical market committed to the public interest.

1.5. Market growth and piracy in the context of telecommunications

In recent decades, Brazil has experienced significant growth in demand for

telecommunications services, driven by the democratization of access to the internet, mobile telephony, and the distribution of digital content. However, this technological advance has not been accompanied, in many cases, by the expansion of digital education and awareness of the risks associated with the use of irregular products. At the same time, factors such as economic informality, the high tax burden on electronic equipment and the ease of access to international online commerce platforms have contributed to the emergence of a robust parallel market, with a wide supply of non-approved telecommunications equipment, considered pirated products, without proven safety and quality, without confirmation of origin, without technical support to the user and harmful to the economic sustainability of the sector.

In this context, Anatel's actions has become essential, not only for the protection of the regulated sector, but, mainly, to ensure the security and right of consumers to reliable telecommunications services, in accordance with technical and legal standards. Piracy compromises the proper functioning of networks, interferes with emergency services, harms tax collection, and fosters illicit practices that generate technical and legal risks to society.

1.6. Physical and Digital Risks to Users

The use of non-approved telecommunications equipment represents a real risk to the physical and digital security of users. Non-certified devices can cause harmful electromagnetic interference, overheating, electric shocks, and even fires, putting the physical integrity of consumers and networks at risk. In the digital sphere, the risks are equally worrisome, since many of these devices come with altered software, backdoors (a method that allows bypassing normal security measures and gaining privileged access to a system, network, or application), and mechanisms that expose users to data interception, theft of personal information, and cyberattacks (such as pre-installed malicious applications).

Considering the context of telecommunications services, especially those that use the radio spectrum, cases of harmful interference caused by non-approved equipment are perceived by operators based on complaints from users or by monitoring the quality of the networks. In most cases, when Anatel is called, after exhaustive field investigation work, it is common to find, as a motivator for the perceived problems, low-quality equipment or equipment destined for other countries, purchased in e-commerce without going through the certification process established by Anatel².

In addition to the damage to telecommunications services, many devices that use radio frequencies are used for criminal practice. Gangs linked to cargo theft use signal blockers, known as jammers, to block trackers and driver communication while approaching and removing valuable cargo³. Another criminal practice appropriates electronic devices that use radio frequencies to copy wireless control codes from electronic gates or vehicle keys. One of the objectives is home theft⁴, or even vehicle theft, which reveals the vulnerability of these equipment⁵. It was in order to inhibit the proliferation of this type of device that Anatel seized many devices known as "Flipper Zero", imported via e-commerce, resulting in the notification of the main marketplaces in the country to block ads for these

² BRAGA, Lucas; FAVRETTO, Everton. Anatel multa clínica veterinária por usar produto sem homologação. **Tecnoblog**, Feb 23, 2021. Updated on Nov 14, 2023. Available at: <https://tecnoblog.net/noticias/anatel-multa-clinica-veterinaria-por-usar-produto-sem-homologacao/>. Accessed on: Jul 7, 2025.

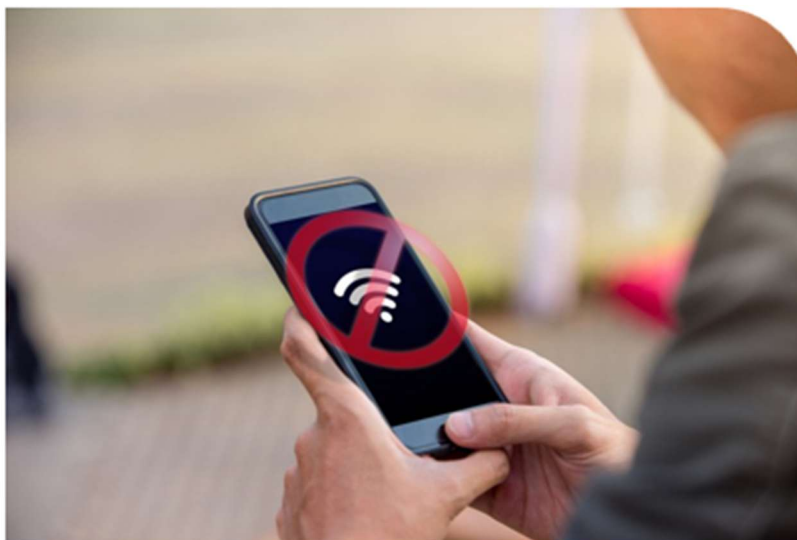
³ POLÍCIA apreende bloqueador de sinal de GPS usado por quadrilha de roubos de cargas no Rio. **G1**, Rio de Janeiro, Feb 14, 2019. Available at: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/02/14/policia-apreende-bloqueador-de-sinal-de-gps-usado-por-quadrilha-de-roubos-de-cargas-no-rio.ghtml>. Accessed on: Jul 7, 2025.

⁴ ALMEIDA, Esther. Dono de construtora morto em SP: saiba como evitar clonagem de controle de portão. **O Globo**, Rio de Janeiro, Jun 7, 2025. Updated on Jul 7, 2025. Available at: <https://oglobo.globo.com/economia/tecnologia/noticia/2025/06/07/dono-de-construtora-morto-em-sp-saiba-como-evitar-clonagem-de-controle-de-portao.ghtml>. Accessed on: Aug 7, 2025.

⁵ GOLPE da chave: bandidos já clonam sinal à distância e levam seu carro. **UOL**, Oct 5, 2023. Available at: <https://www.uol.com.br/carros/noticias/redacao/2025/01/04/bandidos-em-dupla-ja-clonam-chave-a-distancia-e-levam-carro-em-segundos.htm>. Accessed on: Jul 7, 2025.

products⁶.

In the context of the physical integrity of users of telecommunications products, in a recent internet survey by the Agency, it was possible to verify a series of accidents caused by the use of low-quality and non-approved telecommunications products.

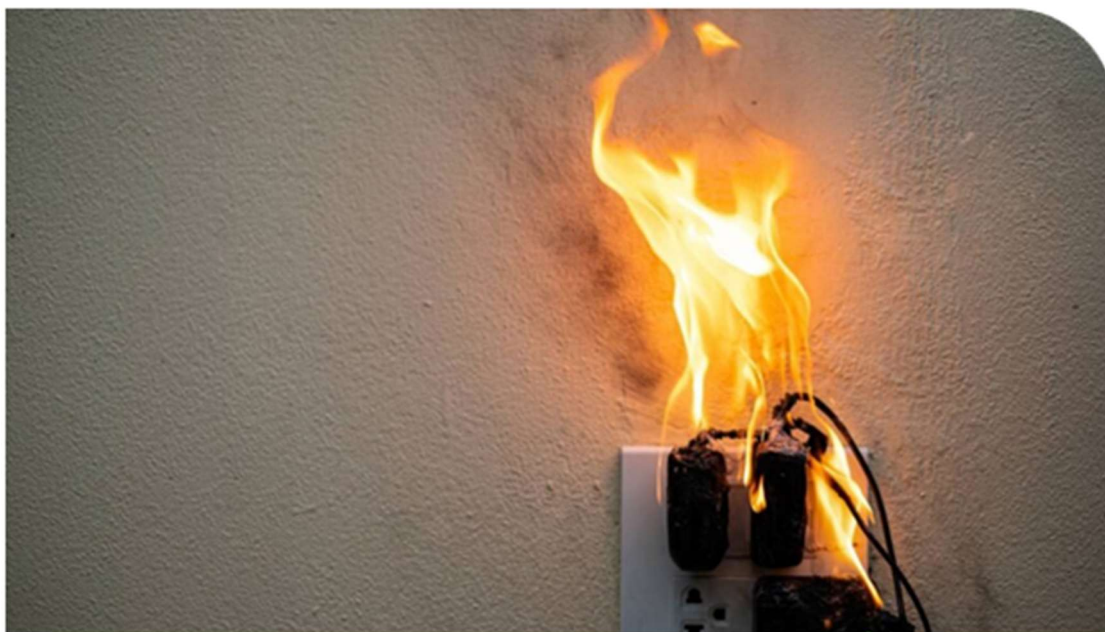


Source: Portal GOV.br

Currently, battery chargers for mobile phone devices are products that, at large, are imported and not certified. These products have been linked to several cases of accidents, such as electric shocks or fires. Electric shocks cause injury and burns. In more serious cases, there are records of deaths. In the case of fires, there are records of relevant financial losses related to the owners of the devices.

The use of battery chargers for non-approved mobile phones deserves special attention, as they are used and handled by the entire population and the dangers associated with their use are closer to the users. In the case of children, the danger is greater, as these products can leave exposed energized metal parts due to their low quality⁷

⁶ AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL. **Anatel apresenta esclarecimentos sobre o Flipper Zero**. Brasília, Mar 29, 2023. Updated on May 31, 2023. Available at: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-apresenta-esclarecimentos-sobre-o-flipper-zero>. Accessed on: Jul 7, 2025.



Source: depositphotos.com/Chonthicha

Another type of product commonly used by the population are mobile phone batteries. It can cause explosions or leakage of chemical elements that pose risks to the consumer's health. There are reports of battery explosions in various conditions⁷, whether when they are in the process of charging, being used along with the mobile phone, or when undergoing maintenance. Resulting in burns and other ailments⁸.

In an article published by the Correio Braziliense newspaper, the Brazilian Association for Awareness of the Dangers of Electricity (Abracopel) found that about 23 (twenty-three) people died in the country, and a total of 41 (forty-one) accidents involved mobile phone

⁷ CINTRA, Caroline. "Perdi meu coração", diz mãe de garoto que morreu após choque em carregador. **Correio Braziliense**, Brasília, Aug 12, 2020. Updated on Aug 12, 2020. Available at: <https://www.correiobraziliense.com.br/cidades-df/2020/08/4868126--perdi-meu-coracao---diz-mae-de-garoto-que-morreu-apos-choque-em-carregador.html>. Accessed on: Jul 7, 2025.

⁸ VÍDEO: incêndio em auditório pode ter sido provocado por carregador de celular, dizem bombeiros. **G1 Tocantins**, Jan 8, 2024 (Updated on Jul 2024). Available at: <https://g1.globo.com/to/tocantins/noticia/2024/01/08/video-incendio-em-auditorio-pode-ter-sido-provocado-por-carregador-de-celular-dizem-bombeiros.ghtml>. Accessed on: Jul 7, 2025.

battery chargers⁹.

The text points out that accidents are related to a set of factors, the main one being the use of non-original chargers, that is, non-approved chargers¹⁰.

In addition to the cases presented of serious risks to consumer health that non-approved telecommunications products can cause, the harm that such products can cause to people's privacy and property is also serious.

The attractiveness of pirated content is directly connected to the ample demand by users, who seek free or easy access to movies, series, sports, and paid channels without bearing legal costs.

This appeal creates an environment conducive to the spread of tampered devices, such as TV boxes and other uncertified equipment, which frequently come preloaded with illegal apps.

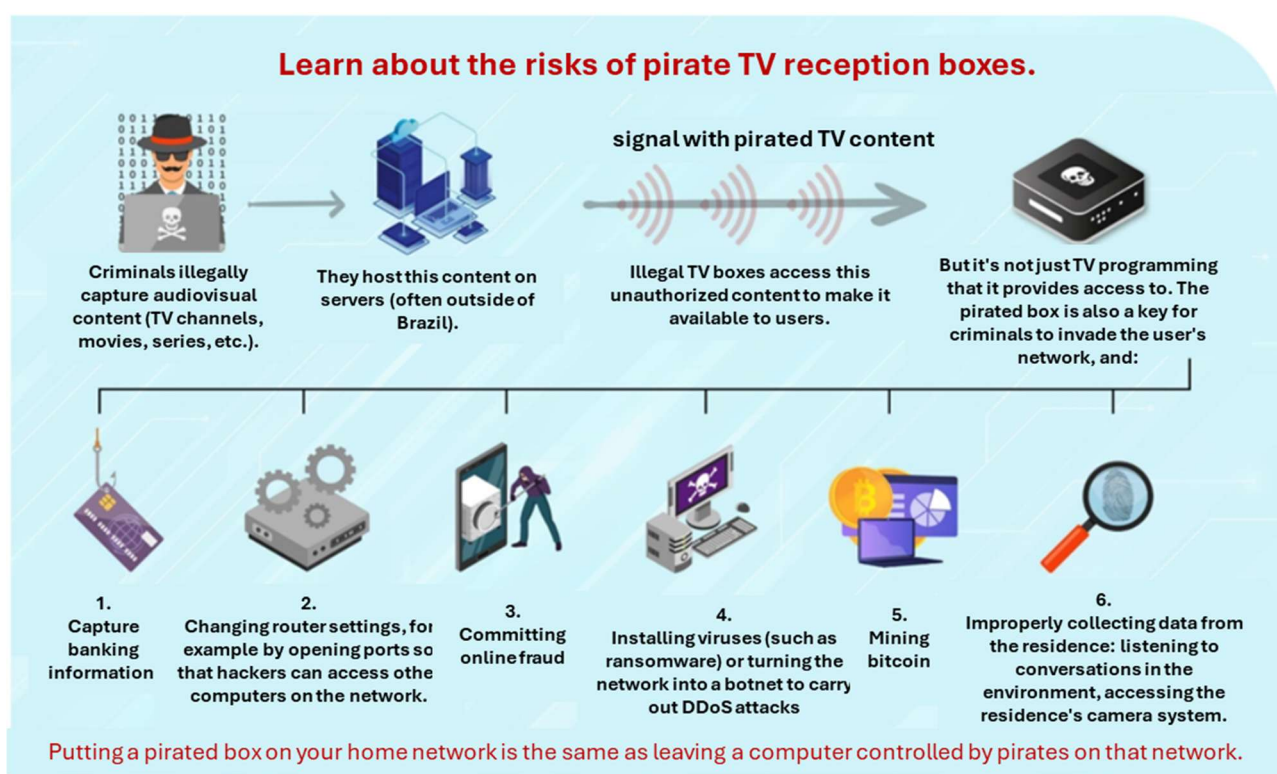
In this context, products intended for the reception of non-approved cable TV or video-on-demand signals can cause copyright infringement, hide malicious code, and have security flaws, allowing hackers to access users' personal data on devices that share the same private network.

Studies by Anatel, with the support of the National Film Agency (Ancine) and the Paid

⁹ DIOGO, Darcianne. Jovem sofre queimadura de 1º grau após celular explodir na tomada no DF. **Correio Braziliense**, Brasília, May 14, 2023. Available at: <https://www.correiobraziliense.com.br/cidades-df/2023/05/5094486-jovem-sofre-queimadura-de-1-grau-apos-celular-explodir-na-tomada-no-df.html>. Accessed on: Jul 7, 2025.

¹⁰ SILVA, Cristiane. Celulares já mataram 23 no Brasil: especialistas apontam principais vilões. **Correio Braziliense**, Brasília, Oct 1, 2019. Available at: https://www.correiobraziliense.com.br/app/noticia/tecnologia/2019/10/01/interna_tecnologia,793061/celulares-ja-mataram-23-no-brasil-especialistas-apontam-principais-vi.shtml. Accessed on: Jul 7, 2025.

Television Association (ABTA), identified a direct link between a certain family of devices and botnets (a network of computers or devices connected to the internet, infected with malware – malicious software – remotely controlled by an attacker for malicious purposes) and capable of taking control of set top boxes (a device that allows access to video applications, games or other online content, through conventional televisions) and execute DDoS attacks (malicious attempt to make an online service inaccessible, flooding it with excessive traffic from multiple sources).¹¹



Source: <https://soulegal.tv.br/2021/05/11/tv-pela-internet/>

Security flaws were also detected in the application update process through their own virtual stores, allowing all the information exchanged to be captured and modified by a malicious

¹¹ Cf. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendência de Fiscalização. **Informe nº 4/2021/FIGF4/FIGF/SFI.** Brasília, 2021. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5PKr37An4NSs6sd1c9IPofluH3e-yRwywlgZfVUh-qW-f-MR8ln0HwABi8MWbOkspZajukWXFCisvs8oBuJmvd. Accessed on: Jul 23, 2025.

attacker, enabling the installation of malicious applications on the device. This vulnerability, associated with another in which the operating system of the devices allows third parties to have unrestricted access to the device with administrator privileges (known as root), enables full control of the TV Box, allowing access to other devices that share the same network, such as computers, televisions, routers, mobile phones, webcams, among others, capturing data and information from users, such as financial records, passwords, files, photos, etc.¹²

In the world of piracy sites and streaming applications (continuous transmission of data, allowing content to be played in real-time without the need for downloading), consumers are unwittingly vulnerable to a range of cyber threats.



PIRACY IN NUMBERS

"Gatonet" generates billions in losses for the Brazilian economy.

15.5 billion reais

This is the annual financial impact of TV piracy. The government fails to collect revenue from taxes alone.

2 billion reais per year



33 million

Brazilians consume pay-TV content through one or more illegal means.



4.2 million

subscription TV accounts **have been cancelled**, either by customer choice or due to non-payment, in the last five years.



150,000

Jobs **could be eliminated** within ten years if the problem is not effectively combated.



10,000 reais

Fines and up to four years in prison can be the penalty for those who **buy or sell** pirated products.

Sources: Ancine, ABTA and Anatel

¹² Cf. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendência de Fiscalização. **Informe nº 8/2022/FIGF4/FIGF/SFI**. Brasília. 2022. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqbGHzc2pUgPteuRLZ6SDuwZoTzuakE9xm340u-SmUAwHzdKU2tlv4WgKQmypi8cvl3ntyOGfLQji7o_Cb0uH4U-. Accessed on: Jul 23, 2025.

- **Malware** – Once installed on the consumer's device, the malware can become the target vector for identity theft and consumer fraud, ransomware attacks, advertising retargeting, and so on¹³. This means that consumers can be attacked directly, with their bank accounts at risk and the possibility of their devices and personal data being held for ransom¹⁴. This means that consumers may see ads that have been hijacked, depriving legitimate companies of the advertising space they paid for.
- **Cryptocurrency mining** – The CPU capacity of consumer devices is used to mine cryptocurrency, significantly increasing CPU load and power consumption¹⁵. Consumers are not the beneficiaries of this cryptocurrency mining – the profits are retained by the website's owners.
- **Social harms** – The promotion of gambling and adult sex sites to consumers, especially children, poses significant risks to society at large, especially gambling addiction¹⁶.

Additionally, in relation to cyber vulnerabilities, the Satori Threat Intelligence Disruption:

¹³ KUMAR, Sachin; MADHAVAN, L.; NAGAPPAN, Meiyappan; SIKDAR, Biplab. Malware in Pirated Software: Case Study of Malware Encounters in Personal Computers. In: **INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY (ARES)**, 11, 2016, Salzburg, Austria, Anais [...] [s.l.], 2016, p. 423-427. Available at: <https://ieeexplore.ieee.org/document/7784601>. Accessed on: Jul 25, 2025.

¹⁴ BAŞESKIOĞLU, Mehmet Özer; TEPECİK, Abdülkadir. Cybersecurity, Computer Networks Phishing, Malware, Ransomware, and Social Engineering Anti-Piracy Reviews. In: **INTERNATIONAL CONGRESS ON HUMAN-COMPUTER INTERACTION, OPTIMIZATION AND ROBOTIC APPLICATIONS (HORA)**, 03, 2021, Ankara, Anais [...]. [s.l.]: IEEE, 2021, p. 1-5. Available at: <https://ieeexplore.ieee.org/document/9461272>. Accessed on: Aug 31, 2025.

¹⁵ VAN DER SAR, Ernesto. **The Pirate Bay Website Runs a Cryptocurrency Miner**. 2017. Available at: <https://torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/>. Accessed on: Jun 14, 2025.

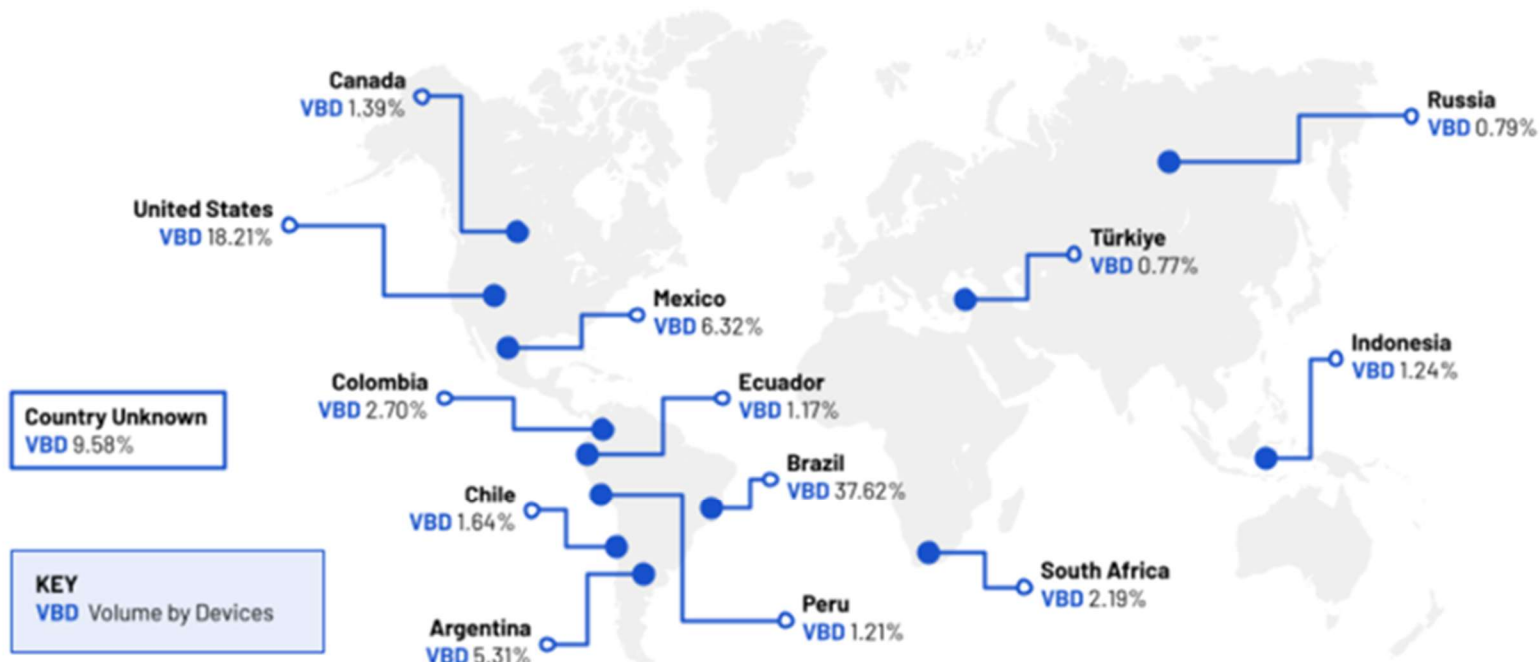
¹⁶ SURIADI, Suriadi; SUSNJAK, Teo; PONDER-SUTTON, Agate; WATTERS, Paul; SCHUMACHER, Christoph. Using data-driven and process mining techniques for identifying and characterizing problem gamblers in New Zealand. **Complex Systems Informatics and Modeling Quarterly**, Riga, Latvia, n. 9, p. 44-66, 2016. DOI: 10.7250/csimq.2016-9.03. Available at: <https://csimq-journals.rtu.lv/csimq/article/view/csimq.2016-9.03..> Accessed on: Aug 31, 2025.

BADBOX 2.0 Targets Consumer Devices with Multiple Fraud Schemes¹⁷ report, published by Human Security (a North American company that develops solutions to protect organizations from sophisticated bots, fraud, and digital abuse) in March 2025, stands out.

According to the report, BADBOX 2.0 is a large-scale cybercriminal network, which stands out for infiltrating malware directly into the firmware (type of software that controls the hardware of an electronic device) of Android devices during their manufacture or distribution — a supply chain attack with global impacts.

It is estimated that more than 200 device models were compromised, including set top boxes, tablets, smartphones and streaming devices, with Brazil concentrating approximately 37% of the estimated 1 million affected devices at the time of the study's development.

¹⁷ SATORI THREAT INTELLIGENCE AND RESEARCH TEAM. **Satori Threat Intelligence Disruption: BADBOX 2.0 Targets Consumer Devices with Multiple Fraud Schemes**. 2025. Available at: <https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/>. Accessed on: May 19, 2025.

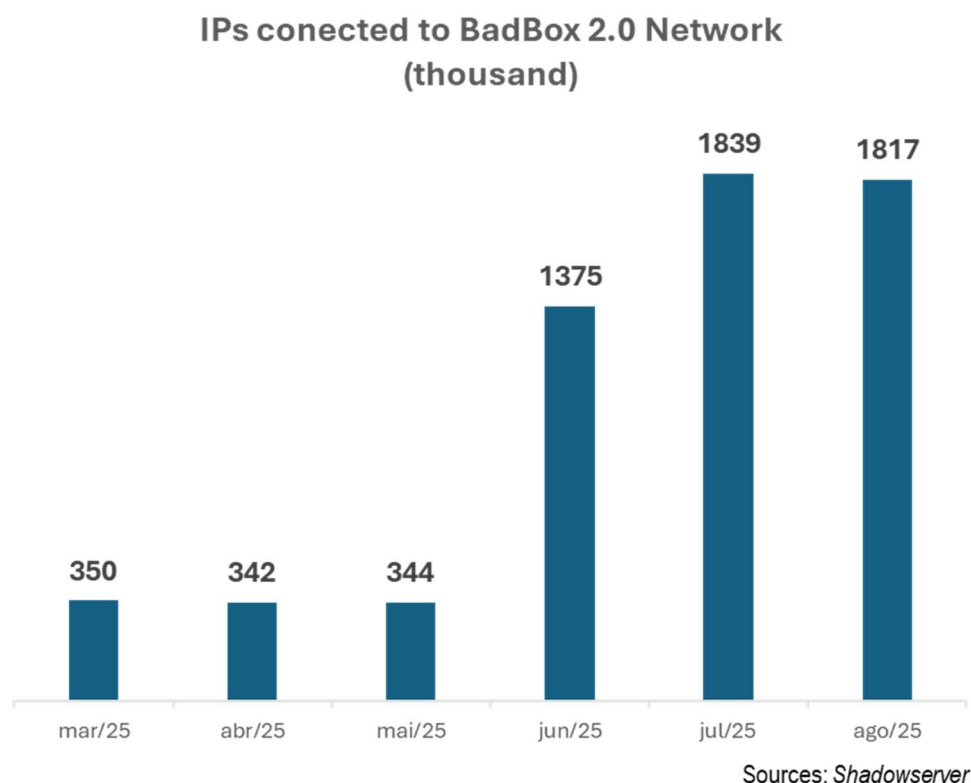


Source: Human Security

Anatel has issued an urgent alert regarding the BadBox 2.0 malware, identified in non-approved TV Boxes, which can act as vectors for cybercrime, compromising both user data and the security of telecommunications networks.

The Agency's study, conducted in a specialized laboratory, revealed that these devices contain persistent malware. Even after multiple reboots and, in standby mode, maintain connections to malicious external servers. The unauthorized use of these devices as a residential proxy was detected, enabling advertising fraud, credential theft, DDoS attacks and access to sensitive websites, such as banks and courts. In updated data from August 2025, Brazil alone already concentrates nearly 2 million infected devices connected to the BadBox 2.0 network.¹⁸

¹⁸ AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL. **Anatel emite alerta sobre malware BadBox 2.0 em TV Boxes piratas.** Brasília, DF: Anatel, Jul 25, 2025. Available at: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-emite-alerta-sobre-malware-bad-box-2-0-em-tv-boxes-piratas>. Accessed on: Aug 14, 2025.



These data demonstrate that the fight against piracy goes beyond the protection of the regulated sector: it is a public policy focused at preserving the economic order, health and safety of users, and the integrity of telecommunications networks. Anatel's work has sought not only the repression of illicit practices, but also prevention, through educational actions, updating regulations and expanding cooperation with national and international entities.

Thus, the Agency's active presence in this scenario is justified not only by its institutional role, but by the urgency of protecting Brazilian society in the face of a problem that affects, directly or indirectly, millions of citizens and compromises the future of communications in the country.

2. ACTIONS TO COMBAT PIRACY AND THEIR REACTIONS

2.1. PACP – Action Plan to Combat Piracy

Since the creation of the National Telecommunications Agency in 1997, the inspection actions of approved products were initially focused on verifying complaints and, indirectly, performing routine technical inspections at broadcasting or telecommunications stations. When inspecting the technical characteristics, the inspectors eventually found equipment without the required certifications.

To investigate the complaints presented to the Agency, the inspection actions took place in stores and shopping centers, that is, in the retail market.

In its organizational structure, Anatel has institutional representation in all 27 federative units. For each decentralized unit of Anatel, there were inspection teams that worked individually to meet the demands received. Between 2012 and 2017, 492 complaints were answered, an average of 82 demands per year, distributed to all federative units.

The number of inspections demands to verify the certification of telecommunications products was much lower when compared to complaints of clandestine use of broadcasting or telecommunications services, radio interference or demands on other topics such as inspection of network or station infrastructure.

In 2017, P&D Brasil - Association of National Technological Development and Innovation Companies, an entity of representatives of manufacturers of equipment with national technology, presented a dossier to the Agency, with a study in which it concluded that, in the Internet Service Providers (ISPs) market, approximately 70% of the equipment used did

not have Anatel approval.

In the same year, ABTA presented to the Agency information on losses to the electronics industry and taxes collection reaching billions of Reais, related to the misappropriation of telecommunications products or even the legal importation of non-approved products. In the Subscription TV market alone, ABTA's estimate was for annual revenue losses of R\$ 6 billion.

Considering this scenario, the increase in volume of complaints, including from companies that sold non-approved equipment in various regions of the country, and the growth of non-approved products in the domestic market, such as set top boxes, chargers and mobile phones, Anatel's Superintendence of Inspection (SFI) concluded that there was a need for a change in the planning of inspection actions and the procedures applicable to combating the sale of irregular products.

The SFI then developed an action plan in which a new approach to inspection actions on the certification of telecommunications products was considered. Instead of acting only as a reaction to complaints presented in a timely manner, the Agency began to act in accordance with an annual plan, which would seek to prioritize the inspection of the central and most important elements of the chain of commercialization of telecommunications products, such as manufacturers, distributors and importers. The objective was to increase the efficiency of inspection actions in preventing and combating the commercialization of non-approved telecommunications products, seeking as a result the reduction of the use of these products in telecommunications networks.

It should be noted that, according to this strategy, the response to specific complaints would continue, however, the planning and analysis of the resulting inspection actions would be done in a centralized manner for the entire national territory. In addition to providing greater standardization in the treatment of complaints, the resulting inspection actions could be

planned in a coordinated manner.

On February 9, 2018, the SFI approved the Action Plan to Combat Piracy (PACP) and designated Anatel's Regional Management in the States of Goiás, Mato Grosso, Mato Grosso do Sul and Tocantins (GR07) as responsible for coordinating the implementation of the plan at the national level.

Among the first actions of the new action plan, face-to-face inspections were planned in a few dozen distributors of telecommunications products. This was a great innovation in the procedure adopted by the Agency, which historically acted directly on the market, inspecting hundreds of stores.

At first, six axes or groups were defined, which would encompass the inspection actions to compose the PACP:



In the first year of PACP, in 2018, about 164 thousand irregular products were withdrawn

from the market, including restricted radiation equipment used in networks of internet service providers, metallic cables, optical cables and data network equipment. Inspection actions were done only by Anatel. This number represented a big jump in the volume of apprehensions, which were limited to a few hundred units in previous years.

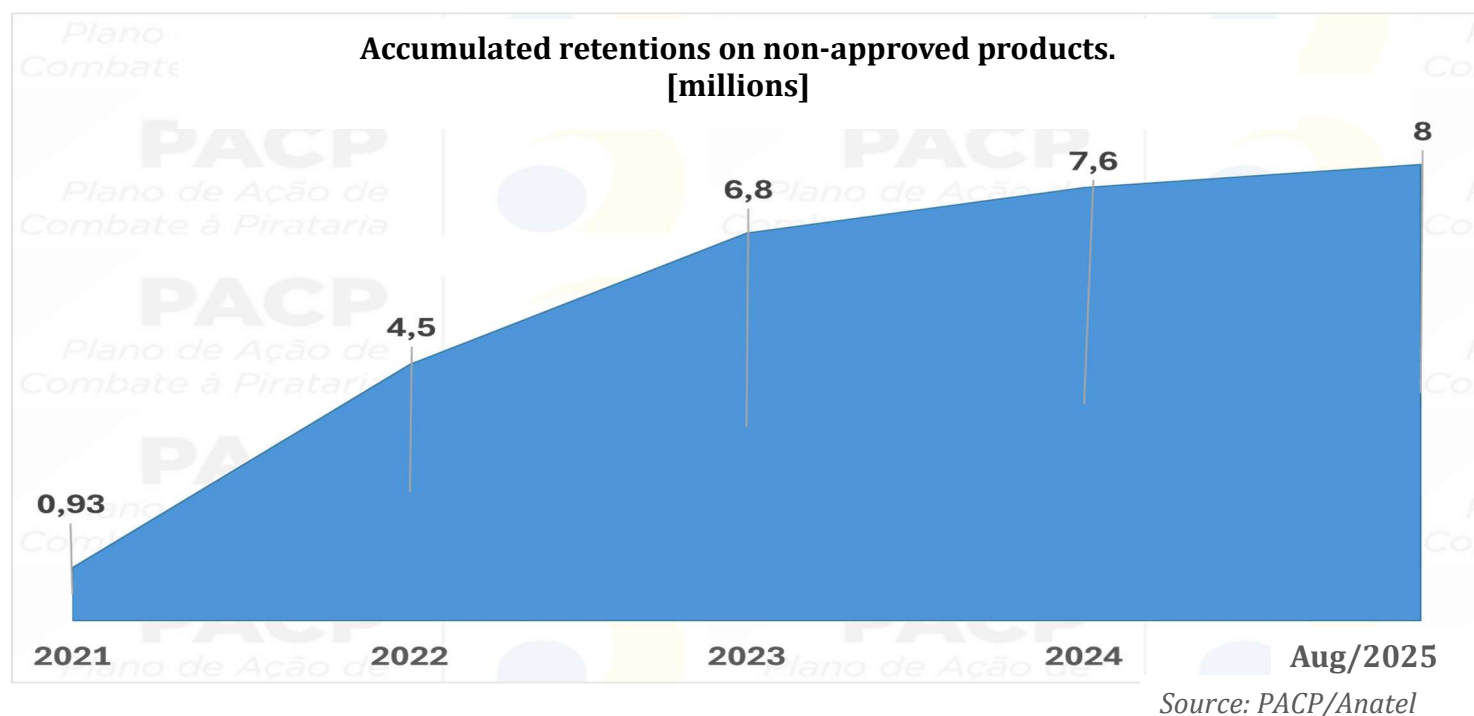
In the following year, in 2019, the result was approximately 165 thousand irregular telecommunications products withdrawn from the market, including battery chargers, TV Boxes, restricted radiation equipment, and metallic and optical cables. That year, there was a rapprochement with the Internal Revenue Service of Brazil, at the International Postal Remittance Treatment Centers (CEINT), in Pinhais/PR, and at the Galeão International Airport, in Rio de Janeiro/RJ. It is worth mentioning that, since 2012, before PACP, there was already work done by Correios, in São Paulo/SP, which was incorporated into PACP.

It should be noted that the CEINT are facilities of the Post Office, but controlled by the Brazilian Internal Revenue Service, as it is a customs location for receiving goods purchased abroad and imported into the national territory. In this environment, Anatel inspects products such as drones, TV Boxes, transceivers and radio frequency emitting products.

Relevant information from the CEINT is that hundreds of jammers have already been retained in it, which have restrictive use in the country, being prohibited for use both by individuals and private companies, as provided for in the Regulation on Radiocommunication Signal Blockers, approved by Anatel Resolution No. 760, of February 6, 2023 as this equipment causes extreme harmful interference in mobile networks and, in some cases, is used by criminal entities, its use is very limited, under certain conditions, to police forces, armed forces, and correctional establishments.

At some airports, Anatel inspects goods imported by private companies, known as couriers, in customs areas controlled by the Brazilian Internal Revenue Service.

By the end of 2020, more than 930 thousand irregular telecommunications products were withdrawn from the market. By the end of 2021, this total had risen to 4.5 million, a record. This number reflected Anatel's approach to the Brazilian Internal Revenue Service in some national ports.



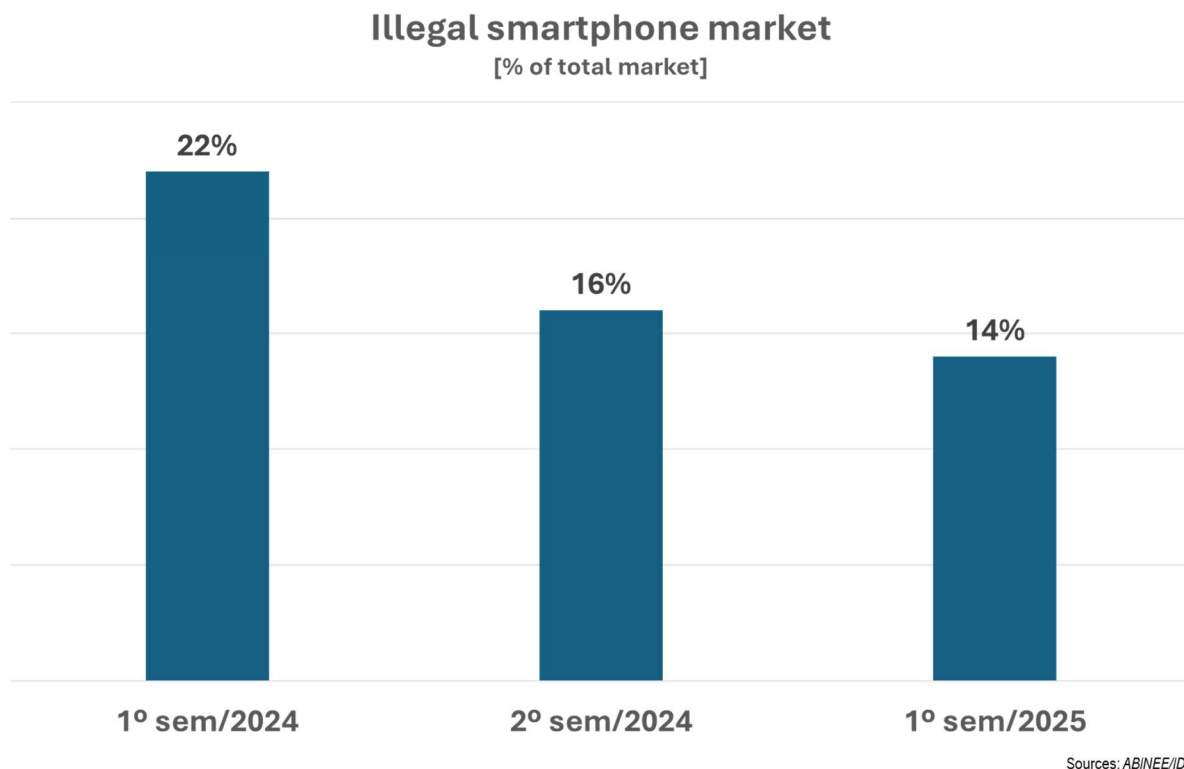
Considering the need for better monitoring of the results of the activities and greater transparency in the information related to PACP's inspection actions, a public dashboard was created at the following address: <https://informacoes.anatel.gov.br/paineis/fiscalizacao>. Information related to inspection actions, such as the federation unit, the month and year in which it occurred, as well as the type of equipment inspected and the geographic region, are presented on the dashboard and can be consulted freely, as they are of public domain.

In a consultation to the public panel at the end of July 2025, it was found that, through inspection actions, a total of 3,779,825 products were inspected and considered regular, and another 8,053,098 non-approved products were withdrawn from the market, with an estimated value of R\$ 833,617,356.00 (eight hundred and thirty-three million, six hundred

and seventeen thousand, three hundred and fifty-six reais). The analysis of these results is presented below:

- Around 71% of the products withdrawn from the market resulted from actions by the Brazilian Internal Revenue Service in ports, with the support of Anatel. These retained products had not been approved.
- The products retained by the BIRS are in custody of the customs agency. If the importer does not regularize the products, the Brazilian Internal Revenue Service gives a specific legal destination, which can be destruction, return to origin or even donation to educational programs that transform these products into others with different purposes. The set top box is an example of a product that can be transformed into minicomputers or sensors for industrial equipment.
- The vast majority of non-approved products retained by the Brazilian Internal Revenue Service with the support of Anatel originate from China.
- Some techniques used by importers to evade customs inspection were the falsification of seals, the use of real seals on non-approved products, disassembly of products into smaller pieces and even the alteration of the description of the products.

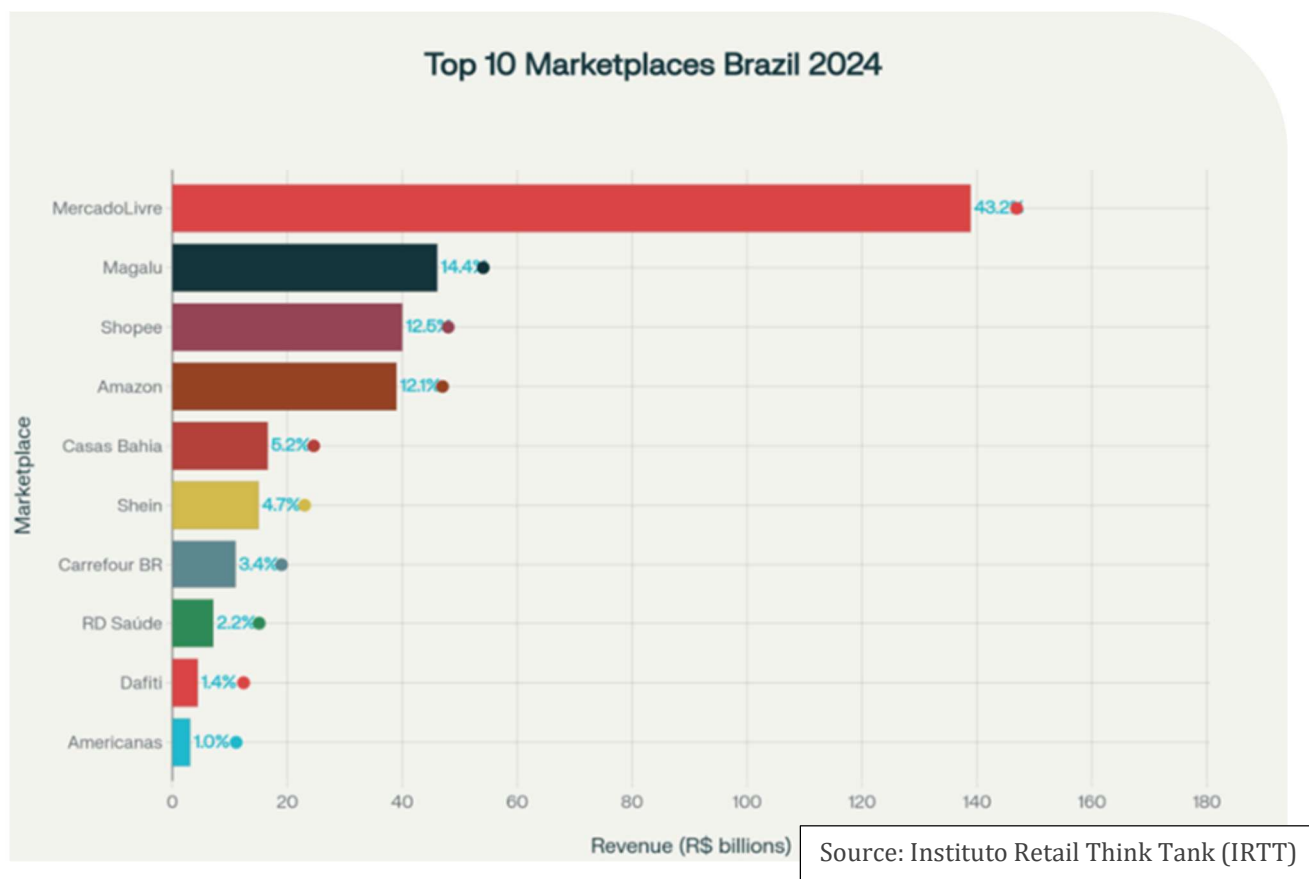
The fight against piracy by Anatel has intensified especially in relation to the so-called "gray market" of mobile phones in Brazil, which involves the sale of imported devices without approval or guarantees of compliance with the required technical and security standards.



2.2. Combating Piracy in Marketplaces

In addition to inspection actions involving the partnership with the Brazilian Internal Revenue Service, there is another axis of action that has had an important highlight in PACP: e-commerce, especially companies that operate as marketplaces.

During the Covid-19 pandemic, the sale of goods by electronic means increased exponentially, with large marketplace platforms present in the country such as Mercado Livre, Amazon, Shopee, Casas Bahia, Carrefour, Americanas and Magalu gaining prominence.



In this scenario, Anatel has instituted regulatory inspection procedures against the aforementioned marketplaces, in an attempt to reach an amicable settlement for the regularization of the electronic commerce of telecommunications products. However, Anatel always ran into the unwillingness of the monitored economic agents to apply their technological knowledge (despite all the efforts of the regulatory agency to provide the necessary subsidies) to prevent the sale of non-approved products on its websites.

Considering the universe of tens or hundreds of thousands of ads on marketplace platforms, the work of manual inspection proved to be unfeasible or impossible. To develop solutions to problems like this, the Superintendence of Inspection created an Innovation Laboratory, composed of servers dedicated to the production of advanced tools to support inspection actions. One of the first products developed by the Innovation Laboratory was the creation of a bot, using Artificial Intelligence, called "Regulatron", to monitor platform ads and

identify non-approved telecommunications products.

The analysis of the data provided by "Regulatron" in June 2024, consisting of the electronic verification of ads published on e-commerce platforms compared to technical information of approved products in the Agency's database, demonstrated an evolution in the inclusion of approval codes in product ads on the platforms of Mercado Livre, Amazon, Shopee, Carrefour, Magalu, Americanas and Casas Bahia. However, it was evident that, despite all the efforts by Anatel since 2018, the percentage of products whose approval codes are not validated within Anatel's database, including non-existent codes or of different products, remained high.



Source: <https://br.freepik.com/>

The dangers of this large commercialization of non-approved products to consumer motivated the issuance of a precautionary measure materialized by Decision Orders No.

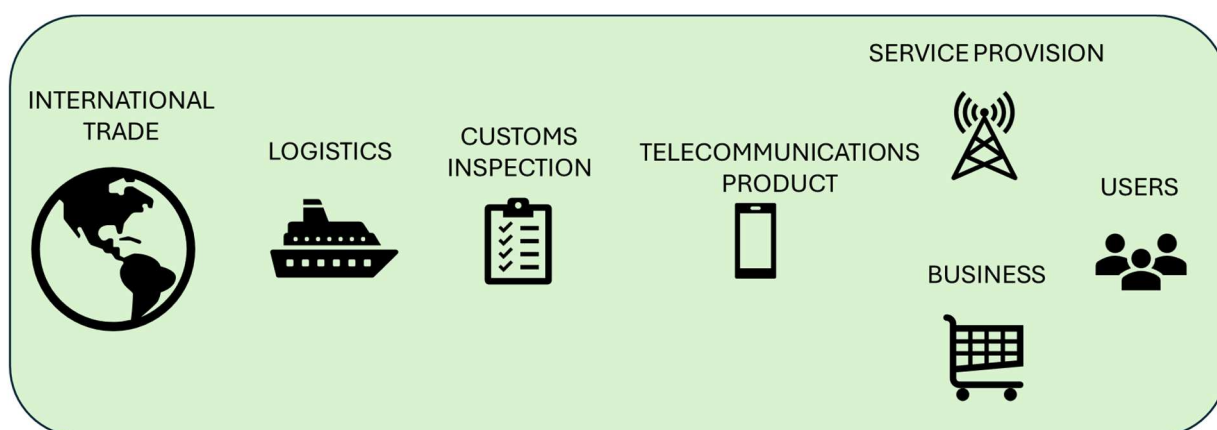
5657/2024/ORCN/SOR¹⁹ (SEI nº 12160352) e 5686/2024/ORCN/SOR²⁰ (SEI nº 12163126), 12163126), still in force, an important signal to the online market that the inspection agency monitors its activities in order to prevent the sale of irregular products.

In addition to the validation of approval codes, it is important that marketplaces or anyone involved in the marketing process verify its origin when purchasing or making available a telecommunications product. This is because only the holder of the Homologation Certificate can sell or authorize others to sell the telecommunication product, since the holder is responsible for the product in the Brazilian consumer market.

Since the beginning of PACP, the Agency made efforts to partner with other agencies in inspection activities, whether in border areas or in the national internal market. The numbers presented prove that, when there are partnerships between the agencies, the results improve. However, there are barriers to be overcome so that the agencies can effectively work synergistically, as will be shown next.

¹⁹ AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendência de Outorga e Recursos à Prestação, Superintendência de Fiscalização. [NATIONAL TELECOMMUNICATIONS AGENCY – ANATEL (Brazil). **Despacho Decisório nº 5657/2024/ORCN/SOR**. Brasília, 2024. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYMk7UOAww8fj5jIUHIDwe0NhuPf9JzG-Uyip5lqqRmZXWq3_FHP60CDJBwjfirYwgLZsBySFp8Kq5_qlyt8sBgO. Accessed on: Jul 23, 2025.

²⁰ AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendência de Outorga e Recursos à Prestação, Superintendência de Fiscalização, Superintendência de Controle de Obrigações. **Despacho Decisório nº 5686/2024/ORCN/SOR**. Brasília, 2024a. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqZApP7PurlyWa1s0oaWqCwkV7A2ZHNvzf5QswTfpGIhwO97BwkTz78Z4IVzklfCymKa1dhf6kvAa4Vna4sXaT3. Accessed on: Jul 23, 2025.



2.3. Partnerships with public administration entities

Brazilian Internal Revenue Services

Brazil has an immense land border close to 16.9 thousand kilometers long and with 10 neighboring countries. The longest border is with Bolivia, with around 3,400 kilometers. In the immensity of the border, a large number of pirated products from various segments, including telecommunications, such as mobile phones, battery chargers, TV Boxes, batteries, drones, products with wi-fi and Bluetooth technologies, transceivers, as well as equipment for restricted use such as signal jammers, enters the country.

The Special Secretariat of the Brazilian Internal Revenue Services (RFB) is a federal public administration entity responsible for administering federal taxes and customs control. In addition, the RFB acts to combat tax evasion, embezzlement and smuggling of goods that enter the national territory.

In the organizational structure of the Brazilian Internal Revenue Service, the Undersecretariat of Customs Administration (SUANA) is divided into the General Coordination of Customs Administration (COANA), the General Coordination for Combating Smuggling and Embezzlement (COREP) and the General Coordination of Customs Risks (CORAD). For greater control and inspection, the RFB defined two major areas of action: the primary zone,

under the responsibility of COANA, and the secondary zone, under the responsibility of COREP.

The primary zone, in the context of foreign trade, refers to locations where the entry and exit of goods from the national territory take place, such as ports, airports and border regions with customs, where customs inspection actions take place in import and export activities. The secondary zone, in turn, refers to the part of the customs territory that is not considered a primary zone. Basically, everything that is not included in the primary zone, including territorial waters and airspace.

Anatel's partnership with the RFB takes place in some primary zones located in ports and airports, in the international postal shipment processing centers, which are areas of the Post Office, but under the supervision of the RFB, and in the secondary zone, in some states.



Source: Portal GOV.br

The Agency's efforts to expand the partnership with the RFB throughout the national territory continue. More recently, the Agency was admitted as an intervening party in the Foreign Trade System (Siscomex). This integration will allow Anatel to access Siscomex data and, thus, conduct a prior analysis of import records, ensuring the identification of

equipment in accordance with the rules established by the Agency.

The draft of the Operational Procedure for Administrative Treatment in the Foreign Trade System of Import Operations of Goods Subject to Approval by Anatel was placed for public consultation, under number 17/2025 in the period from June 17 to August 26, 2025.

The proposal intends to replace the current Operational Procedure for Importing Telecommunications Products, approved by Act No. 4521, of July 21, 2021. This operational procedure defines the conditions for administrative treatment of import actions of products and equipment subject to Anatel's approval in the Integrated Foreign Trade System (SISCOMEX).

Anatel, as an intervening entity of Siscomex, presents great technical expertise in the assessment of the conformity of telecommunications products into the customs clearance process, allowing the identification and restriction of irregular products, that is, non-approved, from entering the national market. This process strengthens the integration between the two agencies, with complementary tasks that add up to the fight against the entry of non-approved products into the country.

Federal Highway Police

The Agency has been invited to participate in inspection actions in conjunction with other agencies in an action coordinated by the Federal Highway Police (PRF). The main objective of these actions is to train federal highway police officers for routine actions that may occur on federal highway roads.

The actions are structured in thematic operations with the objective of aligning and updating multidisciplinary knowledge and skills of local personnel; strengthen the integration between public agencies and private institutions of public interest, especially with the Ministry of Agriculture and Livestock, other Agencies, the Brazilian Internal Revenue Services,

the State Treasury Secretariat and other Secretariats involved; promote the improvement and exchange of information between the PRFs and the employees of partner institutions and intensify the fight against crime, promoting the preservation of public order and the safety of people and property on federal highways.



Source: Portal GOV.br

Federal Police

Inspection actions under the Action Plan to Combat Piracy (PACP) have frequently found highly restricted, non-approved equipment, in the country. As the cases of signal jammers, known as jammers and recently anti-drone jammers. The jammers are nearly always used by criminal organizations to steal goods on highways. Anti-drone jammers, on the other hand, were found in actions in partnership with the Internal Revenue Service and police agencies. In this case, the equipment was intended for use by criminal organizations to obstruct police actions. These products are commonly imported, entering the country clandestinely and usually using gangs specialized in product smuggling.

Considering this scenario and the need to deepen investigations to identify the recipients of this equipment, the purpose and commercialization, Anatel seeks to share intelligence

information with the Federal Police as it understands that it involves risks to national security, notably the occurrence of various crimes by criminal organizations.

In July 2025, the Federal Police led an operation supported by Anatel inspection agents to dismantle a sophisticated criminal organization specializing in importing and selling illegal IPTV devices, commonly known as TV BOX and Gatonet.

The Federal Police identified that the organization moved a large amount of money, operated with a sophisticated structure of front companies and transnational logistics, with devices coming from the border with Paraguay, through the city of Foz do Iguaçu/PR.

Inspection agents identified about 140 non-approved TV BOX sets in the possession of the gang, with an estimated value of R\$ 125,860.00. In addition to the exchange of information



Source: Portal GOV.br

between agencies and cooperation in joint actions focused on non-approved products, the Federal Police investigate crimes such as tax evasion, fraudulent loans and money

laundering, with the support of Anatel's inspection teams^{21,22}

CNCP

The National Council to Combat Piracy and Crimes Against Intellectual Property (CNCP) is a government entity part of the Ministry of Justice and Public Safety (MJSP), composed of twenty representatives of public authorities and Organized Civil Society, in addition to dozens of collaborators.

The CNCP aims to articulate and execute public policies to combat piracy, smuggling and other crimes against intellectual property. The union between public and private sectors in the fight against piracy and smuggling is of fundamental importance to combat criminal organizations that introduce irregular products into the economy and bring losses to the entire society.

Anatel is represented on the board by the Superintendent of Inspection, as a full member, and by the Superintendent of Granting and Provision of Resources, as an alternate member.

2.4. Evolution of legal understanding (marketplace, social media and distribution chain)

As previously mentioned, Anatel has acted to combat piracy of telecommunications products through a set of legal and regulatory actions, including inspecting actions, entering into cooperation agreements and launching educational campaigns. The objective is to

²¹AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brazil). Anatel, **Polícia Federal e Receita Federal realizam ação conjunta em Pelotas (RS)**. Brasília, DF: Anatel, Jul 9, 2025. Available at: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-policia-federal-e-receita-federal-realizam-acao-conjunta-em-pelotas-rs>. Accessed on: Jul 27, 2025.

²²AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brazil). **Anatel e PF desarticulam esquema milionário de "TV Box" e "Gatonet" em Operação PRAEDO**. Brasília, DF: Anatel, Jul 29, 2025. Available at: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-e-pf-desarticulam-esquema-milionario-de-tv-box-e-gatonet-em-operacao-praedo>. Accessed on: Jul 29, 2025.

ensure the safety of consumers, the reliability of networks, the quality of telecommunications services and fair competition in the market.

2.4.1. *Marketplace liability*

As previously mentioned, the telecommunications product certification model currently in force, implemented by the Regulation approved by Resolution No. 715/2019, regulates the entire certification process within Anatel and, along with operational procedures and technical requirements, details the form and technical parameters necessary for the approval of a product.

Despite the existence of the aforementioned regulation, at the beginning of inspection activities on e-commerce platforms, marketplaces claimed neutrality (inspired by Article 19 of Law No.12,965, of April 23, 2014 - Civil Rights Framework for the Internet), arguing that they could not be held responsible for third-party content.

In view of this, Anatel requested the support of the Specialized Federal Prosecutor's Office (PFE-Anatel) in order to present a teleological interpretation of these rules, in order to improve Anatel's performance and accountability of various economic agents — especially marketplaces and digital platforms — for the sale of non-approved telecommunications products.

2015

Opinion No. 1,580/2015/PFE ANATEL/PGF/AGU ²³

Consultation:

Administrative responsibility of intermediaries (Marketplace)

Response:

Not subject to fines.

Even though notified, the platforms claimed to act only as intermediaries, not as sellers.

In 2018, a Pado was filed against a company that offered non-approved telecommunications products on the grounds that it was a market test. In view of this, Anatel's technical area consulted PFE-Anatel if the offer of non-approved products, without effective sale, would constitute commercialization.

2018

Opinion No. 524/2018/PFE ANATEL/PGF/AGU ²⁴

Consultation:

Administrative responsibility for offering and promoting (Marketplace)

Response:

This constitutes commercialization and is subject to fines.

Along with such conclusions, the administrative liability of marketplaces in the commercialization of irregular products has always been marked by legal debates about the extent of the liability of online sales intermediaries. The jurisprudence and doctrine oscillated between objective liability, based on the Consumer Protection Code, and the need to delimit the scope of this liability, considering the nature of the marketplace's performance as a mere intermediary.

²³ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **Parecer n.º 01580/2015/PFE ANATEL/PGF/AGU**. Brasília, 2015. Available at https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?Yj72kUioo_z14_E1ere_NErKAAYpCDMsB4uhQFHnURzICcsEezBx7gPUNtxU8bNUcaTcr0nBnveExhjIYaFQPg7w474YcqjoUmoQPS4yTNLNaUCTtkxM0SgmZMjHGDh. Accessed on: Jul 21, 2025.

²⁴ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **PARECER n.º 00524/2018/PFE-ANATEL/PGF/AG**. Brasília, 2018. Available at https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5Aq93gDCiAKZgfvdufplsL2yUPD34g1U-JBQb1D9R_dacgaUTkfl4JNVnd23QsN5FoeTx1MPAZEgSqZRwJaIOS. Accessed on: Jul 21, 2025.

However, the aforementioned digital scenario evidenced the limitation of the traditional duty of state protection — historically conceived as a criterion for control and conformation of legislative activity — in the face of the new challenges imposed by the dynamics of the contemporary informational environment.

As Gilmar Mendes and Victor Oliveira Fernandes point out, such a paradigm proves to be insufficient for the adequate resolution of conflicts between fundamental rights in the digital context²⁵. This is due to the fact that, on digital platforms, the structuring of public informational space has been, to a large extent, defined by private agents, who have a growing capacity to condition the exercise of constitutional freedoms.

In this environment, practices related to algorithmic curation, recommendation systems, and architecture of choice allow these agents to exert relevant influence on information flows, affecting the reach, visibility, and content of communication of users. This reality imposed on the Government the challenge of developing normative and regulatory instruments capable of effectively guaranteeing the protection of fundamental rights in the digital ecosystem.

In this scenario, the state's duty to protect has taken on multiple dimensions, such as the obligation to interpret the rules in accordance with the Constitution, considering the structural vulnerability of the consumer; the duty of administrative action, through effective regulation and inspection; and the responsibility to formulate norms, through the construction of a regulatory architecture that ensures the effectiveness of protection in the face of new market dynamics and technological risks emergent markets²⁶.

²⁵MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. **Revista Brasileira de Direito**, Passo Fundo, RS, Brasil, v. 16, n. 1, p. 1–33, 2020. DOI: 10.18256/2238-0604.2020.v16i1.4103. Available at: <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103>. Accessed on: Aug 10, 2025.

²⁶In this sense, cf. MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, v. 106, jul./ago., p. 37-69, 2018.

In 2020, the National Consumer Secretariat (Senacon) faced the issue of sale of prohibited and pirated products that pose a risk to the life, health and safety of consumers, and issued a Technical Note.

2019

Technical Note No. 610/2019/SENACON/MJ ²⁷

Legal Context

It is based on the Consumer Protection Code (CDC) and the Federal Constitution, which prohibit the sale of illegal and counterfeit products, including on digital platforms.

The consumer's right to life, health, and safety is a priority and inalienable.

Prohibition and Liability:

products **cannot be sold** under any circumstances.

Platforms **can be held liable** :

Due to the **lack of registration or identification** of the sellers;

Due to a **lack of clear information** about the suppliers;

Due to their **failure to acknowledge the limits of their own responsibility** .

Consumer Protection:

The CDC imposes a **duty of prevention and care** on platforms.

There is a possibility of **strict and joint liability** for the damages caused.

Economic Freedom vs. Responsibility:

Freedom **of expression** **This does not apply** as justification for maintaining advertisements for illegal products.

This refers to the **exercise of economic freedom** , **subject to the law and the public interest** .

Platforms **must remove** advertisements for irregular products and **cannot claim neutrality** .

Conclusion

E-commerce platforms **must adopt effective mechanisms for controlling, preventing, and removing advertisements** for illegal or counterfeit products, under penalty of **being held jointly liable** with the sellers, in accordance with the principles of the Consumer Protection Code and the Constitution.

In turn, a new Technical Note to the National Consumer Secretariat stated:

²⁷ MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA SECRETARIA NACIONAL DO CONSUMIDOR COORDENAÇÃO DE CONSUMO SEGURO E SAÚDE **Nota Técnica n.º 610/2019/CCSS/CGCTSA/DPDC/SENACON/MJ**, Available at: <https://www.gov.br/mj/pt-br/assuntos/noticias/senacon-questiona-sites-sobre-politica-para-evitar-anuncio-e-venda-de-produtos-falsificados/NTPirataria.pdf> . Accessed on: Aug 10, 2025.

2019**Technical Note No. 91/2020/SENACON/MJ** ²⁸**Legal Context**

This study analyzes responses from e-commerce platforms regarding measures to combat the sale of counterfeit products, highlighting the need for proactive action in protecting consumers and preventing illegal activities in online transactions.

Platform Stance and Responsibility:

Denying responsibility for **advertising, promoting, or offering counterfeit products** may result in:

Sanctioning procedures ;

Administrative sanctions , based on **article 55 of the Consumer Protection Code (CDC)** .

The **platforms' omission** is seen as **conduct that is potentially harmful** to consumers.

Regulatory Challenges:

Authorities and consumer protection agencies, **both in Brazil and abroad** , face **difficulties in adopting effective measures against pirated or counterfeit products** .

It is essential for platforms to **adopt preventive and collaborative measures** .

Conclusion

Omissions can give rise to civil and consumer liability , in light of:

- From the **Civil Code** , and
- From the **Consumer Protection Code (CDC)** .

Digital platforms **cannot claim a lack of responsibility** for the presence of counterfeit products on their platforms.

They must **act preventively** , ensuring **transparency, traceability, and security** in consumer relations, under penalty of **joint liability** .

In view of this, and considering the evolution of marketplace practices, PFE-Anatel was consulted again in 2021.

2021**Opinion No. 453/2021/PFE ANATEL/PGF/AGU** ²⁹**Consultation:**

evolution of *marketplace practices* — which have started to offer services such as warehousing, packaging and shipping.

Response:

This constitutes commercialization and is subject to fines and precautionary measures such as sealing and seizure.

²⁸ MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA SECRETARIA NACIONAL DO CONSUMIDOR COORDENAÇÃO DE CONSUMO SEGURO E SAÚDE **Nota Técnica n.º 91/2020/CCSS/CGCTSA/DPDC/SENACON/MJ**, Available at: <https://www.gov.br/mj/pt-br/aceso-a-informacao/perguntas-frequentes/consumidor/consumo-seguro-e-saude#:~:text=Nota%20T%C3%A9cnica%20n%C2%BA%2091/2020,Permanentes%20de%20Acidentes%20de%20Consumo> . Accessed on: Aug 10, 2025.

2021**Opinion No. 453/2021/PFE ANATEL/PGF/AGU** ²⁹**Consultation:**

evolution of *marketplace practices* — which have started to offer services such as warehousing, packaging and shipping.

Response:

This constitutes commercialization and is subject to fines and precautionary measures such as sealing and seizure.

As a result, face-to-face inspections, seizures of irregular products, and the establishment of Regulatory Inspection Procedures (PFRs) were made possible, based on the Regulatory Inspection Regulation (RFR), approved by Resolution No. 746, of June 22, 2021, and PADOs directly against marketplaces.

After the issuance of Opinion No. 453/2021/PFE-ANATEL/PGF/AGU and the entry into force of the new Regulatory Inspection Regulation (RFR), the current Ordinance No. 2,431/2022 (SEI No. 8941316), approved a new Inspection Instruction on the commercialization of products via e-commerce.

Despite the aforementioned conclusions, the neutralist thesis of marketplaces clashed with PACP and there were some courts that adopted such position. However, the jurisprudence has evolved in the sense of attributing duties of proactive diligence to platforms, which was pacified by a recent decision of the Federal Supreme Court (STF), with general repercussion,

²⁹ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **Parecer n.º 00453/2021/PFE-ANATEL/PGF/AGU**. Brasília, 2021. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO4t0UuV0d7ERjywGrRjzWiwaEv5qDiucqzOSkmGuYZGIA6a-B118QiuybPF9Bdki34wmGMyB6GhHGdoEUeFV5_. Accessed on: Jul 21, 2025.

on June 2025³⁰. The Supreme Court decided that content platforms must create self-regulation and that marketplaces are civilly liable in accordance with the Consumer Protection Code (Law No. 8,078/1990). The judgment on Article 19 of the Brazilian Civil Rights Framework for the Internet marked a turning point in the liability of digital platforms for third-party content, as it expanded the responsibilities and obligations of digital platforms regarding moderation and accountability for publications made by third parties. This understanding directly legitimizes Anatel's preventive stance when acting before marketplaces, provides legal certainty to the Agency in consumer protection and market equity in the telecommunications sector.

On August 1, 2025, based on the legal opinions of the Attorney General's Office, in line with the understanding of the Federal Supreme Court, Anatel approved the revision of the Regulation for Conformity Assessment and Approval of Telecommunications Products through Resolution No. 780, formalizing the joint liability of marketplaces and other digital platforms involved in the marketing process, even if only acting in the dissemination and advertising, by offering telecommunications products that are not approved or in disagreement with Anatel's technical requirements. The measure includes the obligation to disclose the approval code in advertisements and to verify the regularity of the items offered. Thus, marketplaces are now jointly liable with sellers for infractions related to the offer of irregular products, standardizing an understanding already consolidated in Anatel's decisions and making it clear that the performance of these platforms goes far beyond a mere 'virtual showcase', being an effective part of the marketing chain.

³⁰ SUPREMO TRIBUNAL FEDERAL (STF) (Brazil). **STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros.** Brasília, Jun 26, 2025. Available at: <https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/>. Accessed on: Jul 29, 2025. Note: judgment still pending issuance on October 10, 2025.

2.4.2. Accountability of social media (Youtube and Facebook)

In addition to the aforementioned initiatives focused on marketplaces, in 2019, due to complaints that YouTube channels and Facebook pages were broadcasting tutorials encouraging the use and/or sale of non-approved telecommunications equipment, the SFI carried out legal consultation with PFE-Anatel on the possibility of action.

2019

Opinion No. 695/2019/PFE ANATEL/PGF/AGU ³¹

Consultation:

Monitoring and sanctioning *websites* and *YouTubers* that encourage the use and sale of unapproved products.

Response:

Yes, since their expertise relates to user safety and maintaining a healthy and competitive sector market.

Based on this understanding, the websites, digital influencers and content channels denounced were formally notified to remove irregular advertisements and to publish a public retraction regarding the dissemination of messages that encouraged the use and marketing of products not approved by Anatel.

2.4.3. Accountability of the product supply chain

Distinction between correspondence and parcel

³¹ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **Parecer n.º 00695/2019/PFE-ANATEL/PGF/AGU**. Brasília, 2019. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5Sb4M9fy78errTgNmS1KvYO6MDBaTC20TJyVcVGyXzrRmS0t-IDw7p9ZA-wiumFQdmhpVP6MIDcdohmso_Flu_ . Accessed on: Jul, 21, 2025.

Another area of activity of Anatel's Action Plan to Combat Piracy derives from the cooperation with the activities of the RFB and the Post Office, in the inspection of the imports of telecommunications products.

The RFB and the Post Office, when identifying the attempt to import telecommunications products subject to approval, notify Anatel for inspection (via email or Whatsapp). After the screening of parcels via x-ray (by Correios employees), the shipments selected for Anatel's analysis are opened, checked, photographed and evaluated regarding the possibility of homologation. Then, the wrappers are resealed by Anatel's inspector, and the "product verification form" is filled out, recording the product data, object's tracking code and its regularity. Irregular products are communicated to the RFB regarding the possibility of regularization.

Depending on the nature of the equipment, Anatel may issue an opinion for import authorization, return to the sender, retention for regularization or forfeiture. Category I products and those that operate connected to the electricity grid are generally returned to their origin, while products that can be approved by declaration of conformity receive a deadline for regularization. Illegal products, such as signal jammers and pirated decoders, are declared lost.

It is important to note that Anatel acts on behalf of the RFB in this case, limiting itself to verifying the regulatory compliance of the equipment, without administrative assessments. It so happens that, after the beginning of these activities, legal doubts arose in relation to the regularity of the procedure adopted, which led to legal consultation with PFE-Anatel.

2019**Opinion No. 770/2019/PFE ANATEL/PGF/AGU** ³²**Consultation:**

Regularity of the support procedure in the inspection of parcels.

Response:

Yes, because there is a distinction between mail and parcels, and there is no violation of mail confidentiality. Furthermore, Anatel acts as technical support to the RFB (Brazilian Federal Revenue Service).

The consolidation of Anatel's inspection actions, in conjunction with the RFB, has proven to be a fundamental instrument in the fight against piracy of telecommunications products. The technical-operational approach based on on-site inspections, compliance analysis and systematic screening of postal and express shipments contributes to inhibiting the entry, commercialization and use of irregular equipment in the country.

In addition to protecting consumers against risks from non-certified products, these actions strengthen the formal market, ensure compliance with technical standards and promote fair competition in the telecommunications sector. The continuous improvement of these procedures — combined with the development of clearer rules and effective interinstitutional mechanisms — is essential for the effectiveness of public policy to combat technological piracy in Brazil.

Import liability

³² ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **Parecer n.º 00770/2019/PFE-ANATEL/PGF/AGU**. Brasília, 2019a. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uUqrLYJw_9INcO7vcSiACcxViZXBtJEqlYo_G5oZ0GTWldJ5bFQldK3XB0qatznYBYSXvUPbLchNV9NPFSFr5wuknNblsCUZqEXN. Accessed on: Jul 21, 2025.

Still as a result of the inspection activities in cooperation with the RFB, in 2023, PFE-Anatel was questioned on the responsibility of the import operation, in cases of importation on behalf of and by order of a third party.

2023

Opinion No. 385/2023/PFE ANATEL/PGF/AGU ³³

Consultation:

Responsibility for the import operation, in cases of import on behalf of a third party.

Response:

Responsibility for the infraction of importing non-approved products falls on the purchaser of the goods, and not on the contracted importing company.

Trade relationships

Another issue that emerged in the inspection activities that required a legal statement from PFE-Anatel was related to the commercial partnerships signed by the companies holding the approval certificates issued by Anatel, aiming at the commercialization of telecommunications products in the country by third parties.

³³ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **Parecer n.º 00385/2023/PFE-ANATEL/PGF/AGU**. Brasília, 2023. Available at: sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqa6i8M5H4M2ICd-In0Ov5885pJq4NQwRwrORFIXmO-AeuSMT701C3h8Xc2ljkSS0nxN_TT-x1yflY6U6Z-DPLZK . Accessed on: Jul 21, 2025.

2020**Parecer nº 329/2020/PFE ANATEL/PGF/AGU**³⁴**Consulta:**

parcerias comerciais firmadas pelas empresas titulares dos certificados de homologação expedidos pela Anatel

Resposta:

não pode ser utilizada por terceiros se prejudicar as responsabilidades do representante comercial no Brasil
declaração particular de autorização submetida a registro público

Subsequently, Anatel's Certification and Numbering Management (ORCN), of the Superintendence of Granting and Provision of Resources (SOR) issued Memorandum No. 52/2022/ORCN/SOR³⁵, of July 5, 2022 (SEI No. 8304709), in which it reinforced the understanding of PFE-Anatel expressed in Opinion No. 329/2020/PFE-ANATEL/PGF/AGU and added that any means of proof (admitted by law) of authorization to the marketing of products issued by the holder of the product should be considered valid approval to the inspected third party (in possession of the product sold) presented during the inspection action by the telecommunications inspection, in honor of the presumption of good faith of the inspected.

In 2022, a new consultation addressed the inclusion of equipment rental in the concept of commercialization.

³⁴ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **Parecer n.º 00329/2020/PFE-ANATEL/PGF/AGU**. Brasília, 2020. Available at https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLjqrLYJw_9INcO5BzURuP5bhnuacdW_NWcJqJATu7fxFbPmmPsQQNOp8Spe2mTwP5nRw2ylwB4yQmuqdKfNHT6EjUJB25_jBtPM7. Accessed on: Jul 21, 2025.

³⁵AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brazil). Superintendência de Outorga e Recursos à Prestação. Gerência de Certificação e Numeração. **Memorando n.º 52/2022/ORCN/SOR**. Brasília, 2022. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLjqrLYJw_9INcO6twY5HXXccmxWop68eTQTqTn9ixgaLS49XCr64tUHCc5brumli3HaJDlhWKGozPY-2iCX7HynMovVtKoW_wErB. Accessed on: Jul 23, 2025.

2022**Opinion No. 223/2022/PFE ANATEL/PGF/AGU** ³⁶**Consultation:**

inclusion of equipment rental in the concept of commercialization

Response:

Yes, falling under article 83, I, of the Regulation (Resolution No. 715/2019).

Storage of non-approved equipment

An issue that also demanded a statement by PFE-Anatel was related to the scope of Article 83, I, of the Regulation on Conformity Assessment and Approval of Telecommunications Products, approved by Resolution No. 715/2019, at the time, considering the possession of non-approved equipment in stock by service providers, even if they were not in use or connected to the telecommunications network.

2021**Opinion No. 454/2021/PFE ANATEL/PGF/AGU** ³⁷**Consultation:**

The possession of non-approved equipment in stock by service providers, even if not in use or connected to the telecommunications network, is subject to penalty.

Response:

The term "use" is not limited to "actual utilization," encompassing the potential usefulness or utility of the equipment in stock, generating profit for the service provider.

³⁶ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **Parecer n.º 00223/2022/PFE-ANATEL/PGF/AGU**. Brasília, 2022a. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5ax4ZZUq2xuaXLoaMiATdWGelxczd1TqyaqC0PDsQ2KQBdeJJETr0mD_5EQjZWmZoQcKGDxWFWugbgv77UV3fU. Accessed on: Jul 21, 2025.

³⁷ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **Parecer n.º 00454/2021/PFE-ANATEL/PGF/AGU**. Brasília, 2021a. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO68ltWjtJ7YHhYP85DAYRwXLVYefsWGyUfp3DobEpcyWtximBn8o7NqLIGfbu_cwgEdo_tujUfwlH-bKJxPpKKZ. Accessed on: Jul 21, 2025.

Obstruction of inspection

Another question posed to PFE-Anatel was related to the ability of entities that manufacture, import, supply, distribute or sell telecommunications products to practice the infraction of obstruction to the Agency's inspection activity, provided for in Articles 39 to 41 of the Regulatory Oversight Regulation, approved by Resolution No. 746, of June 22, 2021.

2022

Opinion No. 103/2022/PFE ANATEL/PGF/AGU ³⁸

Consultation:

The practice of obstruction by distributors and retailers of telecommunications products.

Response:

Yes, because special subjection is not essential for Anatel's competencies. Suppliers are able to obstruct oversight, according to the Regulatory Oversight Regulation.

Inapplicability of the principle of consumption

Finally, in 2024, a consultation with PFE-Anatel on the application of the principle of consumption in cases of import and sale of telecommunications products not approved by Anatel. The legal doubt consisted in understanding whether the import conduct could be legally absorbed by the commercialization conduct - considered a subsequent stage of the same process - or whether both should be treated as autonomous infractions, subject to cumulative sanctions.

³⁸ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **Parecer n.º 00103/2022/PFE-ANATEL/PGF**. Brasília, 2022. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5sBHBMJmM0fxKRu2a4Qr-PGPvBLNbHPOOdoC0BU3-3lvzfzZw6OxT9C7mfgGXwntQyXc5eX5wVKWjddc0HI21S. Accessed on: Jul 21, 2025.

2024**Opinion No. 63/2024/PFE ANATEL/PGF/AGU** ³⁹**Consultation:**

The conduct of importing could be legally absorbed by that of commercialization.

Response:

No, because importation constitutes an autonomous act with its own potential for harm, and is not necessarily a step linked to commercialization.

Cumulative punishment for both offenses does not constitute "double jeopardy".

This interpretation reinforces Anatel's regulatory performance, allowing the full accountability of importers and traders who introduce irregular products into the market, increasing the effectiveness of control and repression mechanisms.

Synopsis

Anatel's action in combating piracy of telecommunications products has been strongly supported by PFE-Anatel opinions, which provide legal certainty to the Agency's actions.

Initially, marketplaces claimed neutrality based on the Civil Rights Framework for the Internet. However, over time, PFE-Anatel has consolidated the understanding that such platforms, when providing services such as storage and delivery, are part of the marketing chain and can be held responsible for the offer of non-approved products.

³⁹ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. **Parecer n.º 00063/2024/PFE-ANATEL/PGF/AGU**. Brasília, 2024. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqZPZr_MlidKv2NAOXJQ69gtBrT0pFzcupimr_D0SIJIM4dMMIefb5Nlui0BcjfUnUpz93sTE18zCmc569falTP7. Accessed on: Jul 21, 2025.

Other relevant milestones include the recognition that the mere offer or lease of non-approved products constitutes commercialization; that retailers and digital influencers can be held responsible; and that the storage of irregular equipment can also result in sanctions. The joint action with the RFB, especially in the inspection of postal parcels, was also legally legitimized.

In addition, PFE-Anatel ruled out the application of the principle of consumption between importation and commercialization, as it understands that they are distinct conducts with their own harm.

Based on these understandings, Anatel structured a proactive, effective and legally sound inspection action, reinforcing its role in consumer protection, network integrity and fair competition in the telecommunications sector.

2.5. Plan to Combat the Use of Clandestine Decoders

The growing spread of clandestine set-top boxes — devices used to illegally access paid-TV signals, streaming content, and other protected services — represents one of the main challenges to the integrity of the telecommunications sector in Brazil. Faced with this scenario, the National Telecommunications Agency launched, in 2023, a strategic initiative of national scope for the systematic confrontation of the use and commercialization of this equipment, significantly expanding the scope and effectiveness of the actions initiated in previous years.

Anatel's concern is the vulnerability to the network created by non-approved equipment and the provision of Conditional Access Service (technical name for subscription TV) without authorization. These concerns led to the signing of Cooperation Agreement No. 2/2023

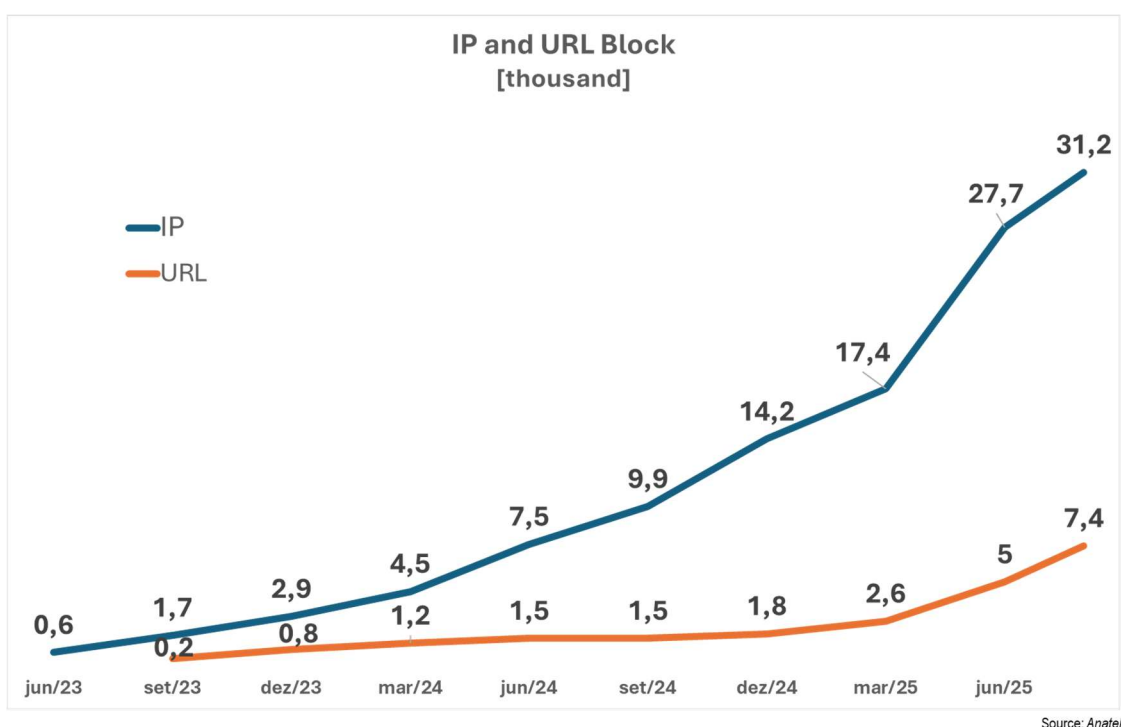
between the Agency and ABTA, to structure laboratories that perform technical analyses on equipment and other illegal means of pirated audiovisual offers, with the exchange of information, instituting the plan to combat clandestine decoders, with an integrated approach, involving normative, operational, preventive and repressive actions, protecting critical telecommunications infrastructure, ensuring the digital safety of consumers, and the economic balance of the sector.

The laboratory has technological resources to perform and monitor technical analyses on illegal equipment and offerings of pirated audiovisual, in compliance with the Action Plan to Combat the Use of Clandestine Decoders of the Conditional Access Service (SeAC). The structure has 12 monitoring screens, six workstations for in person work and can be accessed remotely.



In addition to the laboratory, there are more than 15 probes strategically distributed throughout Brazil, with at least two in each region of the country. This capillarity is essential to keep up with the operational dynamics of pirate systems, which use technologies such as CDN (Content Delivery Network), proxy servers, and P2P (peer-to-peer) networks for both device authentication and content distribution. The wide geographical dispersion of the probes allows the detection of regional variations in traffic, identification of patterns of action and guarantee of greater efficiency in the collection of data for actions to combat piracy.

The Action Plan to Combat Clandestine Decoders currently monitors around 34.1 thousand IP addresses and 8.2 thousand URLs, maintains about 2.7 thousand IP addresses blocked during certain periods (data updated on 08/23/2025), as they are directly linked to illegal activities, and monitor dozens of device models. This procedure is due to the fact that IP addresses can be reused for other lawful purposes, being monitored in case it is used again for illegal purposes.



Currently, the Agency is implementing measures to expand the Action Plan to Combat Clandestine Decoders, such as the automation of blocking orders for Internet providers and submarine cable providers (which will receive the command in real time as soon as the addresses are identified by the Agency).

Actions to combat piracy in Brazil have relevant legal support, allowing substantiated complaints to be accepted by the Public Prosecutor's Office and result in effective actions, such as the removal of groups on messaging apps (such as Telegram and WhatsApp), channels on video platforms (such as YouTube) and websites that promote the updating and use of clandestine IPTV decoders.

These complaints are based on legal provisions that typify as a crime the practice of activities aimed at the unauthorized distribution of copyrighted content, as well as the favoring of the use of clandestine equipment that violates the legal system established and maintained by Anatel. Among the main legal grounds used, the following stand out:

Law No. 9,472/1997 (General Telecommunications Law)

It prohibits the operation of telecommunications services without proper authorization, applicable to cases of using unapproved or manipulated decoders to illegally capture pay-TV signals;

Law No. 12.965/2014 (Brazilian Internet Bill of Rights)

Accountability of intermediaries and the obligation to comply with court orders for the removal of illegal content.

Law No. 8.078/1990 (Consumer Protection Code),

Consumer protection as one of the extensions of fundamental constitutional rights (Recent decision of the STF in RE 1037396 and RE 1057258, which determines that marketplaces are civilly liable under the CDC, including for acts of third parties who use their platforms).

The Public Prosecutor's Office, upon receiving technical representations and documented evidence – such as screenshots, traffic reports, sales records and illegal tutorials – can judicially request the blocking or removal of the content, with technical support from Anatel to identify servers, domains and devices involved.

This cooperation strengthens Anatel's actions within the scope of its Action Plan to Combat the Use of SeAC's Clandestine Decoders, ensuring that administrative measures, such as seizure of equipment and suspension of approvals, are complemented by judicial measures that reach the support networks and dissemination of piracy, both in the physical and digital environment.

The combination of these strategies – legal, technical and operational – has proven effective in weakening piracy structures and protecting the legal audiovisual ecosystem, preserving the rights of content producers, distributors and operators.

During research, it has been shown⁴⁰ that actions that make legal content more attractive to users or that make illegal content less attractive to users can lead pirates to migrate to legal content. Despite the difficulty in quantifying the market for irregular set top boxes, Anatel's actions are already being observed, with the main models of illegal set top boxes starting to charge to have access to pirated content and with set top box companies certified by Anatel investing in the development and production of equipment⁴¹.

⁴⁰Cf. DANAHER, Brett; SMITH, Michael D.; TELANG, Rahul. Piracy and copyright enforcement mechanisms. **Innovation Policy and the Economy**, v. 14, n. 1, p. 25-61, 2014. Available at: <https://www.journals.uchicago.edu/doi/full/10.1086/674020>. Accessed on: May 19, 2025.

⁴¹PROELETRONIC exhibits SmartPRO 4K, TV box with Anatel approval for providers and IPTV. **RTI Magazine (Aranda Net)**, São Paulo, updated on: Jun 14, 2024. Available at: <https://www.arandanet.com.br/revista/rTI/noticia/8998-Proeletronic-expoe-o-SmartPRO-4K,-TV-box-com-homologacao-da-Anatel-para-provedores-e-IPT>. Accessed on: Jul 7, 2025.

Over time, Anatel has received 5 Anti-Piracy awards granted by the National Council to Combat Piracy (CNCP), presented by the Ministry of Justice and Public Safety, in recognition of its actions to combat telecommunications piracy.

In 2024, Anatel received a recognition award from the International Telecommunication Union. The Action Plan to Combat Clandestine Decoders project entered the "Enabling Environment" category of the WSIS 2024 – World Summit on the Information Society Award, being among the four winners in the category, competing with projects from all over the world submitted by companies, regulators and governments.



Ancine

In 2025, a new Technical Cooperation Agreement was signed between the National Film Agency (Ancine) and Anatel with the purpose of establishing a fast and direct communication flow, by electronic means, between the two entities for the forwarding by Anatel, of decisions by Ancine determining the suspension and termination of unauthorized use of protected Brazilian and foreign works, through websites.

Since the signing of the agreement, 684 IP addresses have been blocked during a certain period (data updated on July 12, 2025) and 159 domains that promoted the unauthorized use of Brazilian and foreign protected works in violation of the related legislation.



3. OTHER ADMINISTRATIONS ACTIONS TO COMBAT PIRACY

Combating piracy of telecommunications products is a growing concern and shared by administrations and their regulatory bodies around the world. Technological advancement, digitalization of services, and the expansion of international e-commerce have created an environment conducive to the dissemination of irregular devices and clandestine content distribution networks, requiring coordinated, modern, and effective responses from regulatory entities.

Several countries have developed robust strategies to curb the circulation of stolen, counterfeit, and uncertified products, as well as illegal access to copyrighted content and the manipulation of critical telecommunications infrastructure. These international experiences offer valuable references for Anatel's actions and demonstrate the fundamental role of regulatory agencies in defending the public interest and the integrity of the digital ecosystem.

3.1. Combating piracy in e-commerce

In recent years, the exponential growth of e-commerce, combined with the complexity of the global logistics chain, has driven the proliferation of counterfeit and uncertified products on various digital platforms. Faced with this scenario, several international authorities have been developing cooperation and inspection mechanisms to mitigate the impacts of piracy on the economy, consumer safety, and the integrity of strategic sectors. In this context, the initiatives led by the United States Department of Homeland Security Investigations (HSI) and Europol in Europe stand out.

United States

In the United States, Homeland Security, through its Homeland Security Investigations (HSI) arm, has been systematically engaged in joint operations with the private sector, customs authorities, and regulatory agencies. Among the key actions taken are strengthening the accountability of online platforms, requiring them to adopt seller verification policies, supply chain traceability, proactive removal of illegal listings, and increased cooperation with customs authorities. The report also recommends measures such as stricter customs inspections, blocking shipments of counterfeit goods and sanctions against repeat sellers, promoting an integrated approach between government and the private sector to protect consumers and strengthen the integrity of digital commerce⁴².

Europe

In Europe, Europol coordinates transnational operations such as Operation Fake Star, aimed at cracking down on digital and physical piracy in multiple sectors, including electronics and telecommunications. Through partnerships with customs, online platforms, and national authorities, these operations have resulted in significant seizures, removal of illicit content, and blocking of distribution networks. The European actions also emphasize the use of artificial intelligence to identify fraud patterns, expanding the response capacity of the agencies involved.

Operation Fake Star was launched in 2022 under EMPACT's Operational Action (O.A.) 3.4. EMPACT Operational Action 3.4 is a specific action plan within the framework of the is a specific action plan within the framework of the European Multidisciplinary Platform against

⁴²DEPARTMENT OF HOMELAND SECURITY (United States of America). Office of Strategy, Policy & Plans. **Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States.** Available at: https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf. Accessed on: Jun 14, 2025.

Criminal Threats^{43,44} (EMPACT), focusing on police cooperation. EMPACT is a European Union initiative that reunites various law enforcement authorities, agencies and partners to fight organized and serious crime.

EMPACT operations are provided for in the Europol Programming Document, drawn up on the basis of Article 12 of the Europol Regulation⁴⁵ and Articles 32 and 33 of the Financial Regulation^{46,47} applicable to Europol.

Anatel's pioneering spirit in Brazil

Although these international actions are, for the most part, comprehensive and applied to various market segments, Brazil has stood out through a pioneering and sectoral approach, led by the National Telecommunications Agency (Anatel). Anticipating a still incipient action in the fight against piracy in e-commerce in the country, Anatel has been promoting specific actions to combat the irregular commercialization of telecommunications products, especially on digital platforms.

⁴³UNITED STATES OF AMERICA (USA). **United States Code. Title 18. Part I. Chapter 1. Section 18 - Organization defined.** Available at: <https://www.law.cornell.edu/uscode/text/18/18>. Accessed on: Jun 19, 2025.

⁴⁴COUNCIL OF THE EUROPEAN UNION. **EMPACT Terms of Reference.** Brussels: 2023. Available at: <https://data.consilium.europa.eu/doc/document/ST-8975-2023-INIT/en/pdf>. Accessed on: Jun 19, 2025.

⁴⁵EUROPOL (European Union). **Europol Programming Document 2025 – 2027.** The Hague: 2024. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2025-2027.pdf. Accessed on: Jun 14, 2025.

⁴⁶EUROPEAN UNION (EU). **Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022.** Strasbourg: 2022. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_2022.169.01.0001.01.ENG. Accessed on: Jun 14, 2025.

⁴⁷EUROPEAN UNION (EU). **Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012.** Strasbourg: 2012. Available at: https://www.epo.org/en/legal/up-upc/2022/upcaannexi_ciii.html. Accessed on: Jun 14, 2025.

Through the Action Plan to Combat Piracy, launched in 2018, Anatel has articulated an integrated strategy that involves automated monitoring of marketplaces, notifications to sellers, removal of irregular ads, seizures at physical locations and partnerships with agencies such as the Internal Revenue, Federal Police, Procons and e-commerce platforms. These initiatives place Brazil at the forefront of sectoral regulation facing the challenge of digital piracy, with significant results both in consumer protection and in ensuring the quality and compliance of the products sold.

Thus, although the US and Europe have robust and articulated structures in the fight against piracy in the digital environment, Anatel's performance is differentiated by its specialization, technical focus and interinstitutional coordination oriented to the telecommunications sector. This Brazilian pioneering spirit demonstrates the importance of targeted regulatory initiatives, reinforcing the need to strengthen digital governance in specific markets considering the protection of the public interest, technological innovation and security of telecommunications networks in the country.

3.2. Combating the use of non-approved equipment

Regarding the battle against the use and selling of non-approved products and counterfeit telecommunications equipment, some actions adopted by some administrations are presented below.

United States

In the United States, the inspection of telecommunications equipment is mainly done by the Federal Communications Commission (FCC), the regulatory body for the sector. The FCC establishes standards and regulations to ensure the safety, compatibility, and quality of equipment used in the country. In addition, other agencies and laws play a role in

enforcement, in accordance with the Law Enforcement Communication Assistance Act⁴⁸ (CALEA) and the Telecommunications Act of 1996⁴⁹.

FCC certification is a mandatory process in the United States to ensure that telecommunications equipment, including wireless devices, meets the technical standards and regulations set by the FCC ⁵⁰. This certification aims to ensure safety, compatibility with other devices, and non-interference with communication networks. FCC certification is essential for manufacturers to be able to market their products in the US.

The FCC monitors the ongoing compliance of certified equipment and can act against companies that do not meet the standards and have the authority to block the sale of equipment from foreign companies that pose national security risks. Each certified device is assigned an FCC ID code, which can be searched to identify the manufacturer and model of the device.

The FCC monitors the ongoing compliance of certified equipment and can act against companies that do not meet the standards and have the authority to block the sale of equipment from foreign companies that pose national security risks. Each certified device is assigned an FCC ID code, which can be searched to identify the manufacturer and model of the device.

⁴⁸UNITED STATES OF AMERICA (USA). **Communications Assistance for Law Enforcement Act** - P.L. 103–414, Enacted October 25, 1994 - As Amended Through P.L. 104–316, Enacted October 19, 1996. Washington (D.C.): 1996. Available at: <https://www.govinfo.gov/content/pkg/COMPS-937/uslm/COMPS-937.xml>. Accessed on: Jun 14, 2025.

⁴⁹UNITED STATES OF AMERICA (USA). **Telecommunications Act of 1996** - Public Law 104–104; Approved February 8, 1996 -As Amended Through P.L. 115–141, Enacted March 23, 2018. Washington (D.C.): 2018. Available at: <https://www.govinfo.gov/content/pkg/COMPS-959/uslm/COMPS-959.xml>. Accessed on: Jun 14, 2025.

⁵⁰FEDERAL REGISTER (United States of America). **Code of Federal Regulations**. Title 47 - Telecommunication, as of June 14th, 2025. Washington (DC): 2025. Available at: <https://www.ecfr.gov/on/2025-06-14/title-47>. Accessed on: Jun 14, 2025.

The FCC also has a role in ensuring net neutrality and overseeing internet service outages, to ensure that services are provided properly.

Japan

The legislation for certification of telecommunications equipment in Japan mainly involves two laws: the Radio Law⁵¹ and the Telecommunications Law⁵². The certification is issued by the Ministry of Internal Affairs and Communications (MIC). Depending on the characteristics of the equipment, one or both certification regimens may apply. Certification ensures that the equipment complies with Japanese laws and regulations, including safety and electromagnetic compatibility (EMC) requirements. Failure to obtain certification prevents the legal commercialization of equipment in the Japanese market.

The inspection of telecommunications equipment in Japan is done by the Ministry of Internal Affairs and Communications (MIC). The ministry is responsible for ensuring compliance with the Radio Law and Japan's Telecommunications Law. Radio and telecommunications equipment intended for sale in the country must go through a mandatory certification process.

Japan is also attentive to cybersecurity and data privacy issues, especially regarding telecommunications equipment of foreign origin. In some cases, the government may ask

⁵¹JAPAN. **The Broadcast Act** (Act No. 132 of 1950) - as amended last by the Act for Partial Revision of the Broadcast Act and Other Related Acts (Act No. 65 of 2010). Tokyo, 2010. Available at: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_5.pdf. Accessed on: Jun 14, 2025.

⁵²JAPAN. **Telecommunications Business Law** (Law No. 86 of December 25, 1984) - as amended last by: Law No. 125 of July 24, 2003. Tokyo, 2003. Available at: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/TBL/TBL-index.html. Accessed on: Jun 14, 2025.

businesses to take precautions regarding the purchase of equipment that may pose safety risks.

Europe

The Radio Equipment Directive (RED) 2014/53/EU⁵³ establishes a regulatory framework for launching radio equipment on the market. It ensures a single market for radio equipment by setting out essential requirements for safety and health, electromagnetic compatibility and efficient use of the radio spectrum. It also provides the basis for additional regulation that governs some additional aspects, including technical features for the protection of privacy, personal data and fraud. In addition, additional aspects cover interoperability, access to emergency services and compliance with the combination of radio equipment and software. The certification of telecommunications equipment in Europe is a regulated process to ensure safety, performance, and compliance with European standards. The CE marking, along with the Radio Equipment Directive (RED), plays a crucial role in the certification of communication devices and equipment that use radio frequency.

Article 45 of RED establishes the Committee for Conformity Assessment and Telecommunications Market Surveillance (TCAMok), a committee related to Regulation (EU) No 182/2011⁵⁴. TCAM issues its opinion on proposed implementation acts under RED.

⁵³EUROPEAN UNION (EU). **Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014**. Strasbourg, 2014. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053>. Accessed on: Jun 14, 2025.

⁵⁴EUROPEAN UNION (EU). **Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011**. Strasbourg, 2011. Available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32011R0182>. Accessed on: Jun 14, 2025.

África

In Botswana, the Communications Regulatory Act of 2012 requires all authorized, manufacturers and distributors to approve their electronic communication devices before connection to the public network⁵⁵.

In Ghana, the regulatory body is required by law to certify and test communication equipment for compliance with international health and safety standards⁵⁶.

3.3. Combating the connection of non-approved equipment and access to content

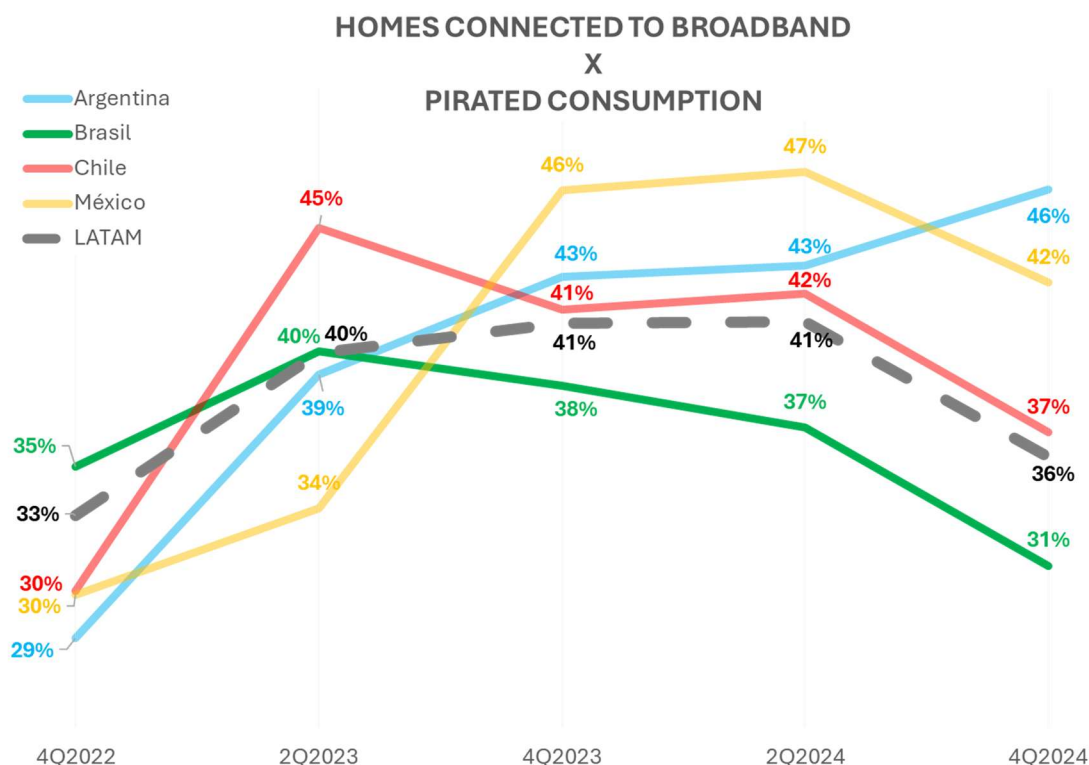
Anatel acts in the blocking of irregular set top boxes, with the goal of protecting the national telecommunications infrastructure and telecommunications users from cyber threats. The blocking of irregular set top boxes is done in line with the Plan to Combat Piracy, as it occurs on devices inspected by PACP.

Brazil reduced the consumption of online audiovisual piracy in homes connected to broadband internet in 2024. According to the latest report by the Alliance Against Audiovisual Piracy (Alianza), the ratio of households that accessed illegal content fell from 39.7% in the second quarter of 2023 to 36.8% in the same period of 2024, among the 43.9 million households connected to the internet⁵⁷.

⁵⁵INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Agreement - draft Supplement Q.Suppl.75. 2021.** Available at: <https://www.itu.int/md/T17-SG11-211201-TD-GEN-1800/en>. Accessed on: Jul 23, 2025.

⁵⁶ITU, 2021.

⁵⁷ALIANZA CONTRA LA PIRATERÍA AUDIOVISUAL - ALIANZA. **Piratería de Señales de Televisión Paga y en Línea 2q-2024.** 2024. Available at: <https://telesintese.com.br/wp-content/uploads/2024/12/Informe-de-Alianza.pdf>. Accessed on: Jul 23, 2025.



Administrations in other countries block piracy of illegal content that, in addition, affect set top boxes that transmit this content, but Anatel is a pioneer in this type of action, as it only targets devices, preventing them from connecting to servers, never blocking the content that travels through them. International studies, such as the one by Human Security⁵⁸, ratify that several administrations from other countries are interested in the work conducted in Brazil.

Next, the manners in which other administrations that share the same objective as Anatel act in protecting the national telecommunications network are presented.

⁵⁸ SATORI THREAT INTELLIGENCE AND RESEARCH TEAM, 2025.

United States

ACE (Alliance for Creativity and Entertainment) promotes actions against companies that facilitate access to unlicensed paid TV signals, with millionaire fines, revoking licenses and judicial blocks^{59, 60}

United Kingdom

In the United Kingdom, the fight against piracy is done in collaboration between the Office of Communications – Ofcom (communications regulating entity) and the Intellectual Property Crimes Unit (IPPCU), linked to the London Metropolitan Police. The actions combine physical inspection, operation against illegal IPTV networks, blocking of domains and public awareness campaigns.

Courts in the UK have granted injunctions to block live sporting events and against pirate cyberlockers and streaming sites^{61, 62} since 2011. A cyberlocker is essentially a file hosting service that is similar to a legitimate cloud storage service, such as DropBox, but one that piracy operators use to allow users to upload and download copyright-infringing content.

⁵⁹BROADBAND TV NEWS CORRESPONDENT. Anti-piracy alliance ACE settles copyright infringement cases with IPTV operators. **Broadband TV News**, Aug 17. 2024. Available at: <https://www.broadbandtvnews.com/2024/Aug/17/anti-piracy-alliance-ace-settles-copyright-infringement-cases-with-iptv-operators/>. Accessed on: Jul 7, 2025.

⁶⁰BRIEL, Robert. ACE takes legal action against IPTV pirates. **Broadband TV News**, Mar 11, 2025. Available at: <https://www.broadbandtvnews.com/2025/03/11/ace-takes-legal-action-against-iptv-pirates/>. Accessed on: Jul 7, 2025.

⁶¹DICKERSON Jeremy. Premier League 'live' blocking order against livestream servers renewed for 2017/18 season. **Lexology**, Aug 2, 2017. Available at: <https://www.lexology.com/library/detail.aspx?g=a68db02f-12f5-4169-aa8f-56d35395d3b5>. Accessed on: Jul 23, 2025.

⁶²ENGLAND AND WALES HIGH COURT (United Kingdom). Chancery Division. **Matchroom Boxing Ltd & Anor v British Telecommunications Plc & Ors** (Decision). London, Sep 20, 2018. Available at: <https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2018/2443.html&query=IL-2018-000155+>. Accessed on: Jul 23, 2025.

Piracy cyberlockers allow users to upload/download illegal material for free and reward users who upload illegal content, allowing them to earn money each time their content is downloaded. Piracy operators allow users to create shareable URL links to make it easier for third parties to access pirated content⁶³.

According to studies by Danaher et al.⁶⁴, when 19 major piracy sites were blocked simultaneously in October-November 2013, there was a sharp reduction in total piracy levels, which led users of the blocked sites to increase their use of paid legal streaming sites by 11%. Blocking 53 sites in 2014 caused users to decrease piracy and increase their use of legal subscription sites by 7 to 12 percent.

Europe

The European Union promotes integrated action through the EUIPO (European Union Intellectual Property Office) and Europol (European Union Agency for Law Enforcement Cooperation), coordinating joint campaigns with national administrations to combat digital piracy. The "IPTV Crime and Enforcement" project is an example of a cross-border initiative that involves seizing equipment, tracking financial transactions, and dismantling organized networks that operate pirate IPTV in multiple EU countries.

Blocking websites for copyright enforcement is legally possible across the EU,⁶⁵ but it is actively used only in a subset of Member States. Several rulings by the Court of Justice of

⁶³HEENAN, Emily. High Court blocks cyberlocker and stream-ripping websites. **Lexology**, Mar 24, 2021. Available at: <https://www.lexology.com/library/detail.aspx?g=87ca8734-1d84-4be3-85b9-325ec9d56d4d>. Accessed on: Jul 23, 2025.

⁶⁴DANAHER, Brett; SMITH, Michael D.; TELANG, Rahul, **The Effect of Piracy Website Blocking on Consumer Behavior**. 2019. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612063. Accessed on: Jul 23, 2025.

⁶⁵EUROPEAN UNION (EU). **Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019**. Strasbourg, 2019. Available at: <https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng>. Accessed on: Jun 16, 2025.

the European Union (CJEU), the EU's highest court, have clarified its use as a valid anti-piracy tool. While these court rulings support the availability of dynamic blocking — blocking mirror and proxy sites, as well as the primary IP address — only static injunctions are available in all Member States. Ireland, Spain, and the United Kingdom have taken this practice a step further and implemented real-time blocking injunctions.

In 2021, Germany created Die Clearingstelle Urheberrecht im Internet (CUII), a joint initiative of copyright holders (music, film, gaming, and scientific publishing sectors), industry associations, internet service providers (ISPs), legal experts, and the government to more efficiently manage the blocking of websites that systematically infringe copyright, as well as consider net neutrality requirements. All decisions are subject to judicial review and evaluation by the Bundesnetzagentur (BNetzA), Germany's Federal Network Agency, which is responsible for enforcing net neutrality requirements. This refutes another unjustified criticism: blocking websites undermines net neutrality. BNetzA considers the implications of net neutrality in each block request⁶⁶.

In December 2024, the German Federal Office for Information Security (BSI) conducted an operation against the BadBox 2.0 botnet, which infected Android devices and smart TVs. The botnet, already present in a pre-installed form on several devices such as set top boxes, tablets and vehicle systems, had its communication interrupted on about 30 thousand devices during the first phase of the operation⁶⁷.

⁶⁶HOMANN, Jochen. **Online Copyright Clearance System arranges block of streaming site**. Bonn: Bundesnetzagentur, Mar 11, 2021. Available at: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2021/20210311_Clearingstelle.html. Accessed on: Jul 23, 2025.

⁶⁷SATORI THREAT INTELLIGENCE AND RESEARCH TEAM, 2025.

Section 60c of the Finnish Copyright Act provides the legal framework for determining that an ISP blocks access to infringing websites⁶⁸. Finland first blocked The Pirate Bay in 2011.

In Italy, the blocking of websites became possible with the implementation of Article 8.3 of the EU Copyright Directive⁶⁹, criminal law and a special administrative procedure (AGCOM, Regulation), which came into force at the end of March 2014. Under the regulation, AGCOM (the national communications regulatory authority) has the power to order ISPs to block access to infringing websites after consideration of a complaint filed by a rights holder and there is an "expedited" procedure for websites responsible for massive copyright infringements.

Canada

CRTC (Canadian Radio-television and Telecommunications Commission) maintains a strong presence in defense of intellectual property and the integrity of telecommunications networks. The agency has the authority to determine the blocking of pirate sites and coordinate with ISPs (Internet Service Providers) actions to deactivate clandestine services. The "FairPlay Canada" program, launched with the support of media companies, operators and civil entities, aims to combat illegal streaming through block lists maintained by court decision and technical support from providers.

Asia

Japan implements severe penalties for those who share or sell devices capable of circumventing content encryption systems.

⁶⁸FINLAND. **Copyright Act (Act No. 404/1961 of July 8, 1961, as amended up to Act No. 608/2015 of May 22, 2015)**. 2015. Available at: <https://www.wipo.int/wipolex/en/legislation/details/15992>. Accessed on: Jul 23, 2025.

⁶⁹EU, 2019.

In South Korea, the blocking of websites is possible through an administrative procedure that involves government authorities. According to the information available by the World Intellectual Property Organization (WIPO).⁷⁰ By early 2021, more than 180 domains had been blocked, including popular BitTorrent sites and cyberlockers. In January 2019, a new center was launched by the Korean Communications Standards Commission (KCSC) to deal with website-blocking apps faster, as part of its overall mission to combat child pornography, video piracy, and illegal gambling.

Austrália

On 22 June 2015, the Australian government enacted the Copyright Amendment^{71,72} (Online Infringement). Section 115A of the Amendment gives the federal court in Australia the power to order an injunction to require an ISP to block access to "online venues," even outside of Australia, whose primary purpose is to infringe or facilitate copyright infringement. "Online location" has been used as an intentionally broad term that includes but is not limited to websites, as well as adapting to future technologies. Currently, copyright holders and ISPs can privately agree to extend the injunction to include any new websites that host the same infringing material as the original court order, without having to go to court to obtain a new injunction. Similarly, search engines like Google and Bing are held responsible for removing links to blocked websites, as well as their mirrors and proxies.

⁷⁰https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_13.pdf

⁷¹AUSTRALIA. **Copyright Amendment (Online Infringement) Act 2015**. Canberra, 2015. Available at: <https://www.legislation.gov.au/C2015A00080/latest/text>. Accessed on: Jul 23, 2025.

⁷²MOTION PICTURE ASSOCIATION (MPA). **Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior: December 2018**. 2020. Available at: <https://www.mpa-apac.org/wp-content/uploads/2020/02/Australia-Site-Blocking-Summary-January-2020.pdf>. Accessed on: Jul 23, 2025.

According to the report *Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior: December 2018*⁷³, traffic to websites presenting legal content increased by 5% in the period after the blocks.

3.4. Multilateral Partnerships and Global Forum

International bodies such as the International Telecommunication Union (ITU) and the World Intellectual Property Organization (WIPO) promote the exchange of good practices between administrations and encourage the development of common technical standards. The ITU, in particular, recognizes piracy as a risk to the resilience of networks and the digital sovereignty of countries, recommending the adoption of integrated national policies to combat the circulation of non-compliant equipment.

Anatel, in its competence as the international representative of Brazil on telecommunications subjects, actively works with the ITU, including leading the debate internationally with the preparation of the Technical Report ITU-T QSTR-MCM-UC⁷⁴, which deals with use cases of combating the misappropriation of multimedia content, and the proposition of the new recommendation on combating the misappropriation of multimedia content (REC. ITU-T Q.FC-MCM), within the scope of the Study Commission 11, of the standardization sector of the ITU⁷⁵.

⁷³MPA, 2020.

⁷⁴INTERNATIONAL TELECOMMUNICATION UNION (ITU). **LS on the agreement of Technical Report ITU-T QSTR-MCM-UC "Use Cases on the combat of Multimedia Content Misappropriation"**. 2024. Available at: <https://www.itu.int/md/T22-SG16-240415-TD-GEN-0295/en>. Accessed on: Jul 23, 2025.

⁷⁵INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Output - Updated text of the draft Recommendation ITU-T Q.FC-MCM: Framework for combating Multimedia Content Misappropriation**. Geneva, 2024. Available at: <https://www.itu.int/md/T22-SG11-240501-TD-GEN-0993/en>. Accessed on: Jul 23, 2025.

Several member countries of the International Telecommunication Union (ITU) are seeking to implement regulatory methods and solutions to combat stolen and counterfeit mobile phones. These initiatives are largely based on ITU-T Q.5050 and Q.5051 recommendations, which had the active participation of the Brazilian administration in its creation, notably Anatel's contributions.

Thus, what can be seen with the studies of the work done by other countries is that there are efforts with similar processes in the fight against stolen or counterfeit mobile phones and content. However, the Brazilian experience in combating piracy is broader than any country, as there is a strong action by Anatel with the conduction of the PACP, which covers the most varied segments of the marketing chain and has the integration of several agencies, public and private, especially customs agencies.

As for combating the misuse of copyrighted content, Anatel's actions focuses on preventing the connection of equipment used for these illicit purposes to telecommunications networks, while some countries act directly in blocking protected content. Both perspectives open up possibilities for administrations and regulatory bodies for the protection of copyright and proper use of telecommunications networks, according to the legal understanding of the legislation of each country.

4. FUTURES CHALLENGES AND OPPORTUNITIES

The fight against telecommunications piracy is a strategic front of Anatel's regulatory action, which requires constant technological updating, institutional articulation and alignment with the dynamics of the digital market. While significant progress has been made — such as seizures of non-approved equipment, remote blocking of clandestine devices, cracking down on illegal IPTV networks, and strengthening enforcement — the landscape still poses complex and multifactorial challenges, while providing opportunities for regulatory innovation and cross-industry collaboration.

4.1. Key Challenges

Misinformation and Low-Cost Appeal - Many consumers still do not realize the risks associated with the use of non-approved devices. The attractiveness of low cost, coupled with the false sense of legality of some sales channels, contributes to the continued demand for pirated products.

Capillarity and Logistics of Illegal Trade - The distribution structure of clandestine devices involves multiple channels — physical and virtual — making inspection more costly and reactive. Effective action requires expanding real-time response capacity and preventive intelligence.

Legal and Normative Limitations - Although there are normative instruments that give Anatel the competence to act in the repression of piracy, there are still regulatory and legal gaps that make it difficult to hold offenders accountable, especially in cases where illegal services are offered by entities outside the country.

Fragmentation and Anonymity of Digital Distribution - The commercialization of decoders and pirated services takes place, in large part, through international digital platforms, groups on social media and marketplaces operating outside the Brazilian

authority. This requires multilateral solutions and cooperation with digital intermediaries and international entities.

Technological Sophistication of Pirated Devices - The technology applied to illegal equipment adapts and advances rapidly, with hiding capabilities, remote updating and integration with decentralized platforms, which makes it difficult to identify and block. Many devices have over-the-air firmware mechanisms (technology that allows the update of the equipment's control software through a radio connection, such as Wi-Fi or mobile data), which circumvent conventional detection systems.

4.2. Future Opportunities

Progress in Cooperation with Digital Platforms - There is room to consolidate cooperation agreements with large marketplaces and social media to enable the proactive and automated removal of ads and profiles involved in the commercialization of irregular products, using technical criteria defined by Anatel.

Integration with Customs and Artificial Intelligence Systems - Anatel can expand the use of AI and machine learning technologies in conjunction with the Brazilian Internal Revenue Service and security agencies, for automatic identification of suspicious cargo and blocking at origin, still at the country's entry points.

Review and Modernization of the Regulatory Framework - The fight against piracy can be strengthened through legislative proposals that more objectively criminalize the import, commercialization and operation of illegal devices and the consumption of multimedia content that violates copyright and intellectual property, as well as by updating resolutions to allow for faster and more interoperable responses.

Strengthening Educational Campaigns - Consumer awareness is one of the pillars of the long-term effectiveness of anti-piracy strategies. Anatel can expand its digital education and

citizenship actions, in partnership with schools, Procons, operators and media outlets, reinforcing risks to security, privacy and legality.

Active Participation in International Forums - Engagement in initiatives such as those of the ITU, OECD, WIPO and networks of telecommunications administrators can bring learning, technical standardization and transnational good practices that contribute to more effective actions in the national territory.

Adoption of Automated Response Infrastructures - The creation of integrated incident response systems, with the participation of access providers, operators, and technology companies, can enable automated, real-time blocking of irregular devices and servers, based on regulatory and security data.

Strengthening Partnerships with Other Public Administration Entities - In 2025, an agreement was signed with Ancine, allowing the blocking not only of set top boxes but also of websites and applications for the distribution of pirated content.

Furthermore, negotiations continue with the RFB to expand joint actions with Anatel in ports and airports, to curb the importing of non-approved equipment.

The telecommunications piracy scenario is constantly changing, requiring Anatel to take a proactive, adaptable and technological stance. The combination of regulatory, operational, and cultural challenges must be addressed with a systemic vision, inter-institutional engagement, and continuous innovation.

The opportunities for strengthening the fight against piracy in Brazil are significant — from the strategic use of data and artificial intelligence to the development of public policies integrated with the private sector and civil society. By leading this movement with technical rigor and public commitment, Anatel contributes to the protection of legality, digital sovereignty and the rights of the Brazilian consumer.

REFERENCES

1. In technical vocabulary, a connection or interconnection is the linking of a user's terminal or network to public telecommunications networks. Available at: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2018/1142-resolucao-693>. Accessed on: Jul 7, 2025.
2. BRAGA, Lucas; FAVRETTO, Everton. Anatel multa clínica veterinária por usar produto sem homologação. Tecnoblog, 23 fev. 2021. Updated on Nov 14, 2023. Available at: <https://tecnoblog.net/noticias/anatel-multa-clinica-veterinaria-por-usar-produto-sem-homologacao/>. Accessed on: Jul 7, 2025.
3. POLÍCIA apreende bloqueador de sinal de GPS usado por quadrilha de roubos de cargas no Rio. G1, Rio de Janeiro, Feb 14, 2019. Available at: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/02/14/policia-apreende-bloqueador-de-sinal-de-gps-usado-por-quadrilha-de-roubos-de-cargas-no-rio.ghtml>. Accessed on: Jul 7, 2025.
4. ALMEIDA, Esther. Dono de construtora morto em SP: saiba como evitar clonagem de controle de portão. O Globo, Rio de Janeiro, Jun 7, 2025. Updated on Jul 7, 2025). Available at: <https://oglobo.globo.com/economia/tecnologia/noticia/2025/06/07/dono-de-construtora-morto-em-sp-saiba-como-evitar-clonagem-de-controle-de-portao.ghtml>. Accessed on: Aug 7, 2025.
5. GOLPE da chave: bandidos já clonam sinal à distância e levam seu carro. UOL, Oct 5, 2023. Available at: <https://www.uol.com.br/carros/noticias/redacao/2025/01/04/bandidos-em-dupla-ja-clonam-chave-a-distancia-e-levam-carro-em-segundos.htm>. Accessed on: Jul7, 2025.
6. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL. Anatel apresenta esclarecimentos sobre o Flipper Zero. Brasília, Mar 29, 2023. Updated on May 31, 2023. Available at: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-apresenta-esclarecimentos-sobre-o-flipper-zero>. Accessed on: Jul 7, 2025.
7. CINTRA, Caroline. "Perdi meu coração", diz mãe de garoto que morreu após choque em carregador. Correio Braziliense, Brasília, Aug 12, 2020. Updated on Aug 12, 2020. Available at: <https://www.correiobraziliense.com.br/cidades-df/2020/08/4868126--perdi-meu-coracao---diz-mae-de-garoto-que-morreu-apos-choque-em->

- carregador.html. Accessed on: Jul7, 2025.
8. VÍDEO: incêndio em auditório pode ter sido provocado por carregador de celular, dizem bombeiros. G1 Tocantins, Jan 8, 2024 (updated on Jul 2024). Available at: <https://g1.globo.com/to/tocantins/noticia/2024/01/08/video-incendio-em-auditorio-pode-ter-sido-provocado-por-carregador-de-celular-dizem-bombeiros.ghtml>. Accessed on: Jul 7, 2025.
 9. DIOGO, Darcianne. Jovem sofre queimadura de 1º grau após celular explodir na tomada no DF. Correio Braziliense, Brasília, May 14, 2023. Available at: <https://www.correiobraziliense.com.br/cidades-df/2023/05/5094486-jovem-sofre-queimadura-de-1-grau-apos-celular-explodir-na-tomada-no-df.html>. Accessed on: Jul 7, 2025.
 10. SILVA, Cristiane. Celulares já mataram 23 no Brasil: especialistas apontam principais vilões. Correio Braziliense, Brasília, Oct 1, 2019. Available at: https://www.correiobraziliense.com.br/app/noticia/tecnologia/2019/10/01/interna_tecnologia,793061/celulares-ja-mataram-23-no-brasil-especialistas-apontam-principais-vi.shtml. Accessed on: Jul 7, 2025.
 11. Cf. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendência de Fiscalização. Informe nº 4/2021/FIGF4/FIGF/SFI. Brasília, 2021. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5PKr37An4NSs6sd1c9IPofluH3e-yRwywlgZFvUh-qW-f-MR8ln0HwABi8MWbOkspZajukWXFCisvs8oBuJmvd. Accessed on: Jul 23, 2025.
 12. Cf. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendência de Fiscalização. Informe nº 8/2022/FIGF4/FIGF/SFI. Brasília. 2022. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqbGHzc2pUgPteuRLZ6SDuwZoTzukaE9xm340u-SmUAwHzdKU2tlv4WgKQmypi8cvl3ntyOGfLQji7o_Cb0uH4U-. Accessed on: Jul 23, 2025.
 13. KUMAR, Sachin; MADHAVAN, L.; NAGAPPAN, Meiyappan; SIKDAR, Biplab. Malware in Pirated Software: Case Study of Malware Encounters in Personal Computers. In: INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY

- (ARES), 11, 2016, Salzburg, Austria, Anais [...] [s.l.], 2016, p. 423-427. Available at: <https://ieeexplore.ieee.org/document/7784601>. Accessed on: Jul 25, 2025.
14. BAŞESKIOĞLU, Mehmet Özer; TEPECİK, Abdülkadir. Cybersecurity, Computer Networks Phishing, Malware, Ransomware, and Social Engineering Anti-Piracy Reviews. In: INTERNATIONAL CONGRESS ON HUMAN-COMPUTER INTERACTION, OPTIMIZATION AND ROBOTIC APPLICATIONS (HORA), 03, 2021, Ankara, Anais [...]. [s.l.]: IEEE, 2021, p. 1-5. Available at: <https://ieeexplore.ieee.org/document/9461272>. Accessed on: Aug 31, 2025.
 15. VAN DER SAR, Ernesto. The Pirate Bay Website Runs a Cryptocurrency Miner. 2017. Available at: <https://torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/>. Accessed on: Jun 14, 2025.
 16. SURIADI, Suriadi; SUSNJAK, Teo; PONDER-SUTTON, Agate; WATTERS, Paul; SCHUMACHER, Christoph. Using data-driven and process mining techniques for identifying and characterizing problem gamblers in New Zealand. Complex Systems Informatics and Modeling Quarterly, Riga, Latvia, n. 9, p. 44–66, 2016. DOI: 10.7250/csimq.2016-9.03. Available at: <https://csimq-journals.rtu.lv/csimq/article/view/csimq.2016-9.03..> Accessed on: Aug 31, 2025.
 17. SATORI THREAT INTELLIGENCE AND RESEARCH TEAM. Satori Threat Intelligence Disruption: BADBOX 2.0 Targets Consumer Devices with Multiple Fraud Schemes. 2025. Available at: <https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/>. Accessed on: May 19, 2025.
 18. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL. Anatel emite alerta sobre malware BadBox 2.0 em TV Boxes piratas. Brasília, DF: Anatel, Jul 25, 2025. Available at: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-emite-alerta-sobre-malware-bad-box-2-0-em-tv-boxes-piratas>. Accessed on: Aug 14, 2025.
 19. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendência de Outorga e Recursos à Prestação, Superintendência de Fiscalização. Despacho Decisório nº 5657/2024/ORCN/SOR. Brasília, 2024. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYmK7UOAaw8fj5jIUHIDwe0NhuPf9JzG-Uyip5lqqRmZXWq3_FHP60CDJBwjfirYwgLZsBySFp8Kq5_qlYt8sBgO. Accessed on: Jul 23, 2025.
 20. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendência de Outorga e Recursos à Prestação, Superintendência de Fiscalização,

- Superintendência de Controle de Obrigações. Despacho Decisório nº 5686/2024/ORCN/SOR. Brasília, 2024a. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqZApP7PurlyWa1s0oaWqCwkV7A2ZHNvzF5QswTfpGIhwO97BwkTz78Z4IVzkLfICyMkA1dhf6kvAa4Vna4sXaT3. Accessed on: Jul 23, 2025.
21. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Anatel, Polícia Federal e Receita Federal realizam ação conjunta em Pelotas (RS). Brasília, DF: Anatel, Jul 9, 2025. Available at: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-policia-federal-e-receita-federal-realizam-acao-conjunta-em-pelotas-rs>. Accessed on: Jul 27, 2025.
22. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Anatel e PF desarticulam esquema milionário de "TV Box" e "Gatonet" em Operação PRAEDO. Brasília, DF: Anatel, Jul 29, 2025. Available at: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-e-pf-desarticulam-esquema-milionario-de-tv-box-e-gatonet-em-operacao-praedo>. Accessed on: Jul 29, 2025.
23. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n.º 01580/2015/PFE ANATEL/PGF/AGU. Brasília, 2015. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?Yj72kUioo_z14_E1ere_NErKAAYpCDMsB4uhQFHnURzICcsEezBx7gPUNtxU8bNUcaTcr0nBnveExhjlYaFQPg7w474YcqjoUmoQPS4yTNLNaUCTtkxM0SgmZMjHGDh. Accessed on: Jul 21, 2025.
24. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. PARECER n.º 00524/2018/PFE-ANATEL/PGF/AG. Brasília, 2018. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5Aq93gDCiAKZgfvdufplsL2yUPD34g1U-JBQb1D9R_dacgaUTkfl4JNVnd23QsN5FoeTx1MPAZEgSqZRwJalOS. Accessed on: Jul 21, 2025.
25. MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito, Passo Fundo, RS, Brasil, v. 16, n. 1, p. 1–33, 2020. DOI: 10.18256/2238-0604.2020.v16i1.4103. Available at:

- <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103>. Accessed on: Aug 10, 2025.
26. In this sense, cf. MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. *Revista de Direito do Consumidor*, v. 106, jul./ago., p. 37-69, 2018.
 27. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA SECRETARIA NACIONAL DO CONSUMIDOR COORDENAÇÃO DE CONSUMO SEGURO E SAÚDE Nota Técnica n.º 610/2019/CCSS/CGCTSA/DPDC/SENACON/MJ, Available at: <https://www.gov.br/mj/pt-br/assuntos/noticias/senacon-questiona-sites-sobre-politica-para-evitar-anuncio-e-venda-de-produtos-falsificados/NTPirataria.pdf> . Accessed on: Aug 10, 2025.
 28. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA SECRETARIA NACIONAL DO CONSUMIDOR COORDENAÇÃO DE CONSUMO SEGURO E SAÚDE Nota Técnica n.º 91/2020/CCSS/CGCTSA/DPDC/SENACON/MJ, Available at: <https://www.gov.br/mj/pt-br/aceso-a-informacao/perguntas-frequentes/consumidor/consumo-seguro-e-saude#:~:text=Nota%20T%C3%A9cnica%20n%C2%BA%2091/2020,Permanentes%20de%20Acidentes%20de%20Consumo> . Accessed on: Aug 10, 2025.
 29. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n.º 00453/2021/PFE-ANATEL/PGF/AGU. Brasília, 2021. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO4t0UuV0d7ERjywGrRjfzWiwaEv5qDiucqzOSkmGuYZGIA6a-B118QiuybPF9Bdki34wmGMyB6GhHGdoEUeFV5_ . Accessed on: Jul 21, 2025.
 30. SUPREMO TRIBUNAL FEDERAL (STF) (Brasil). STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros. Brasília, Jun 26, 2025. Available at: <https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/>. Accessed on: Jul 29, 2025. Note: judgment still pending issuance on October 10, 2025.
 31. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n.º 00695/2019/PFE-ANATEL/PGF/AGU. Brasília, 2019. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-

- wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5Sb4M9fy78errTgNmS1KvYO6MDBaTC20TJyVcVGyXzrRmS0t-IDw7p9ZA-wiumFQdmhpVP6MIDcdohmso_Flu_ . Accessed on: Jul 21, 2025.
32. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n.º 00770/2019/PFE-ANATEL/PGF/AGU. Brasília, 2019a. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO7vcSiACcxViZXBtJEqIYo_G5oZ0GTWldJ5bFQldK3XB0qatznYBYSXvUPbLchNV9NPFsFr5wuknNblsCUZqEXN . Accessed on: Jul 21, 2025.
33. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n.º 00385/2023/PFE-ANATEL/PGF/AGU. Brasília, 2023. Available at: sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqa6i8M5H4M2ICd-In0Ov5885pJq4NQwRwrORFIXmO-AeuSMT701C3h8Xc2ljkSS0nxN_TT-x1yflY6U6Z-DPLZK. Accessed: Jul 21, 2025.
34. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n.º 00329/2020/PFE-ANATEL/PGF/AGU. Brasília, 2020. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5BzURuP5bhnuacdW_NWcJqJATu7fxFbPmmPsQQNOp8Spe2mTwP5nRw2ylwB4yQmuqdKfNHT6EjUJB25_jBtPM7. Accessed on: Jul 21, 2025.
35. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendência de Outorga e Recursos à Prestação. Gerência de Certificação e Numeração. Memorando n.º 52/2022/ORCN/SOR. Brasília, 2022. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO6twY5HXXccmxWop68eTQTqTn9ixgaLS49XCr64tUHCc5brumli3HaJDIhwKGOzPY-2iCX7HynMovVtKoW_wErB. Accessed on: Jul 23, 2025.
36. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n.º

- 00223/2022/PFE-ANATEL/PGF/AGU. Brasília, 2022a. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5ax4ZZUq2xuaXLoaMiATdWGeIxczd1TqyaqC0PDsQ2KQBdeJJETr0mD_5EQjZWmZoQcKGDxWFWugbgv77UV3fU. Accessed on: Jul 21, 2025.
37. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n.º 00454/2021/PFE-ANATEL/PGF/AGU. Brasília, 2021a. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO68ltWJtJ7YHhYP85DAYRwXLVYefsWGyUfp3DobEpcyWtximBn8o7NqLIGfbu_cwgEdo_tujUfwlH-bKJxFpKKZ. Accessed on: Jul 21, 2025.
38. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n.º 00103/2022/PFE-ANATEL/PGF. Brasília, 2022. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5sBHBMJmM0fxKRu2a4Qr-PGPvBLNbHPOOdoC0BU3-3lvzfzZw6OxT9C7mfgGXwntQyXc5eX5wVKWjddc0HI21S. Accessed on: Jul 21, 2025.
39. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n.º 00063/2024/PFE-ANATEL/PGF/AGU. Brasília, 2024. Available at: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqZPZr_MlidKv2NAOXJQ69gtBrT0pFzcupimr_D0SIJIM4dMMlefb5Nlui0BcjfUnUpz93sTE18zCmc569falTP7. Accessed on: Jul 21, 2025.
40. Cf. DANAHER, Brett; SMITH, Michael D.; TELANG, Rahul. Piracy and copyright enforcement mechanisms. *Innovation Policy and the Economy*, v. 14, n. 1, p. 25-61, 2014. Available at: <https://www.journals.uchicago.edu/doi/full/10.1086/674020>. Accessed on: May 19, 2025.
41. PROELETRONIC expõe o SmartPRO 4K, TV box com homologação da Anatel para provedores e IPTV. Revista RTI (Aranda Net), São Paulo, updated on Jun14, 2024.

- Available at: <https://www.arandanet.com.br/revista/rti/noticia/8998-Proeletronic-expoe-o-SmartPRO-4K,-TV-box-com-homologacao-da-Anatel-para-provedores-e-IPT>. Accessed on: Jun 7, 2025.
42. DEPARTMENT OF HOMELAND SECURITY (Estados Unidos da América). Office of Strategy, Policy & Plans. Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States. Available at: https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf. Accessed on: Jun 14, 2025.
43. ESTADOS UNIDOS DA AMÉRICA (EUA). United States Code. Title 18. Part I. Chapter 1. Section 18 - Organization defined. Available at: <https://www.law.cornell.edu/uscode/text/18/18>. Accessed on: Jun 19, 2025.
44. COUNCIL OF THE EUROPEAN UNION (União Europeia). EMPACT Terms of Reference. Bruxelas: 2023. Available at: <https://data.consilium.europa.eu/doc/document/ST-8975-2023-INIT/en/pdf>. Accessed on: Jun 19, 2025.
45. EUROPOL (União Europeia). Europol Programming Document 2025 – 2027. Haia: 2024. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2025-2027.pdf. Accessed on: Jun 14, 2025.
46. UNIÃO EUROPEIA (UE). Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022. Estrasburgo: 2022. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2022.169.01.0001.01.ENG. Accessed on: Jun 14, 2025.
47. UNIÃO EUROPEIA (UE). Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012. Estrasburgo: 2012. Available at: https://www.epo.org/en/legal/up-upc/2022/upcaannexi_ciii.html. Accessed on: Jun 14, 2025.
48. ESTADOS UNIDOS DA AMÉRICA (EUA). Communications Assistance for Law Enforcement Act - P.L. 103–414, Enacted October 25, 1994 - As Amended Through P.L. 104–316, Enacted October 19, 1996. Washington (D.C.): 1996. Available at: <https://www.govinfo.gov/content/pkg/COMPS-937/uslm/COMPS-937.xml>. Accessed on: Jun 14, 2025.
49. ESTADOS UNIDOS DA AMÉRICA (EUA). Telecommunications Act of 1996 - Public

- Law 104–104; Approved February 8, 1996 -As Amended Through P.L. 115–141, Enacted March 23, 2018. Washington (D.C.): 2018. Available at: <https://www.govinfo.gov/content/pkg/COMPS-959/uslm/COMPS-959.xml>. Accessed on: Jun 14, 2025.
50. FEDERAL REGISTER (Estados Unidos da América). Code of Federal Regulations. Title 47 - Telecommunication, as of June 14th, 2025. Washington (DC): 2025. Available at: <https://www.ecfr.gov/on/2025-06-14/title-47>. Accessed on: Jun 14, 2025.
51. JAPÃO. The Broadcast Act (Act No. 132 of 1950) - as amended last by the Act for Partial Revision of the Broadcast Act and Other Related Acts (Act No. 65 of 2010). Tóquio, 2010. Available at: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_5.pdf. Accessed on: Jun 14, 2025.
52. JAPÃO. Telecommunications Business Law (Law No. 86 of December 25, 1984) - as amended last by: Law No. 125 of July 24, 2003. Tóquio, 2003. Available at: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/TBL/TBL-index.html. Accessed on: Jun 14, 2025.
53. UNIÃO EUROPEIA (UE). Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014. Strasbourg, 2014. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053>. Accessed on: Jun 14, 2025.
54. UNIÃO EUROPEIA (UE). Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011. Strasbourg, 2011. Available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32011R0182>. Accessed on: Jun 14, 2025.
55. UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES (UIT). Agreement - draft Supplement Q.Suppl.75. 2021. Available at: <https://www.itu.int/md/T17-SG11-211201-TD-GEN-1800/en>. Accessed on: Jul 23, 2025.
56. UIT, 2021.
57. ALIANZA CONTRA LA PIRATERÍA AUDIOVISUAL - ALIANZA. Piratería de Señales de Televisión Paga y en Línea 2q-2024. 2024. Available at: <https://telesintese.com.br/wp-content/uploads/2024/12/Informe-de-Alianza.pdf>. Accessed on: Jul 23, 2025.

58. SATORI THREAT INTELLIGENCE AND RESEARCH TEAM, 2025.
59. BROADBAND TV NEWS CORRESPONDENT. Anti-piracy alliance ACE settles copyright infringement cases with IPTV operators. Broadband TV News, Aug 17, 2024. Available at: [https://www.broadbandtvnews.com/2024 ago. 17/anti-piracy-alliance-ace-settles-copyright-infringement-cases-with-iptv-operators/](https://www.broadbandtvnews.com/2024/ago.17/anti-piracy-alliance-ace-settles-copyright-infringement-cases-with-iptv-operators/). Accessed on: Jul 7, 2025.
60. BRIEL, Robert. ACE takes legal action against IPTV pirates. Broadband TV News, 11 mar. 2025. Available at: <https://www.broadbandtvnews.com/2025/03/11/ace-takes-legal-action-against-iptv-pirates/>. Accessed on: Jul 7, 2025.
61. DICKERSON Jeremy. Premier League 'live' blocking order against livestream servers renewed for 2017/18 season. Lexology, Aug 2, 2017. Available at: <https://www.lexology.com/library/detail.aspx?g=a68db02f-12f5-4169-aa8f-56d35395d3b5>. Accessed on: Jul 23, 2025.
62. ENGLAND AND WALES HIGH COURT (Reino Unido). Chancery Division. Matchroom Boxing Ltd & Anor v British Telecommunications Plc & Ors (Decision). Londres, Sep 20, 2018. Available at: <https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2018/2443.html&query=IL-2018-000155+>. Accessed on: Jul 23, 2025.
63. HEENAN, Emily. High Court blocks cyberlocker and stream-ripping websites. Lexology, Mar 24, 2021. Available at: <https://www.lexology.com/library/detail.aspx?g=87ca8734-1d84-4be3-85b9-325ec9d56d4d>. Accessed on: Jul 23, 2025.
64. DANAHER, Brett; SMITH, Michael D.; TELANG, Rahul, The Effect of Piracy Website Blocking on Consumer Behavior. 2019. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612063. Accessed on: Jul 23, 2025.
65. UNIÃO EUROPEIA (UE). Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019. Strasbourg, 2019. Available at: <https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng>. Accessed on: Jul 16, 2025.
66. HOMANN, Jochen. Online Copyright Clearance System arranges block of streaming site. Bonn: Bundesnetzagentur, Mar 11, 2021. Available at: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2021/20210311_Clearingstelle.html. Accessed on: Jul 23, 2025.

67. SATORI THREAT INTELLIGENCE AND RESEARCH TEAM, 2025.
68. FINLÂNDIA. Copyright Act (Act No. 404/1961 of July 8, 1961, as amended up to Act No. 608/2015 of May 22, 2015). 2015. Available at: <https://www.wipo.int/wipolex/en/legislation/details/15992>. Accessed on: Jul 23, 2025.
69. UE, 2019.
70. https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_13.pdf
71. AUSTRÁLIA. Copyright Amendment (Online Infringement) Act 2015. Canberra, 2015. Available at: <https://www.legislation.gov.au/C2015A00080/latest/text>. Accessed on: Jul 23, 2025.
72. MOTION PICTURE ASSOCIATION (MPA). Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior: December 2018. 2020. Available at: <https://www.mpa-apac.org/wp-content/uploads/2020/02/Australia-Site-Blocking-Summary-January-2020.pdf>. Accessed on: Jul 23, 2025.
73. MPA, 2020.
74. UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES (UIT). LS on the agreement of Technical Report ITU-T QSTR-MCM-UC "Use Cases on the combat of Multimedia Content Misappropriation". 2024. Available at: <https://www.itu.int/md/T22-SG16-240415-TD-GEN-0295/en>. Accessed on: Jul 23, 2025.
75. UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES (UIT). Output - Updated text of the draft Recommendation ITU-T Q.FC-MCM: Framework for combating Multimedia Content Misappropriation. Genebra, 2024. Available at: <https://www.itu.int/md/T22-SG11-240501-TD-GEN-0993/en>. Accessed on: Jul 23, 2025.

ANTI-PIRACY WHITE PAPER

HISTORY, INTERNATIONAL BENCHMARK, RESULTS
OBTAINED AND CHALLENGES FACED