



White Paper Combate a la Piratería

HISTÓRICO, BENCHMARK INTERNACIONAL,
RESULTADOS OBTENIDOS Y DESAFÍOS
ENFRENTADOS

Agencia Nacional de Telecomunicaciones

SAUS Manzana 06, Bloques C, E, F y H

CEP 70.070-940 - Brasília/DF

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

Presidente

Carlos Manuel Baigorri

Consejo Directivo

Vicente Bandeira de Aquino Neto

Alexandre Reis Siqueira Freire

Octavio Penna Pieranti

Edson Holanda

Superintendencias

Daniel Martins D'Albuquerque – Superintendencia de Administración y Finanzas (SAF)

José Borges da Silva Neto – Superintendente de Competencia (SCP)

Suzana Silva Rodrigues – Superintendente de Control de Obligaciones (SCO)

Gesilêa Fonseca Teles – Superintendente de Fiscalización (SFI)

Gustavo Nery e Silva – Superintendente de Gestión Interna de la Información (SGI)

Vinícius Oliveira Caram Guimarães – Superintendente de Otorgamiento y Recursos para la Prestación (SOR)

Nilo Pasquali – Superintendente de Planificación y Reglamentación (SPR)

Cristiana Camarate Silveira Martins Leão Quinalia – Superintendente de Relaciones con los Consumidores (SRC)

Gustavo Santana Borges – Superintendente Ejecutivo (SUE)

Asesorías y órganos vinculados

Daniel Leite Santos França – Jefe de la Asesoría Parlamentaria y de Comunicación Social

Andrea Mamprim Grippa – Jefe de la Asesoría Internacional (AIN)

Maria Lúcia Valadares e Silva – Jefe de la Asesoría de Relaciones con los Usuarios (ARU)

Dagma Sebastiana Caixeta de Macedo – Jefe de la Asesoría de Relaciones Institucionales (ARI)

João Marcelo Azevedo Marques Mello da Silva – Jefe de la Asesoría Técnica (ATC)

André Garcia Pena – Jefe de la Auditoría Interna (AUD)

Silvio Andrade dos Santos – Corregidor (CRG)

Felipe Augusto Esmeraldo de Oliveira – Defensor del Usuario



AGENCIA NACIONAL DE TELECOMUNICACIONES

White Paper Combate a la Piratería:

HISTÓRICO, BENCHMARK
INTERNACIONAL, RESULTADOS OBTENIDOS Y DESAFÍOS
ENFRENTADOS

Coordinador

Alexandre Reis Siqueira Freire

BRASÍLIA-DF

2025



Equipo de investigación

Coordinación

Alexandre Reis Siqueira Freire

Autores

Gabinete del Consejero Director Alexandre Freire

Alexandre Reis Siqueira Freire

Ailfran Moraes Martins

Leonardo Albuquerque Marques

Superintendencia de Fiscalización

Gesiléa 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

Superintendente de Fiscalización

Gesiléa Fonseca Teles

Superintendencia de Otorgamiento y Recursos para la Prestación

Geraldo Magela Benício Junior

Catalogación en la fuente – Biblioteca de Anatel

W582 White paper combate a la piratería: histórico, benchmark internacional, resultados obtenidos y desafíos enfrentados [recurso electrónico] / coordinador: Alexandre Reis Siqueira Freire – Brasília : Anatel, 2025.

1 recurso *online* [106 p.] : il.

Modo de acceso: World Wide Web.
Publicación digital (e-book) en formato PDF.

Varios autores.

1. Piratería. 2. Producto de telecomunicaciones 3. Certificación de productos. 4. Homologación de productos. 5. Sector de telecomunicaciones 6. Regulación gubernamental I. Agencia Nacional de

Ficha catalográfica elaborada por Carolina Pereira Marinho – CRB1/2275

Como citar este libro: FREIRE, Alexandre Reis Siqueira (coord.). White paper combate a la piratería : histórico, benchmark internacional, resultados obtenidos y desafíos enfrentados. Brasília: Anatel, 2025. e-Book. (1 recurso en línea (106 p.)), il.	Agencia Nacional de Telecomunicações SAUS, Manzana 6, Bloque C, E, F y H Código Postal: 70.070-940 – Brasília/DF Tel.: (61) 2312-2000 Sitio web: www.gov.br/anatel
---	--

INDICE

PRESENTACIÓN	5
INTRODUCCIÓN	7
1. VISIÓN GENERAL DE LA PIRATERÍA EN EL SECTOR DE TELECOMUNICACIONES EN BRASIL	10
1.1. Sistema de Evaluación de la Conformidad	11
1.2. Evaluación de la Conformidad (Base Regulatoria)	12
1.3. El modelo de certificación de Anatel	16
1.4. La actuación fiscalizadora de Anatel	23
1.5. El crecimiento del mercado y la piratería en el contexto de las telecomunicaciones	24
1.6. Riesgos Físicos y Digitales a los Usuarios	25
2. Acciones de Combate a la Piratería y sus Reacciones	36
2.1. PACP – Plan de Acción de Combate a la Piratería	36
2.2. Combate a la Piratería en <i>Marketplaces</i>	43
2.3. Alianzas con los organismos de la administración pública	47
2.4. Evolución del entendimiento jurídico (<i>marketplace</i> , redes sociales y cadena de distribución)	53
2.4.1. RESPONSABILIZACIÓN DE LOS MARKETPLACES	53
2.4.2. RESPONSABILIZACIÓN DE LAS REDES SOCIALES (YOUTUBE Y FACEBOOK)	61
2.4.3. RESPONSABILIZACIÓN DE LA CADENA DE DISTRIBUCIÓN DE PRODUCTOS	62
2.5. Plan de Combate al Uso de Decodificadores Clandestinos	70
3. ACCIONES DE COMBATE A LA PIRATERÍA EN OTRAS ADMINISTRACIONES	77
3.1. Combate a la piratería en <i>e-commerce</i>	77
3.2. Combate al uso de equipos no homologados	80
3.3. Combate a la conexión de equipos no homologados y al acceso a contenido	84
3.4. Alianzas multilaterales y Foro Global	91
4. Desafíos y Oportunidades Futuras	93
4.1. Principales Desafíos	93
4.2. Oportunidades Futuras	94
REFERENCIAS	97

PRESENTACIÓN

Los servicios de telecomunicaciones constituyen uno de los pilares del desarrollo económico y social de Brasil. Su utilización, tanto en la experiencia cotidiana de los consumidores sea en la prestación realizada por las empresas que componen el sector, debe garantizar la protección de los derechos fundamentales de los usuarios, el equilibrio de la competencia y el cumplimiento estricto de la legislación. En este sentido, el combate a la piratería de productos y servicios de telecomunicaciones ocupa una posición estratégica en la actuación de Anatel, no solo como una medida de represión de ilícitos, sino como una acción esencial para la preservación de la calidad, la seguridad y la integridad de las redes nacionales.

Este White Paper presenta, de manera amplia y fundamentada, el conjunto de iniciativas emprendidas por la Agencia para enfrentar este desafío. El documento reúne datos técnicos, análisis jurídicos, estadísticas actualizadas y descripciones detalladas de estrategias operativas, al tiempo que evidencia los resultados ya alcanzados mediante operaciones de fiscalización, incautaciones de dispositivos irregulares, bloqueos tecnológicos y medidas regulatorias que refuerzan la protección del sector. Se trata, por tanto, de un informe institucional que combina rigor técnico con una visión estratégica de futuro.

La piratería, más que un problema puntual, constituye una amenaza sistémica. Sus impactos se extienden desde la degradación de la calidad de los servicios hasta el perjuicio a la libre competencia, perjudicando a empresas que actúan dentro de la legalidad y desincentivando nuevas inversiones. Además, los productos y servicios irregulares exponen a los usuarios a riesgos crecientes de ciberseguridad, abriendo espacio para prácticas delictivas sofisticadas y poniendo en jaque la confianza en el ecosistema digital. El combate a tales prácticas, por lo tanto, es condición indispensable para la construcción de un entorno competitivo, innovador y seguro.

Para dar efectividad a esta misión, Anatel ha actuado de manera articulada con organismos gubernamentales, entidades del sector privado y la sociedad civil, reconociendo que solo la acción coordinada de todos los actores permitirá resultados duraderos. Esta cooperación fortalece tanto los mecanismos de prevención como los instrumentos de represión, amplía la concientización de la población y fomenta soluciones conjuntas de carácter estructural.

Los avances ya alcanzados demuestran la relevancia de esta estrategia. Las operaciones realizadas evidencian no solo la eficacia de los instrumentos de fiscalización, sino también la capacidad de la Agencia para innovar en la aplicación de medidas regulatorias que elevan el nivel de confiabilidad del sector. Sin embargo, la dinámica del mercado y la velocidad de la transformación tecnológica imponen nuevos desafíos, como el crecimiento exponencial de la Internet de las Cosas, la sofisticación de las prácticas de ciberdelincuencia y la necesidad de intensificar la cooperación internacional para contener un fenómeno que trasciende fronteras.

Así, este White Paper no se limita a presentar las acciones ya realizadas, sino que busca reafirmar el compromiso de Anatel con la transparencia, la responsabilidad institucional y la defensa del interés público. Al invitar a los lectores a explorar su contenido, la Agencia refuerza su determinación de liderar la construcción de soluciones integradas y sostenibles para el combate efectivo a la piratería. Más que un documento técnico, se trata de una manifestación de compromiso con el futuro de las telecomunicaciones en Brasil: un futuro que debe estar marcado por la calidad, la seguridad, la innovación y la confianza mutua entre la sociedad, el sector productivo y el poder público.



Carlos Baigorri
Presidente da Anatel



Alexandre Freire
Conselheiro Diretor da Anatel

INTRODUCCIÓN

Las redes de telecomunicaciones están compuestas por un conjunto de equipos que permiten la prestación de servicios de comunicación a distancia, tales como los transceptores (de radiocomunicación, como, por ejemplo, el teléfono móvil, de uso del consumidor, y las Estaciones Radio Base – ERB, de uso de las operadoras) y sus periféricos (antenas, cargadores, baterías, etc.), que utilizan recursos públicos escasos (espectro de radiofrecuencias y órbita), además de los dispositivos que permiten que la información circule por medios confinados (cables de cobre, cables coaxiales, cables de fibra óptica, etc.).

El concepto de telecomunicación puede extraerse del Art. 60, § 1º, de la Ley Nº 9.472, del 19 de julio de 1997 — Ley General de Telecomunicaciones (LGT):

Art. 60. (...)

§ 1º Telecomunicación es la transmisión, emisión o recepción, por hilo, radioelectricidad, medios ópticos o cualquier otro proceso electromagnético, de símbolos, caracteres, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza.

Estos equipos deben respaldar la prestación del servicio de telecomunicaciones bajo estándares mínimos de calidad y seguridad, garantizando la protección del consumidor, tanto física como cibernética, y observando la legislación brasileña e internacional aplicable, especialmente en lo relativo al uso regular del espectro de radiofrecuencias.

Todo este conjunto de obligaciones, que deriva de las disposiciones de la LGT, se asegura mediante normas regulatorias, entre las cuales se destacan aquellas sobre certificación/homologación de equipos, que representan un instrumento de gestión de las redes de telecomunicaciones, a partir del establecimiento de parámetros básicos para la utilización y conexión de equipos de telecomunicaciones a las redes, además de la garantía de procedencia, soporte técnico y responsabilidad jurídica de los fabricantes.

En el desempeño de su misión institucional, Anatel viene adoptando una serie de medidas orientadas a la identificación, prevención y represión de prácticas ilícitas asociadas a la utilización de productos no homologados y al uso indebido de las redes de telecomunicaciones. Tales acciones incluyen operaciones de fiscalización cuyo objetivo es retirar del mercado productos irregulares y bloquear dispositivos clandestinos, campañas de concientización de la población y la articulación con otros organismos públicos, como la *Secretaría de Ingresos Federales* y el Ministerio de Justicia y Seguridad Pública, además de asociaciones con el sector privado.



La actuación de Anatel en el combate a la piratería se basa en el marco legal y regulatorio vigente, que exige la certificación de productos de telecomunicaciones, cohibe el uso indebido del espectro y la explotación no autorizada de servicios. Sin embargo, los avances tecnológicos, la globalización —especialmente del comercio electrónico— y la complejidad de las cadenas ilícitas de distribución y uso de las redes imponen la necesidad de un enfoque más estratégico, cooperativo y basado en evidencias.

Este *White Paper* presenta las bases técnicas, administrativas y jurídicas de la certificación y homologación de productos de telecomunicaciones, así como un análisis de las iniciativas de Anatel contra la piratería. Ofrece una visión amplia del problema, de los mecanismos de

actuación, de los resultados obtenidos y de los caminos para mejorar las políticas públicas en el sector.

Reuniendo datos, estudios de caso, experiencias prácticas y fundamentos normativos, el documento busca apoyar a los tomadores de decisiones, agentes regulados, investigadores y demás interesados en el enfrentamiento de la piratería, en favor de un ecosistema digital más seguro, confiable y justo para todos los brasileños.

1. VISIÓN GENERAL DE LA PIRATERÍA EN EL SECTOR DE TELECOMUNICACIONES EN BRASIL

Anatel, conforme los Arts. 19, XII y XIII, y 162, §2º, de la LGT, tiene competencia para certificar o reconocer productos para telecomunicaciones, estando prohibido el uso de equipos emisores de radiofrecuencia sin dicha certificación. Según el Art. 1º, párrafo único, de la LGT, su actuación abarca el disciplinamiento y la fiscalización de las redes, del espectro de radiofrecuencias y de los recursos de órbita.

Sin las reglas de evaluación de la conformidad y de homologación de estos productos, no hay garantía de seguridad, calidad o compatibilidad de los equipos— pudiendo producirse interferencias en los servicios, riesgos eléctricos, explosiones de baterías, exposición excesiva a radiaciones no ionizantes y vulnerabilidades a la seguridad cibernética.

La evaluación de la conformidad y la homologación de productos para telecomunicaciones garantizan seguridad jurídica y protección al consumidor, asegurando la responsabilización de los proveedores y la protección de la parte más vulnerable— el consumidor brasileño. Anatel evalúa estas condiciones antes de la liberación de los productos al mercado, prohibiendo la comercialización de equipos que no cumplan con los requisitos de seguridad.

Antes de abordar el comercio ilegal, es necesario comprender el Sistema Brasileño de Evaluación de la Conformidad de Productos para Telecomunicaciones.



1.1. Sistema de Evaluación de la Conformidad

El sistema de evaluación de la conformidad es un proceso sistematizado, con reglas preestablecidas, debidamente acompañado y evaluado, de manera a proporcionar un grado adecuado de confianza de que un producto, proceso o servicio, o incluso un profesional, cumple con los requisitos establecidos en normas o reglamentos. Conforme la norma ISO/IEC 17000, de la Organización Internacional de Normalización, se trata de la actividad que permite demostrar que se cumplen requisitos específicos relativos a productos, procesos, servicios, sistemas, personas u organizaciones.

Los modelos de evaluación de la conformidad mediante certificación, previstos en el Reglamento de Evaluación de la Conformidad y Homologación de Productos para Telecomunicaciones, se basan en los tipos de esquemas de certificación descritos en la norma ISO/IEC 17067, que presenta los fundamentos para la certificación de productos, procesos o servicios y proporciona directrices para programas/esquemas de certificación.

Los sistemas de gestión de los organismos de certificación de productos para telecomunicaciones deben tener como referencia la norma ISO/IEC 17065, que define los requisitos para los organismos de certificación de productos, procesos y servicios, así como

para los laboratorios de ensayos y calibración.

Por último, los requisitos técnicos definidos por las regulaciones de Anatel siguen referencias normativas establecidas por organismos internacionales de estandarización, como UIT, 3GPP, IEEE, IEC, entre otros.

Así, el proceso de evaluación de la conformidad de productos para telecomunicaciones se desarrolla con base en normas internacionales, garantizando una alineación con los estándares adoptados mundialmente, de modo que se asegure el nivel adecuado de confiabilidad en sus resultados.

1.2. Evaluación de la Conformidad (Base Regulatoria)

La disciplina legal para impedir la comercialización de productos no homologados por Anatel se fundamenta, esencialmente, en los siguientes preceptos de la LGT:

Art. 19. A la Agencia le compete (...)

XIII – expedir o reconocer la certificación de productos, observados los estándares y normas por ella establecidos;

Art. 156. (...)

§ 2º La certificación es el reconocimiento de la compatibilidad de las especificaciones de determinado producto con las características técnicas del servicio al cual se destina.

Art. 162. (...)

§ 2º Se prohíbe la utilización de equipos emisores de radiofrecuencias sin certificación expedida o aceptada por la Agencia.

El Reglamento de Evaluación de la Conformidad y Homologación de Productos para Telecomunicaciones, aprobado por la Resolución Anatel nº 715, de 23 de octubre de 2019, y actualizado por la Resolución Anatel nº 780, de 1 de agosto de 2025, detalla estos preceptos:

Art. 55. La homologación es un requisito previo obligatorio para la utilización y comercialización, en el país, de los productos abarcados por este Reglamento.

Art. 63. Los productos homologados deben contener la identificación de la homologación, conforme el procedimiento operativo.

Art. 83. Son conductas susceptibles de sanción, observada la legislación y la regulación específica:

I – uso o empleo de producto no homologado; (...)

IV – comercialización de producto no homologado; (...)

IX – divulgación de código de homologación inválido o perteneciente a otro equipo en anuncio de producto no homologado;

X – importación de producto no homologado.

Adicionalmente, resulta importante destacar la lógica de actuación de la Agencia frente a la comercialización de productos no homologados.

La LGT y el diseño normativo infralegal formulado por el órgano regulador para la evaluación de la conformidad de productos para telecomunicaciones son producto del nuevo modelo de actuación estatal en el sector de infraestructura consolidado en Brasil en la década de 1990, en el que el Estado pasó de ser productor a regulador.

Bajo este nuevo modelo de actuación estatal, que en el sector de telecomunicaciones fue impulsado por la Enmienda Constitucional nº 8/1995, la cual rompió el monopolio estatal sobre los servicios de telecomunicaciones y previó la creación de un órgano regulador sectorial, dotado de capacidad técnica y poderes normativos infralegales, se configuró, con los contornos establecidos por la LGT, una estructura legal que definió la forma de organización de la explotación de los servicios de telecomunicaciones en Brasil.

Entre las normas que determinan la implantación y funcionamiento de las redes, el Art. 156 de la LGT previó la certificación de productos como un instrumento de gestión de las redes

de telecomunicaciones, estableciendo que la conexión¹ podrá ser prohibida para equipos sin certificación expedida o aceptada por la Agencia. El párrafo segundo de este artículo define la certificación como el reconocimiento de la compatibilidad de las especificaciones de determinado producto con las características técnicas del servicio de telecomunicaciones al cual se destina.

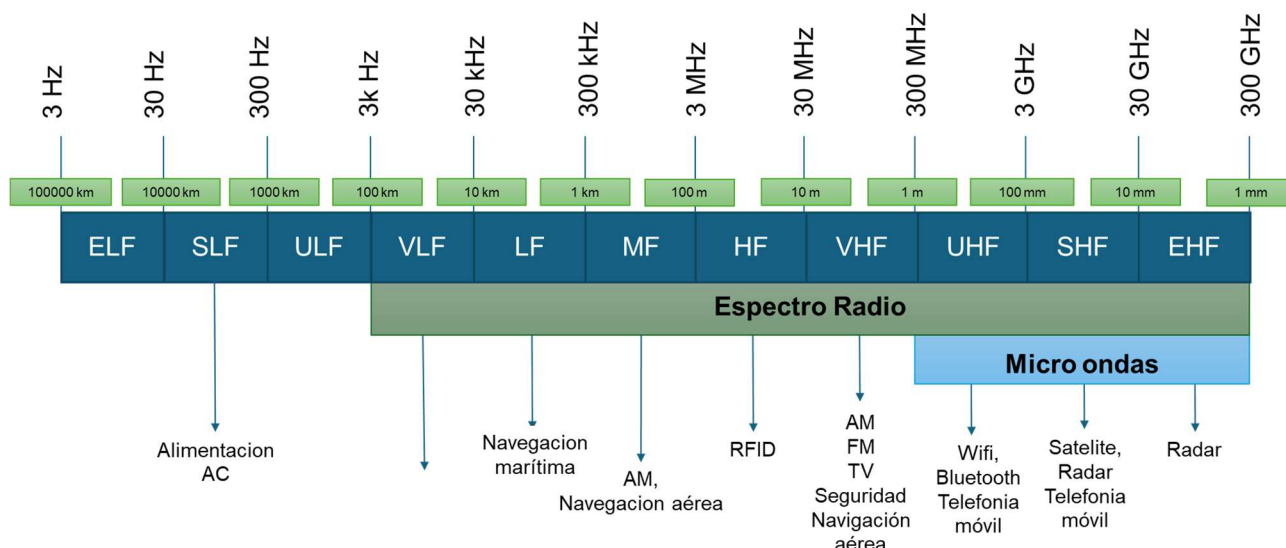
Las redes de telecomunicaciones deben organizarse como vías integradas de libre circulación, en las que es obligatoria la interconexión entre las redes de los diversos prestadores, así como la operación integrada a nivel nacional e internacional, siendo el derecho de propiedad sobre las redes condicionado al deber de cumplimiento de su función social.

Los requisitos de certificación, como se desprende de su propia definición, son responsables de determinar los parámetros de funcionamiento de los equipos utilizados en las redes de telecomunicaciones. Este proceso posee una doble función: la primera, definir parámetros de confiabilidad de los equipos utilizados en las redes de telecomunicaciones nacionales, posibilitando el disfrute de la información con calidad y seguridad, según el estado del arte del desarrollo tecnológico a nivel mundial; y la segunda, la protección del consumidor local respecto a la seguridad y confiabilidad de los equipos.

La certificación es especialmente importante para la gestión del espectro de radiofrecuencias, bien público finito, administrado por Anatel. En la etapa actual de desarrollo de las telecomunicaciones, se observa que la masificación de los servicios se ve favorecida por las redes inalámbricas, y es a través del cumplimiento de los requisitos de certificación de productos (así como de las licencias de operación de estaciones) que se

¹ En el argot técnico, la conexión o interconexión es el enlace del terminal o red del usuario con las redes públicas de telecomunicaciones. Disponible en: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2018/1142-resolucao-693>. Acceso en: 07 jul. 2025.

hacen respetar las normas de uso del espectro y, por consiguiente, del tráfico de información en las redes de telecomunicaciones.



Así, un producto, para ser homologado por Anatel y, consecuentemente, ser compatible con el servicio de telecomunicaciones al que se destina, debe ser seguro para el consumidor (según el estado del arte del desarrollo tecnológico), actual (operar conforme la tecnología adecuada al momento de la homologación) y respetar la regulación brasileña de telecomunicaciones (como las condiciones de uso del espectro de radiofrecuencias).

Si, para el funcionamiento de las redes, la Ley determina que pueden ser prohibidas las conexiones de equipos terminales sin certificación (Art. 156, *caput*, de la LGT), cuando se trata de la utilización del espectro radioeléctrico, la certificación es obligatoria y condición *sine qua non* para el uso del producto. Así, el Art. 162, § 2º, de la LGT prohíbe la utilización de equipos emisores de radiofrecuencias sin certificación expedida o aceptada por la Agencia.

No es casualidad que la LGT, al reconocer la certificación como un instrumento importante de gestión de las redes, haya atribuido a Anatel la competencia para expedir normas y

A partir de la competencia legal determinada por el Art. 19, XIII, de la LGT, Anatel emitió sus resoluciones estableciendo el modelo brasileño de evaluación de la conformidad de productos para telecomunicaciones, formando excepción a la competencia del Instituto Nacional de Metrología, Calidad y Tecnología – Inmetro, como órgano de metrología para los diversos sectores de la economía nacional.

1.3. El modelo de certificación de Anatel

Inicialmente, es importante señalar que el proceso de certificación de equipos en Brasil comenzó con el Estado ya a finales de la década de 1940. Desde entonces, la preocupación central fue asegurar el seguimiento y control de los equipos utilizados en el país, así como su sometimiento a pruebas y evaluaciones. Tal rigor tenía como objetivo comprobar el cumplimiento de las especificaciones técnicas de los servicios que se iban a ofrecer.

En los años siguientes, con la evolución de los sistemas de telecomunicaciones, el proceso de certificación de equipos se perfeccionó. Es relevante destacar que, antes de la creación de Anatel, la Norma General de Telecomunicaciones nº 004/91 (NGT 004/91), aprobada por la Portaria nº 173, de 21 de agosto de 1991, del Ministerio de Infraestructura, fue la primera en establecer reglas y procedimientos sistematizados relativos a la certificación de productos para telecomunicaciones en Brasil. El escenario era muy diferente, ya que el Estado era el proveedor de servicios de telecomunicaciones, limitado a la telefonía fija. Con la evolución de las telecomunicaciones, el Estado pasa de ser proveedor a regulador, frente al creciente aumento de productos sujetos a certificación en un mercado abierto y competitivo.

Período	Tecnología Predominante	Tipos de Dispositivos	Volume Relativo	Impacto Regulatorio
1980s	Telefonia fija	Teléfono	Bajo	Monopólio Estatal
1990s	Internet discada	PCs, modems	Medio	Certificación de terminales analógicos
2000s	Banda ancha	Modems, roteadores, STBs	Alto	Certificación multiprotocolo
2010s	3G/4G	Smartphones, tablets	Muy alto	Ampliación de la certificación RF
2020s	5G / IoT	Dispositivos inteligentes, automatización	Masivo	Atualización normativa y seguridad digital

El modelo de certificación actualmente vigente, considerando los deberes y competencias de la Anatel relativos al tema, fue implementado inicialmente por las Resoluciones nº 242, del 30 de noviembre de 2000, y nº 323, del 7 de noviembre de 2002, las cuales fueron sucedidas por la Resolución nº 715, del 23 de octubre de 2019, y por la Resolución nº 780, del 1º de agosto de 2025 (que las actualizó y complementó), aprobando el Reglamento de Evaluación de la Conformidad y de Homologación de Productos para Telecomunicaciones. Dicho Reglamento normatiza todo el proceso de certificación en el ámbito de la Anatel y está respaldado por reglas técnicas secundarias, denominadas procedimientos operativos y requisitos técnicos, que detallan la forma y los parámetros necesarios para la homologación de un producto.

En el referido Reglamento (aprobado por la Resolución nº 715/2019), se identifica un proceso bifásico que culmina en la homologación de un producto.

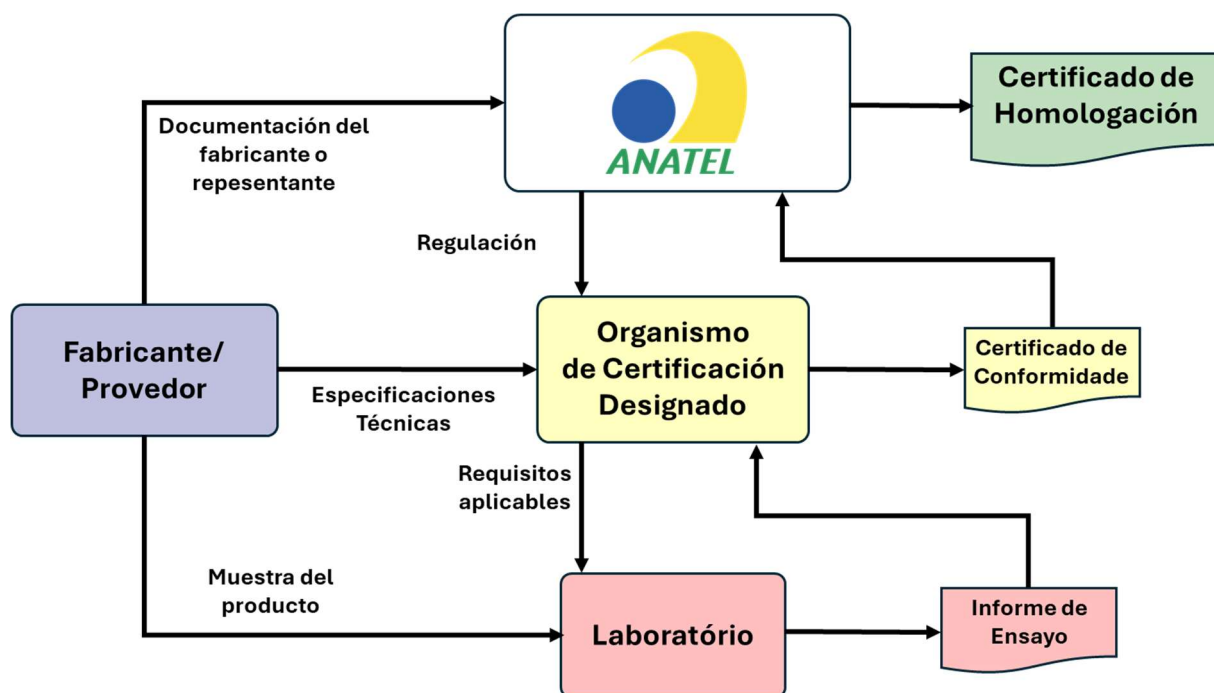
La primera fase es la evaluación de la conformidad del producto, en la cual actúan agentes externos a la Anatel. O la evaluación de la conformidad se realiza por declaración de conformidad (DC, prevista en el Art. 29, I y II, del Reglamento), en la que el propio interesado certifica la conformidad del producto, situación excepcional en el modelo brasileño

(generalmente aplicable a productos artesanales o importados para uso propio, véase Art. 33 del Reglamento); o bien la evaluación de la conformidad puede realizarse mediante certificación de conformidad técnica (CCT, prevista en el Art. 29, III a V, del Reglamento), en la que toda la operación se lleva a cabo a través de un contrato de prestación de servicios que involucra a un Organismo de Certificación Designado (OCD, responsable de la conducción del proceso de certificación, véase Art. 36), un laboratorio de ensayos habilitado (elegido por el solicitante de la homologación, véase Art. 18) y el interesado en la homologación. Cabe destacar que tanto los OCD como los laboratorios habilitados son personas jurídicas de derecho privado que actúan, por lo general, en la certificación de productos para diversos sectores de la economía (muchos de ellos acreditados por el Inmetro). La certificación de conformidad técnica es aplicable a productos destinados a la comercialización, como los teléfonos móviles (véase Art. 32 del Reglamento). Por lo tanto, esta etapa suele involucrar análisis técnicos y de laboratorio realizados por un OCD y por un laboratorio de ensayos habilitado, con capacidad técnica reconocida por la Anatel, para analizar el alcance del producto. El resultado de esta etapa es la expedición del Certificado de Conformidad Técnica (CCT), condición indispensable para la homologación del producto.

La segunda fase consiste en el análisis realizado por la Anatel, que ocurre en el ámbito interno de la Agencia, sobre el cumplimiento de los criterios objetivos (adecuación de la expedición del CCT a las reglas previamente emitidas por la Anatel) y subjetivos (relativos a la legitimidad de la solicitud de homologación y a la capacidad del interesado para responsabilizarse por el producto en el país), lo cual culmina en la autorización estatal para el uso y la comercialización del producto de telecomunicaciones en Brasil. El resultado de esta etapa es el Certificado de Homologación.

La homologación del CCT es un requisito previo para el uso y la comercialización de un producto para telecomunicaciones en el país. La extensión de los derechos derivados de dicha homologación (es decir, derecho únicamente de uso del producto o derecho de uso y

comercialización) depende del tipo de evaluación de la conformidad que haya sido empleada, conforme a los Arts. 55 y 64 del Reglamento aprobado por la Resolución nº 715/2019.



Los Arts. 32 y 33 del Reglamento citado definen en qué condición debe realizarse preferentemente la evaluación de la conformidad (mediante certificación de conformidad o mediante declaración de conformidad). Y, en virtud del Art. 31, la definición de los modelos disponibles para la evaluación de la conformidad de productos para telecomunicaciones debe considerar la aplicación, la complejidad del equipo y el riesgo potencial de su utilización para el usuario.

Para cada familia de productos para telecomunicaciones (p. ej., estaciones terminales de acceso, cables ópticos, antenas, etc.), la Anatel establece un conjunto de requisitos técnicos y define una modalidad de evaluación de la conformidad, que puede ser más o menos interventiva, dependiendo de la relevancia del producto en el escenario de las telecomunicaciones (para el usuario, para los servicios de telecomunicaciones, para las redes, para la política nacional de telecomunicaciones, etc.).

En el ámbito de sus competencias, y considerando lo dispuesto en el Art. 55, § 1º, actualizado por la Resolución nº 780/2025, la Anatel ya había emitido el Resolución nº 4.521, del 21 de junio de 2021, que aprobó el procedimiento operativo para la importación de productos para telecomunicaciones. Este procedimiento establece condiciones para la importación de productos de homologación obligatoria, ya sea para uso propio, comercialización, evaluación de la conformidad de muestras o demostración.

Desde la perspectiva del consumidor, también son relevantes las normas sobre la identificación de la homologación. Los productos homologados deben contener la identificación de la homologación, conforme lo establecido en el procedimiento operativo correspondiente. Existen dos tipos de marcación exigidos por la regulación sectorial: la primera se refiere a la identificación de la homologación de Anatel, y la segunda se refiere al sello de seguridad de homologación para baterías de litio y cargadores.

En lo que concierne a la identificación de la homologación, se publicó el Resolución nº 4.088, del 31 de julio de 2020, que aprobó el procedimiento operativo para la marcación de la identificación de la homologación Anatel en productos para telecomunicaciones, y que define el Código de Homologación (composición de 12 (doce) dígitos que identifica cada producto homologado), la Logomarca Anatel, la Firma Anatel (expresión “Agencia Nacional de Telecomunicaciones”) y el Sello Anatel (formado por la Logomarca Anatel y el código numérico de homologación, acompañado o no de la Firma Anatel). La responsabilidad por la identificación es del fabricante nacional del producto para telecomunicaciones, independientemente de la ubicación de las unidades fabriles; en el representante legal del fabricante, en el caso de producto importado; y en el usuario, en el caso de producto importado directamente para uso propio o en el caso de productos artesanales sin fines comerciales, por ejemplo.

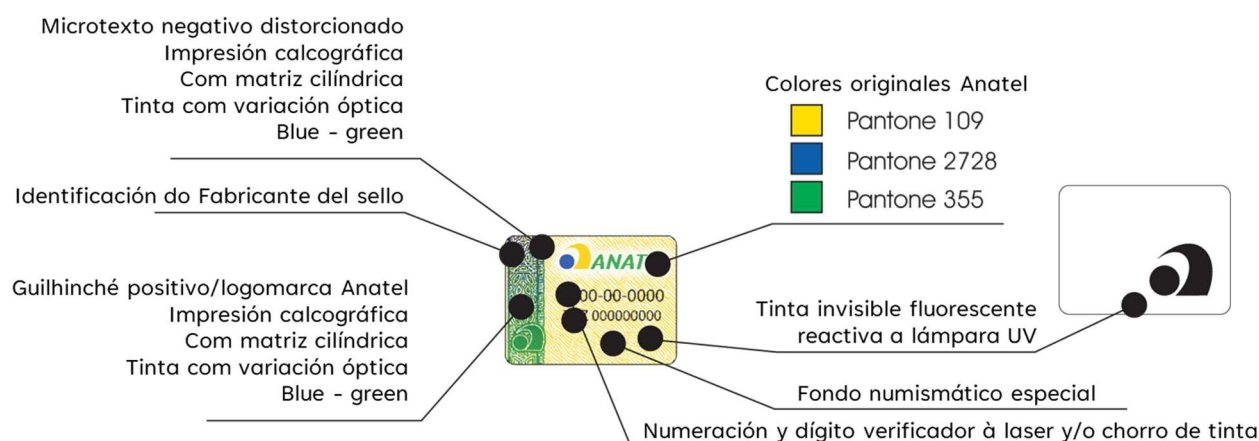


EJEMPLOS DE SELLO ANATEL



Fuente: Anatel

El sello de seguridad consiste en la forma de identificación de la homologación destinada a productos específicos definidos por la Agencia, los cuales cuentan con un sistema de control y trazabilidad de la producción que permite la protección contra la falsificación, el desvío, el contrabando, las alteraciones o las duplicaciones indebidas del Sello Anatel mediante el monitoreo de la cadena productiva. Este asunto está regulado en el procedimiento operativo aprobado por el Resolución nº 14.010, del 4 de octubre de 2022, y se aplica a los interesados en la comercialización de baterías de litio y cargadores para teléfonos móviles, así como a las empresas gráficas debidamente habilitadas para el suministro del sello de seguridad, en el ejercicio de sus funciones como agentes del proceso de evaluación de la conformidad de productos para telecomunicaciones.



Dada su complejidad, la estructura que conduce a la homologación de un producto de telecomunicaciones no es accesible para el consumidor común, lo que exige del organismo regulador un esfuerzo adicional de concienciación sobre su importancia. Este hecho se refleja en el mercado y en los agentes económicos en general.

1.4. La actuación fiscalizadora de Anatel

La actuación de Anatel en el sector ha evolucionado significativamente hacia un modelo regulatorio más moderno, eficiente y responsivo. En este contexto, la Resolución nº 746/2021, que establece el Reglamento de Fiscalización Regulatoria, introduce un enfoque basado en la prevención, la inducción al cumplimiento voluntario y la priorización de riesgos, mientras que la Resolución nº 589/2012, que trata del Reglamento de Sanciones Administrativas, mantiene el marco jurídico necesario para la responsabilización y sanción de conductas infractoras. La interacción entre estos dos instrumentos normativos traduce una estrategia integrada que equilibra educación regulatoria y aplicación de sanciones, promoviendo tanto el cumplimiento espontáneo de las normas como la responsabilización efectiva cuando sea necesaria.

La Resolución nº 746/2021 reconoce que la fiscalización debe ir más allá de la simple represión, adoptando prácticas que incentiven comportamientos regulares por medio de acciones orientativas, campañas educativas y advertencias. Este enfoque busca dialogar con los regulados, identificar fragilidades y estimular correcciones antes de la adopción de medidas punitivas. La Resolución nº 589/2012 entra en escena cuando hay resistencia, reincidencia o gravedad en las infracciones, disciplinando la aplicación proporcional y motivada de sanciones, como advertencia formal, multa, suspensión o revocación de la concesión.

La correlación entre ambos reglamentos permite que Anatel actúe de forma gradual y responsiva, ajustando su intervención según el perfil del agente regulado y la naturaleza de la infracción. Agentes que demuestran buena fe y disposición para corregir conductas pueden ser tratados prioritariamente con medidas educativas. Por otro lado, conductas reiteradas, dolosas o que ocasionen perjuicio al orden público, a los consumidores o a la integridad del sector exigen una respuesta sancionadora firme y ejemplar.



Esta integración fortalece la función pedagógica de la regulación, promueve un ambiente de mayor seguridad jurídica, reduce la litigiosidad y estimula la construcción de una cultura regulatoria basada en el diálogo, la transparencia y la responsabilidad. Al combinar educación y sanción de manera estratégica, Anatel se posiciona como una agencia moderna, orientada no solo al control, sino también a la formación de un mercado más consciente, ético y comprometido con el interés público.

1.5. El crecimiento del mercado y la piratería en el contexto de las telecomunicaciones

En las últimas décadas, Brasil ha experimentado un crecimiento significativo en la demanda por servicios de telecomunicaciones, impulsado por la democratización del acceso a internet, la telefonía móvil y la distribución de contenido digital. Sin embargo, este avance tecnológico no fue acompañado, en muchos casos, por una ampliación de la educación digital ni de la conciencia sobre los riesgos asociados al uso de productos irregulares. Paralelamente, factores como la informalidad económica, la elevada carga tributaria sobre equipos electrónicos y la facilidad de acceso a plataformas internacionales de comercio línea han contribuido al surgimiento de un mercado paralelo robusto, con una amplia oferta de

equipos de telecomunicaciones no homologados, considerados productos piratas: sin seguridad y calidad comprobadas, sin confirmación de procedencia, sin soporte técnico al usuario y perjudiciales para la sostenibilidad económica del sector.

En este contexto, la actuación de Anatel se ha vuelto esencial, no solo para la protección del sector regulado, sino principalmente para garantizar la seguridad y el derecho de los consumidores a servicios de telecomunicaciones confiables y en conformidad con las normas técnicas y legales. La piratería compromete el funcionamiento adecuado de las redes, interfiere en los servicios de emergencia, perjudica la recaudación tributaria y fomenta prácticas ilícitas que generan riesgos técnicos y jurídicos para la sociedad.

1.6. Riesgos Físicos y Digitales a los Usuarios

El uso de equipos de telecomunicaciones no homologados representa un riesgo concreto para la seguridad física y digital de los usuarios. Los dispositivos no certificados pueden causar interferencias electromagnéticas perjudiciales, sobrecalentamiento, descargas eléctricas e incluso incendios, poniendo en riesgo la integridad física de los consumidores y de las redes. En el ámbito digital, los riesgos son igualmente preocupantes, dado que muchos de estos equipos vienen con *software* alterado, *backdoors* (método que permite eludir las medidas de seguridad habituales y obtener acceso privilegiado a un sistema, red o aplicación) y mecanismos que exponen a los usuarios a la interceptación de datos, al robo de información personal y a ataques cibernéticos (como aplicaciones maliciosas preinstaladas).

En el contexto de los servicios de telecomunicaciones, especialmente aquellos que utilizan el espectro radioeléctrico, los casos de interferencias perjudiciales provocadas por equipos no homologados son identificados por las operadoras a partir de reclamaciones de los usuarios o mediante el monitoreo de la calidad de las redes. En buena parte de los casos, cuando la Anatel es requerida, tras un exhaustivo trabajo de investigación de campo, es

común encontrar como causa de los problemas percibidos equipos de baja calidad o destinados a otros países, adquiridos en el comercio electrónico sin pasar por el proceso de certificación establecido por la Anatel².

Además del perjuicio a los servicios de telecomunicaciones, muchos dispositivos que utilizan radiofrecuencias son empleados en la práctica delictiva. Bandas asociadas al robo de cargas utilizan bloqueadores de señal, conocidos como *jammers*, para inutilizar los rastreadores y la comunicación del conductor mientras realizan la interceptación y la retirada de mercancías de alto valor³. Otra práctica delictiva se apropia de dispositivos electrónicos que utilizan radiofrecuencias para copiar los códigos de mandos a distancia de portones eléctricos o de llaves de vehículos. Uno de los objetivos es el robo en residencias⁴, o incluso el hurto de vehículos, lo que revela la vulnerabilidad de estos equipos⁵. Con el fin de inhibir la proliferación de este tipo de dispositivos, la Anatel incautó numerosos aparatos conocidos como "*Flipper Zero*", que fueron importados mediante comercio electrónico, lo que resultó en la notificación a los principales *marketplaces* del país para bloquear los anuncios de dichos productos⁶.

² BRAGA, Lucas; FAVRETTO, Everton. Anatel multa clínica veterinária por usar produto sem homologação. **Tecnoblog**, 23 feb. 2021. Actualizado el 14 nov. 2023. Disponible en: <https://tecnoblog.net/noticias/anatel-multa-clinica-veterinaria-por-usar-produto-sem-homologacao/>. Acceso el: 07 jul. 2025.

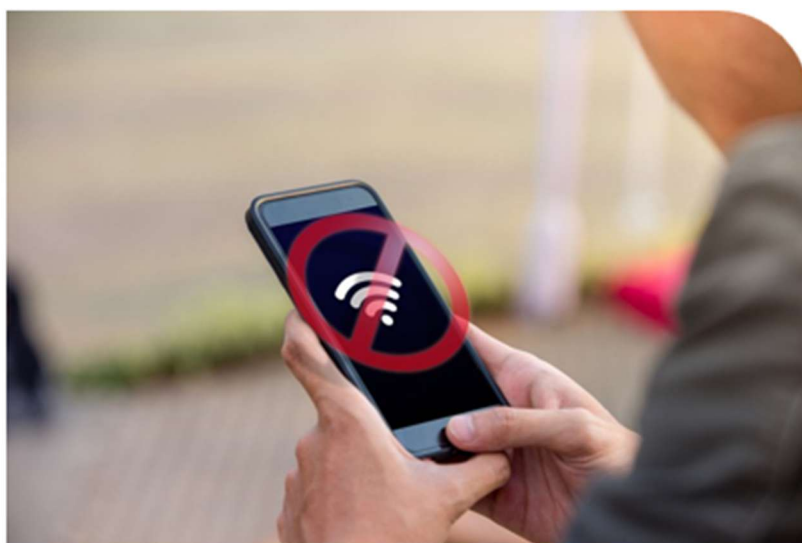
³ Polícia apreende bloqueador de sinal de GPS usado por quadrilha de roubos de cargas no Rio. **G1**, Río de Janeiro, 14 feb. 2019. Disponible en: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/02/14/policia-apreende-bloqueador-de-sinal-de-gps-usado-por-quadrilha-de-roubos-de-cargas-no-rio.ghtml>. Acceso el: 07 jul. 2025.

⁴ ALMEIDA, Esther. Dono de construtora morto em SP: saiba como evitar clonagem de controle de portão. **O Globo**, Río de Janeiro, 7 jun. 2025. Actualizado en 7 jul. 2025. Disponible en: <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>. Acceso el: 07 jul. 2025.

⁵ Bandidos em dupla já clonam chave a distância e levam carro em segundos. **UOL**, 5 oct. 2023. Disponible en: <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>. Acceso el: 7 ago. 2025.

⁶ AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL. **Anatel apresenta esclarecimentos sobre o Flipper Zero**. Brasília, 29 mar. 2023. Actualizado el 31 may. 2023. Disponible en: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-apresenta-esclarecimentos-sobre-o-flipper-zero>. Acceso el: 07 jul. 2025.

En el ámbito de la integridad física de los usuarios de productos de telecomunicaciones, en una investigación reciente realizada por la Agencia en internet, fue posible identificar una serie de incidentes ocasionados por el uso de productos de telecomunicaciones de baja calidad y no homologados.

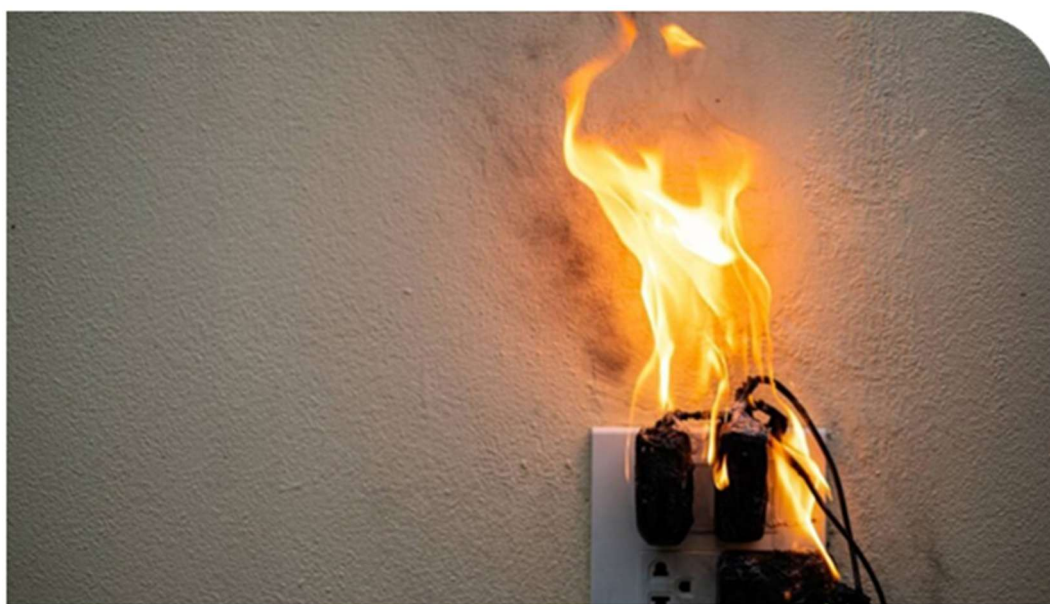


Fuente: portal GOV.br

Actualmente, los cargadores de baterías para dispositivos de telefonía móvil son, en su mayoría, productos importados y no homologados. Estos productos han sido asociados a diversos casos de accidentes, como descargas eléctricas o incendios. Las descargas eléctricas provocan lesiones y quemaduras. En los casos más graves, se han registrado fallecimientos. En caso de incendios, se registran pérdidas financieras significativas relacionadas con los propietarios de los dispositivos.

Merece especial atención el uso de cargadores de baterías para teléfonos móviles no homologados, ya que son utilizados y manipulados por toda la población, y los peligros asociados a su uso están más próximos a los usuarios. En el caso de los niños, el riesgo es aún mayor, pues estos productos pueden dejar expuestas partes metálicas energizadas debido a su baja calidad⁷

⁷ CINTRA, Caroline. "Perdi meu coração", diz mãe de garoto que morreu após choque em carregador. **Correio Braziliense**, Brasília, 12 ago. 2020. Actualizado el 12 ago. 2020. Disponible en: <https://www.correiobraziliense.com.br/cidades-df/2020/08/4868126--perdi-meu-coracao---diz-mae-de-garoto-que-morreu-apos-choque-em-carregador.html>. Acceso el: 07 jul. 2025.



Fuente: depositphotos.com/Chonthicha

Otro tipo de producto comúnmente utilizado por la población son las baterías para teléfonos móviles. Estas pueden provocar explosiones o fugas de elementos químicos que representan riesgos para la salud del consumidor. Existen relatos de explosiones de baterías en diversas situaciones⁸, ya sea durante el proceso de carga, mientras se utilizan junto con el aparato celular o durante su mantenimiento. Como resultado, se registran quemaduras y otras afecciones⁹.

En un reportaje publicado por el periódico *Correio Braziliense*, la *Associação Brasileira de Conscientização dos Perigos de Eletricidade* (Abracopel) verificó que cerca de 23 (veintitrés) personas fallecieron en el país, y un total de 41 (cuarenta y un) accidentes estuvieron relacionados con cargadores de baterías de teléfonos móviles.

⁸ VÍDEO: Incêndio em auditório pode ter sido provocado por carregador de celular, dizem bombeiros. **G1 Tocantins**, 08 ene. 2024 (actualizado em jul 2024). Disponible en: <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>. Acceso el: 07 jul. 2025.

⁹ DIOGO, Darcianne. Jovem sofre queimadura de 1º grau após celular explodir na tomada no DF. **Correio Braziliense**, Brasília, 14 may. 2023. Disponible en: <https://www.correiobraziliense.com.br/cidades-df/2023/05/5094486-jovem-sofre-queimadura-de-1-grau-apos-celular-explodir-na-tomada-no-df.html>. Acceso el: 07 jul. 2025.

El texto señala que los accidentes están asociados a un conjunto de factores, siendo el principal el uso de cargadores no originales, es decir, cargadores no homologados¹⁰.

Además de los casos presentados de graves riesgos para la salud de los consumidores que los productos de telecomunicaciones no homologados pueden ocasionar, son igualmente serios los daños que dichos productos pueden causar a la vida privada y a los bienes de las personas.

La atracción del contenido pirata está directamente vinculada a su amplia demanda por parte de los usuarios, que buscan acceso gratuito o facilitado a películas, series, deportes y canales de pago sin asumir los costos legales.

Este atractivo crea un entorno propicio para la proliferación de dispositivos adulterados, como TV boxes y otros equipos no certificados, que a menudo vienen preinstalados con aplicaciones ilegales.

En este contexto, los productos destinados a la recepción de señales de tele por cable o de vídeo bajo demanda no homologados pueden ocasionar violación de derechos de autor, ocultar códigos maliciosos y presentar vulnerabilidades de seguridad que permiten a piratas informáticos (*hackers*) acceder a los datos personales de los usuarios en dispositivos que compartan la misma red privada. Estudios de la Anatel, con el apoyo de la *Agência Nacional de Cinema* (Ancine) y de la *Associação Brasileira de Televisão por Assinatura* (ABTA), identificaron una relación directa entre determinada familia de equipos y *botnets* (red de computadoras o dispositivos conectados a internet infectados con *malware* —*software* malicioso— que son controlados de forma remota por un atacante con fines ilícitos), capaces

¹⁰ SILVA, Cristiane. Celulares já mataram 23 no Brasil: especialistas apontam principais vilões. **Correio Braziliense**, Brasília, 01 oct. 2019. Disponible en: https://www.correio braziliense.com.br/app/noticia/tecnologia/2019/10/01/interna_tecnologia,793061/celular-es-ja-mataram-23-no-brasil-especialistas-apontam-principais-vi.shtml. Acceso en: 07 jul. 2025.

de asumir el control de los *set-top boxes* (dispositivos que permiten el acceso a aplicaciones de vídeo, juegos u otros contenidos en línea a través de televisores convencionales) y realizar ataques DDoS (intento malicioso de hacer que un servicio en línea sea inaccesible mediante la sobrecarga de tráfico proveniente de múltiples fuentes)¹¹.

También se detectaron fallas de seguridad en el proceso de actualización de aplicaciones a través de tiendas virtuales propias, lo que permitía que toda la información intercambiada fuera capturada y modificada por un atacante malintencionado, posibilitando la instalación de aplicaciones maliciosas en el dispositivo.



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

¹¹ Cf. AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL (Brasil). Superintendencia de Fiscalización. **Informe n.º 4/2021/FIGF4/FIGF/SFI.** Brasília, 2021. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5PKr37An4NSs6sd1c9IPofluH3e-yRwywlgZFvUh-qW-f-MR8In0HwABi8MWbOkspZajukWXFCisvs8oBuJmvd. Acceso el: 23 jul. 2025.

Esta vulnerabilidad, asociada a otra en la cual el sistema operativo de los dispositivos permite que terceros tengan acceso irrestricto al aparato con privilegios de administrador (conocido como *root*)—, posibilita el control total de la TV Box, permitiendo el acceso a otros dispositivos que comparten la misma red, tales como computadoras, televisores, enrutadores, teléfonos móviles, *webcams*, entre otros, capturando datos e información de los usuarios, como registros financieros, contraseñas, archivos, fotos, etc.¹²

En el entorno de los sitios de piratería y de las aplicaciones de *streaming* (transmisión continua de datos que permite la reproducción del contenido en tiempo real sin necesidad de descarga), los consumidores se encuentran involuntariamente expuestos a una serie de amenazas cibernéticas.

- **Malware** – Una vez instalado en el dispositivo del consumidor, el *malware* puede convertirse en un vector utilizado para el robo de identidad y el fraude al consumidor,



LA PIRATERÍA EN NÚMEROS

La “Gatonet” genera perjuicios billonarios a la economía brasileña.

15,5 mil millones de reales

por año es el impacto financiero de la piratería de TV. Solo en impuestos, el gobierno deja de recaudar

2 mil millones de reales por año



33 millones

de brasileños consumen contenido de TV por suscripción por uno o más **medios ilegales**



4,2 millones

de cuentas de TV por suscripción **fueron canceladas** en Brasil, por decisión del cliente o por falta de pago, en los últimos cinco años



150 000

puestos de trabajo **pueden extinguirse** en diez años si no hay un combate eficaz al problema



10 000 reales

de multa y hasta cuatro años de prisión puede ser la pena para quien **compra o vende** productos piratas

fuentes: Ancine, ABTA e Anatel

¹² Cf. AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL (Brasil). Superintendencia de Fiscalización. **Informe n.º 8/2022/FIGF4/FIGF/SFI.** Brasilia. 2022. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqbGHZc2pUgPteuRLZ6SDuwZoTzuakE9xm340u-SmUAwHzdKU2tlv4WgKQmypi8cvl3ntyOGfLQji7o_Cb0uH4U-. Acceso el: 23 jul. 2025.

ataques de *ransomware*, redireccionamiento de publicidad, entre otros¹³. Esto significa que los consumidores pueden ser atacados directamente, con sus cuentas bancarias en riesgo y con la posibilidad de que sus dispositivos y datos personales sean mantenidos como rehén¹⁴. También implica que los consumidores pueden visualizar anuncios secuestrados, privando a las empresas legítimas del espacio publicitario por el cual pagaron.

- **Minería de criptomonedas** – La capacidad de la CPU de los dispositivos del consumidor es utilizada para minar criptomonedas, lo que incrementa significativamente la carga de la CPU y el consumo de energía¹⁵. Los consumidores no son los beneficiarios de esta minería –las ganancias son retenidas por los propietarios del sitio.
- **Daños sociales** – La promoción de sitios de apuestas y de contenido para adultos dirigida a consumidores, especialmente niños, representa riesgos significativos para la sociedad en general, en particular el desarrollo de adicción al juego¹⁶.

Adicionalmente, en lo que se refiere a las vulnerabilidades cibernéticas, se destaca el informe *Satori Threat Intelligence Disruption: BADBOX 2.0 Targets Consumer Devices with*

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. Disponible en: <https://ieeexplore.ieee.org/document/7784601>. Acceso en 25 jul. 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. Disponible en: <https://ieeexplore.ieee.org/document/9461272>. Acceso en: 31 ago. 2025.

¹⁵ VAN DER SAR, Ernesto. **The Pirate Bay Website Runs a Cryptocurrency Miner**. 2017. Disponible en: <https://torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/>. Acceso en: 14 jun. 2025.

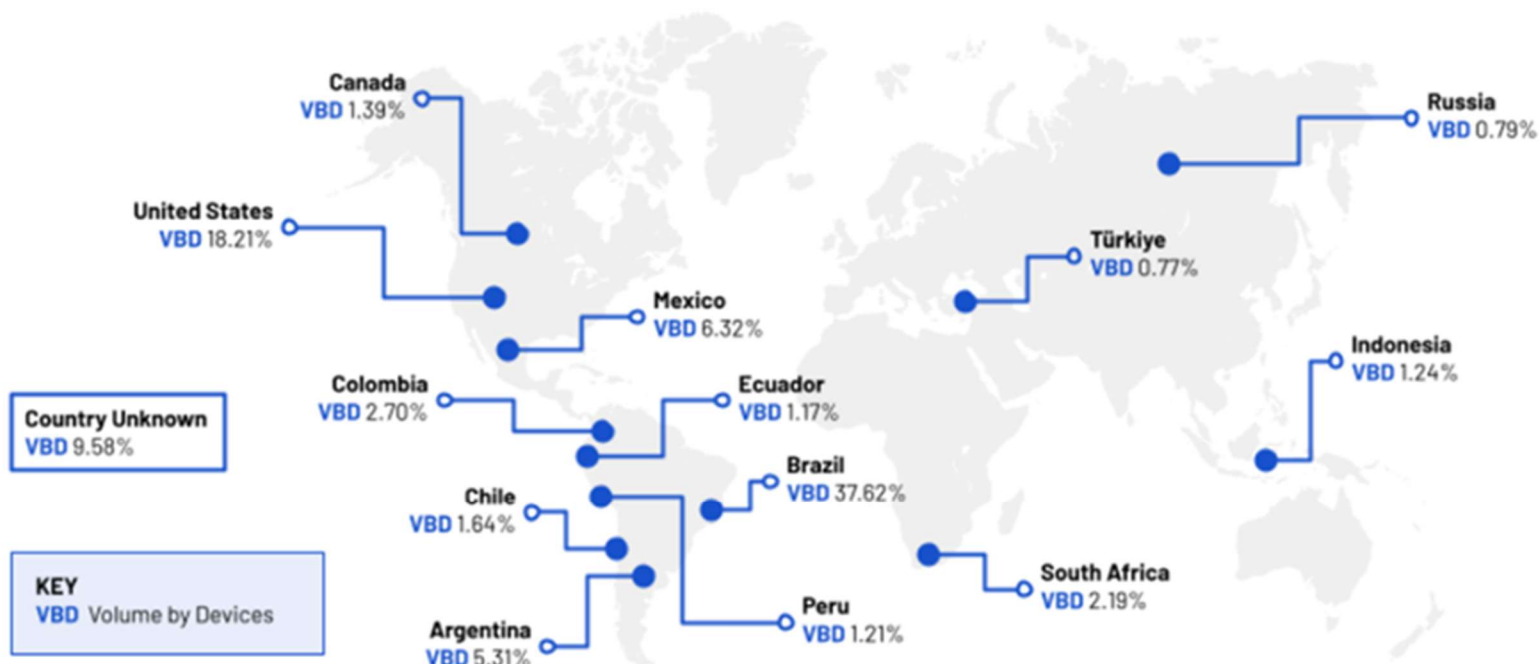
¹⁶ SURIADI, Suriadi; SUSNJAK, Teo; PONDER-SUTTON, Agate; WATTERS, Paul; SCHUMACHER, Christoph. Using data-driven and process mining techniques for identifying and characterizing problem gamblers in New Zealand. **Complex Systems Informática and Medelin Quartela**, Riga, Latvia, n. 9, p. 44–66, 2016. DOI: 10.7250/csimq.2016-9.03. Disponible en: <https://csimq-journals.rtu.lv/csimq/article/view/csimq.2016-9.03..> Acceso en: 31 ago. 2025.

Multiple Fraud Schemes¹⁷, publicado por Human Security (empresa estadounidense dedicada al desarrollo de soluciones para proteger organizaciones contra robots sofisticados, fraudes y abusos digitales) en marzo de 2025.

Según el informe, BADBOX 2.0 es una red cibercriminal de gran escala que se caracteriza por infiltrar *malware* directamente en el *firmware* (tipo de *software* que controla el *hardware* de un dispositivo electrónico) de dispositivos Android durante su fabricación o distribución — un ataque a la cadena de suministro con impactos globales.

Se estima que más de 200 modelos de dispositivos fueron comprometidos, incluyendo *set-top boxes*, tabletas, teléfonos inteligentes y dispositivos de *streaming*, siendo que Brasil concentraba aproximadamente el 37% de un universo estimado de 1 millón de dispositivos afectados en el momento del desarrollo del estudio.

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

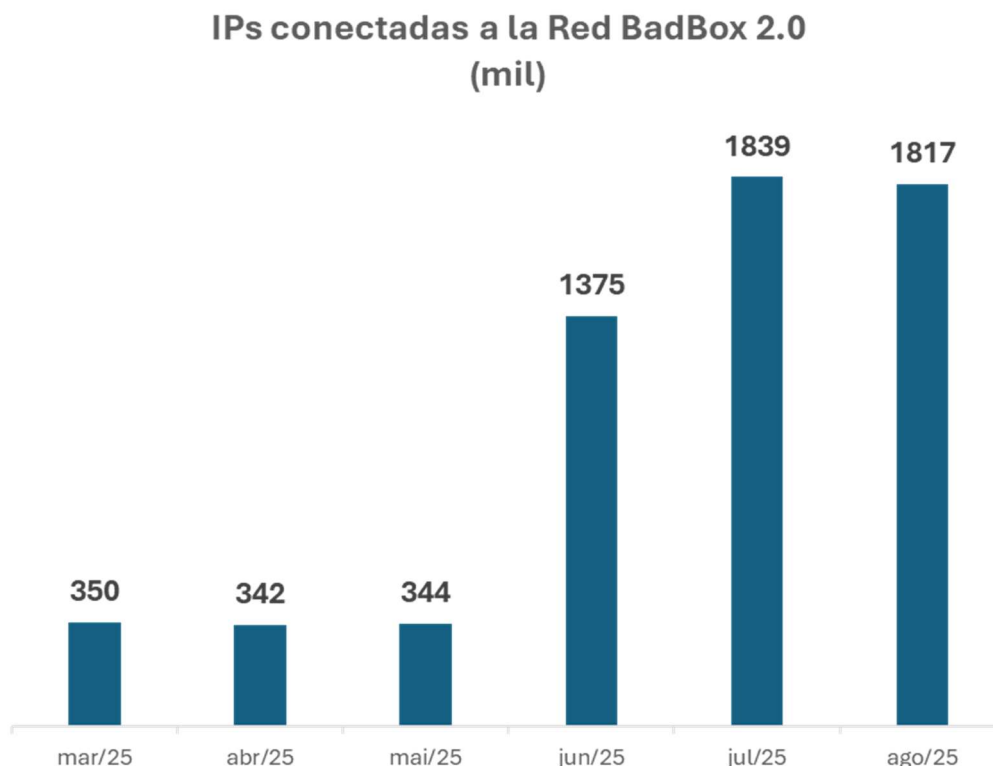


Fuente: Human Security

La Anatel emitió una alerta urgente sobre el *malware* BadBox 2.0, identificado en TV Boxes no homologadas, que pueden actuar como vectores de delitos cibernéticos, comprometiendo tanto los datos de los usuarios como la seguridad de las redes de telecomunicaciones.

El estudio de la Agencia, realizado en un laboratorio especializado, reveló que estos dispositivos contienen *malware* persistente. Incluso después de reinicios y en modo de espera, mantienen conexiones con servidores externos maliciosos. Se detectó el uso no autorizado de estos aparatos como *proxy* residencial, posibilitando fraudes publicitarios, robo de credenciales, ataques DDoS y acceso a sitios sensibles, como bancos y tribunales. En datos actualizados de agosto de 2025, solo Brasil ya concentra casi 2 millones de dispositivos infectados conectados a la red BadBox 2.0¹⁸.

¹⁸ AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL. **Anatel emite alerta sobre malware "Bad Box 2.0" em TV Boxes piratas.** Brasília, DF: Anatel, 25 jul. 2025. Disponible en: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-emite-alerta-sobre-malware-bad-box-2-0-em-tv-boxes-piratas>. Acceso el: 14 ago. 2025.



Estos datos demuestran que el combate a la piratería va más allá de la protección del sector regulado: se trata de una política pública orientada a preservar el orden económico, la salud y la seguridad de los usuarios y la integridad de las redes de telecomunicaciones. La actuación de la Anatel busca no solo reprimir prácticas ilícitas, sino también prevenirlas, por medio de acciones educativas, actualización de la regulación y ampliación de la cooperación con entidades nacionales e internacionales.

De esta forma, la presencia activa de la Agencia en este escenario se justifica no solo por su papel institucional, sino también por la urgencia de proteger a la sociedad brasileña ante un problema que afecta directa o indirectamente a millones de ciudadanos y que compromete el futuro de las comunicaciones en el país.

2. ACCIONES DE COMBATE A LA PIRATERÍA Y SUS REACCIONES

2.1. PACP – Plan de Acción de Combate a la Piratería

Desde la creación de la Agencia Nacional de Telecomunicaciones, en 1997, las acciones de fiscalización de productos homologados inicialmente se centraban en la verificación de denuncias y, de forma indirecta, en la realización de inspecciones técnicas de rutina en estaciones de radiodifusión o telecomunicaciones. Durante la verificación de características técnicas, los inspectores eventualmente encontraban equipos sin la certificación exigida.

Para la verificación de las denuncias presentadas a la Agencia, las acciones de fiscalización se realizaban en tiendas y centros comerciales, es decir, en el mercado minorista.

En su estructura organizacional, la Anatel cuenta con representación institucional en las 27 unidades federativas. En cada unidad descentralizada de la Agencia, existían equipos de fiscalización que actuaban de forma individualizada para atender las demandas recibidas. Entre 2012 y 2017 se atendieron 492 denuncias, un promedio de 82 demandas por año, distribuidas entre todas las unidades federativas.

La cantidad de demandas de fiscalización para verificar la certificación de productos de telecomunicaciones era significativamente menor si se comparaba con las denuncias relativas a la explotación clandestina de servicios de radiodifusión o telecomunicaciones, interferencias radioeléctricas u otras temáticas, como fiscalización de infraestructura de redes o estaciones.

En 2017, P&D Brasil —*Associação de Empresas de Desenvolvimento Tecnológico Nacional e Inovação*—, entidad que representa a fabricantes de equipos con tecnología nacional,

presentó un dossier a la Agencia con un estudio que concluía que, en el mercado de Proveedores de Internet (ISP, por sus siglas en inglés *Internet Service Providers*), aproximadamente el 70% de los equipos utilizados no contaban con homologación de la Anatel.

Ese mismo año, la ABTA presentó a la Agencia información sobre pérdidas millonarias para la industria electro-electrónica y para la recaudación tributaria, relacionadas con el contrabando de productos de telecomunicaciones o incluso con la importación legal de productos no homologados. Solo en el mercado de TV por suscripción, la estimación de la ABTA era de pérdidas anuales de ingresos de R\$ 6 mil millones.

Ante este escenario, considerando el aumento en el volumen de denuncias, incluidas aquellas relativas a empresas que comercializaban equipos no homologados en diversas regiones del país, y el crecimiento de productos no homologados en el mercado nacional, como *set-top boxes*, cargadores y teléfonos móviles, la *Superintendência de Fiscalização* (SFI) de la Anatel concluyó que era necesaria una modificación en la planificación de las acciones de fiscalización y en los procedimientos aplicables al combate de la comercialización de productos irregulares.

La SFI, entonces, elaboró un plan de acción que consideró un nuevo enfoque para las acciones de fiscalización relativas a la certificación de productos para telecomunicaciones. En lugar de actuar únicamente en reacción a denuncias puntuales, la Agencia pasó a operar con base en una planificación anual que priorizara la fiscalización de los elementos centrales y más relevantes de la cadena de comercialización de productos de telecomunicaciones, como fabricantes, distribuidores e importadores. El objetivo era aumentar la eficiencia de las acciones de fiscalización en la prevención y en el combate a la comercialización de productos no homologados, buscando como resultado la reducción del uso de estos productos en las redes de telecomunicaciones.

Cabe destacar que, según esta estrategia, la atención de denuncias puntuales seguiría, pero la planificación y el análisis de las acciones de fiscalización derivadas se realizarían de forma centralizada para todo el territorio nacional. Además de conferir mayor estandarización en el tratamiento de las denuncias, las acciones resultantes podrían ser planificadas de manera coordinada.

El 9 de febrero de 2018, la SFI aprobó el *Plano de Ação de Combate à Pirataria* (PACP) y designó a la Gerencia Regional de la Anatel en los estados de Goiás, Mato Grosso, Mato Grosso do Sul y Tocantins (GR07) como responsable de coordinar la ejecución del plan a nivel nacional.

Entre las primeras acciones del nuevo plan, se planificaron fiscalizaciones presenciales en algunas decenas de distribuidores de productos de telecomunicaciones. Se trataba de una gran innovación en el procedimiento adoptado por la Agencia, que históricamente actuaba directamente en el mercado, inspeccionando cientos de tiendas.

En un primer momento, se definieron seis ejes o grupos que englobarían las acciones de fiscalización para componer el PACP:



En el primer año del PACP, en 2018, fueron retirados del mercado cerca de 164 mil productos irregulares, entre ellos equipos de radiación restringida utilizados en redes de proveedores de servicios de internet, cables metálicos, cables ópticos y equipos de redes de datos. Las acciones de fiscalización eran realizadas exclusivamente por la Anatel. Ese número representó un gran salto en el volumen de incautaciones, que se limitaban a unas pocas centenas de unidades en los años anteriores.

Al año siguiente, en 2019, el resultado fue de aproximadamente 165 mil productos irregulares de telecomunicaciones retirados del mercado, entre ellos cargadores de baterías, *TV Boxes*, equipos de radiación restringida y cables metálicos y ópticos. Ese año hubo un acercamiento con la *Secretaría de Ingresos Federales*, en los Centros Internacionales de Tratamiento de Envíos Postales (CEINT), en Pinhais/PR, y en el Aeropuerto Internacional de Galeão, en Río de Janeiro/RJ. Cabe destacar que, desde 2012, antes del PACP, ya había un trabajo desarrollado en los Correos en São Paulo/SP, el cual fue incorporado al PACP.

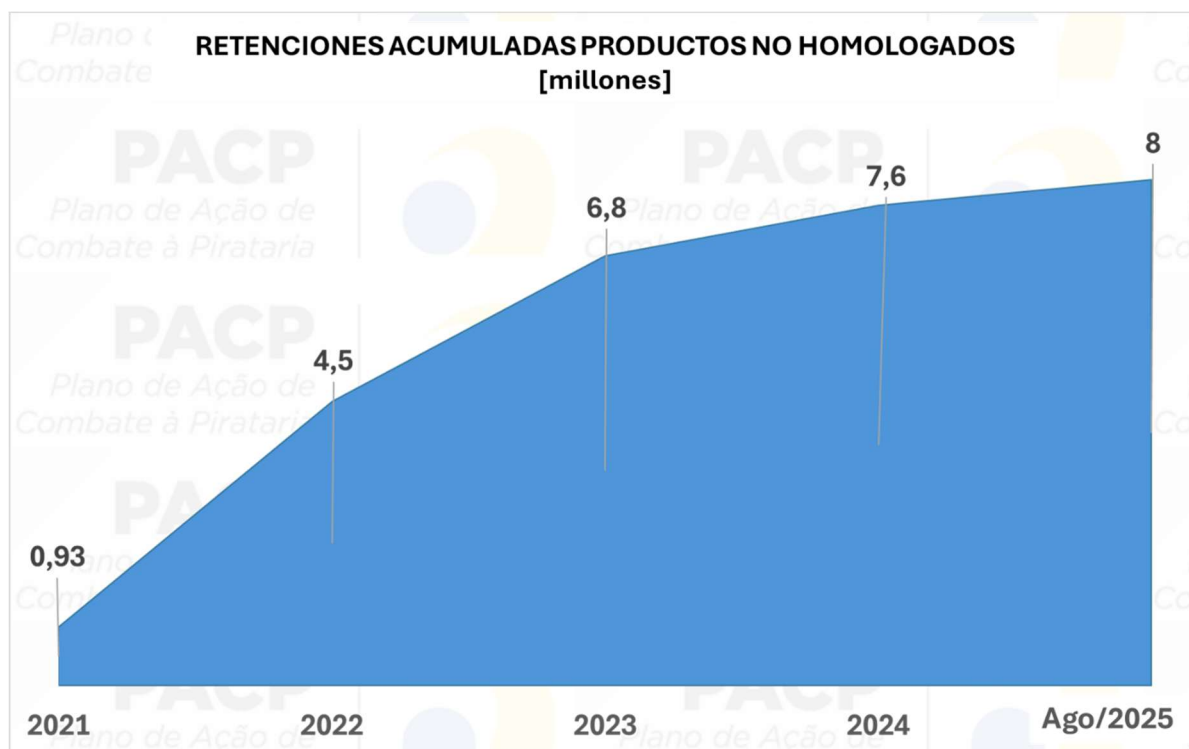
Es importante señalar que los CEINT son instalaciones de los Correos, pero controladas por

la *Secretaría de Ingresos Federales*, por constituir locales aduaneros para la recepción de mercancías compradas en el exterior e importadas al territorio nacional. En estos ambientes, la Anatel inspecciona productos como *drones*, *TV Boxes*, transceptores y productos emisores de radiofrecuencias.

Un dato relevante sobre los CEINT es que en ellos ya se han retenido cientos de *jammers*, cuyo uso es restrictivo en el país y está prohibido tanto para personas físicas como para empresas privadas, conforme lo previsto en el Reglamento sobre Bloqueador de Señales de Radiocomunicaciones, aprobado por la Resolución Anatel nº 760, del 6 de febrero de 2023. Debido a que estos equipos provocan interferencias extremadamente perjudiciales en las redes móviles y, en algunos casos, son utilizados por organizaciones criminales, su uso es estrictamente limitado, bajo determinadas condiciones, únicamente a las fuerzas policiales, fuerzas armadas y establecimientos penitenciarios.

En algunos aeropuertos, la Anatel inspecciona mercancías importadas por empresas privadas, conocidas como *courriers*, en áreas aduaneras controladas por la *Secretaría de Ingresos Federales*.

Hasta finales de 2020, fueron retirados del mercado más de 930 mil productos irregulares de telecomunicaciones. Al cierre de 2021, ese total alcanzó 4,5 millones, un récord. Este número reflejó la mayor integración de la Anatel con la *Secretaría de Ingresos Federales* de Brasil en algunos puertos del país.



Fuente: PACP/ANATEL

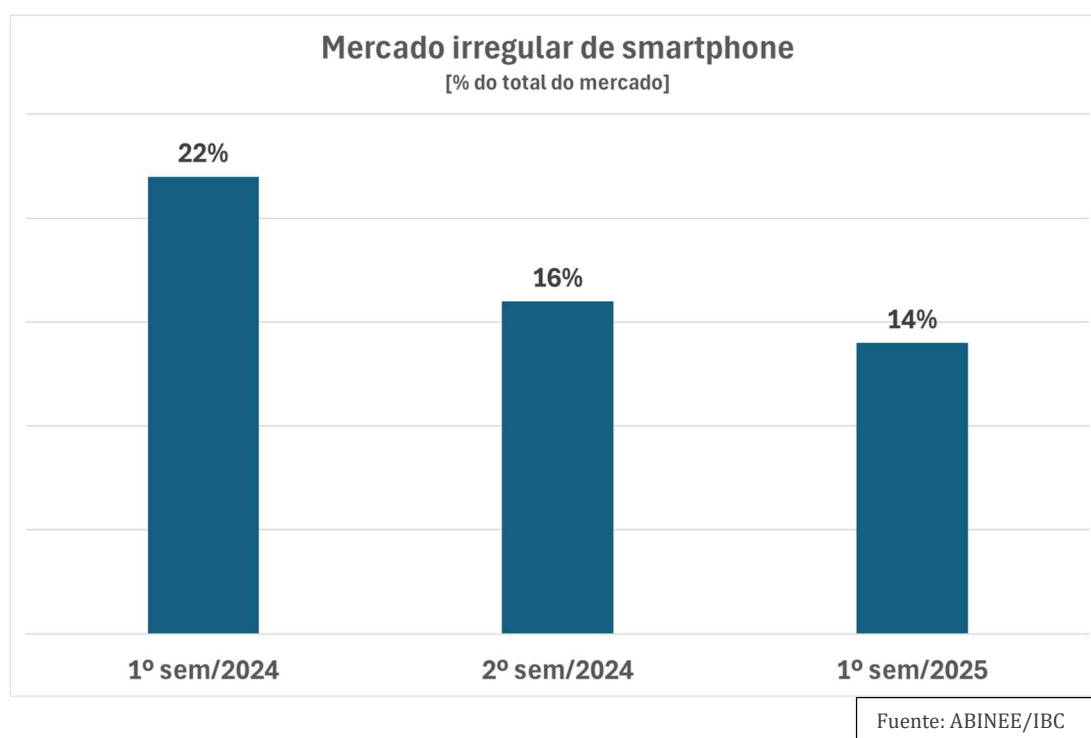
Considerando la necesidad de un mejor seguimiento de los resultados de las actividades y de una mayor transparencia en la información relacionada con las acciones de fiscalización del PACP, se creó un panel público (dashboard) en la siguiente dirección: <https://informacoes.anatel.gov.br/paineis/fiscalizacao>. La información relacionada con las acciones de fiscalización, como la unidad de la federación, el mes y el año en que se realizaron, así como el tipo de equipamiento inspeccionado y la región geográfica, se presenta en el panel y puede consultarse libremente, pues es de dominio público.

- En una consulta realizada al panel público a finales de julio de 2025, se verificó que, por medio de las acciones de fiscalización, fueron inspeccionados y considerados regulares un total de 3.779.825 productos, mientras que otros 8.053.098 productos no homologados fueron retirados del mercado, con un valor estimado de R\$ 833.617.356,00 (ochocientos treinta y tres millones, seiscientos diecisiete mil, trescientos cincuenta y seis reales). El análisis de estos resultados se presenta a

continuación:

- Cerca del 71% de los productos retirados del mercado resultaron de acciones de la Secretaría de *Ingresos Federales* Brasil en los puertos, las cuales contaron con el apoyo de Anatel. Esos productos retenidos no habían sido homologados.
- Los productos retenidos por la RFB permanecen bajo custodia del órgano aduanero. Si el importador no regulariza los productos, la Secretaría de la Receita Federal de Brasil les asigna un destino legal específico, que puede ser la destrucción, la devolución al origen o incluso la donación a programas educativos que transforman esos productos en otros con una finalidad distinta. El *set top box* es un ejemplo de un producto que puede convertirse en minicomputadoras o sensores para equipos industriales.
- La gran mayoría de los productos no homologados que fueron retenidos por la Secretaría de la Receita Federal de Brasil, con el apoyo de Anatel, tienen como origen China.
- Algunas de las técnicas utilizadas por los importadores para burlar la fiscalización aduanera incluyeron la falsificación de sellos, el uso de sellos verdaderos en productos no homologados, el desensamblaje de productos en piezas menores e incluso la alteración de la descripción de los productos.

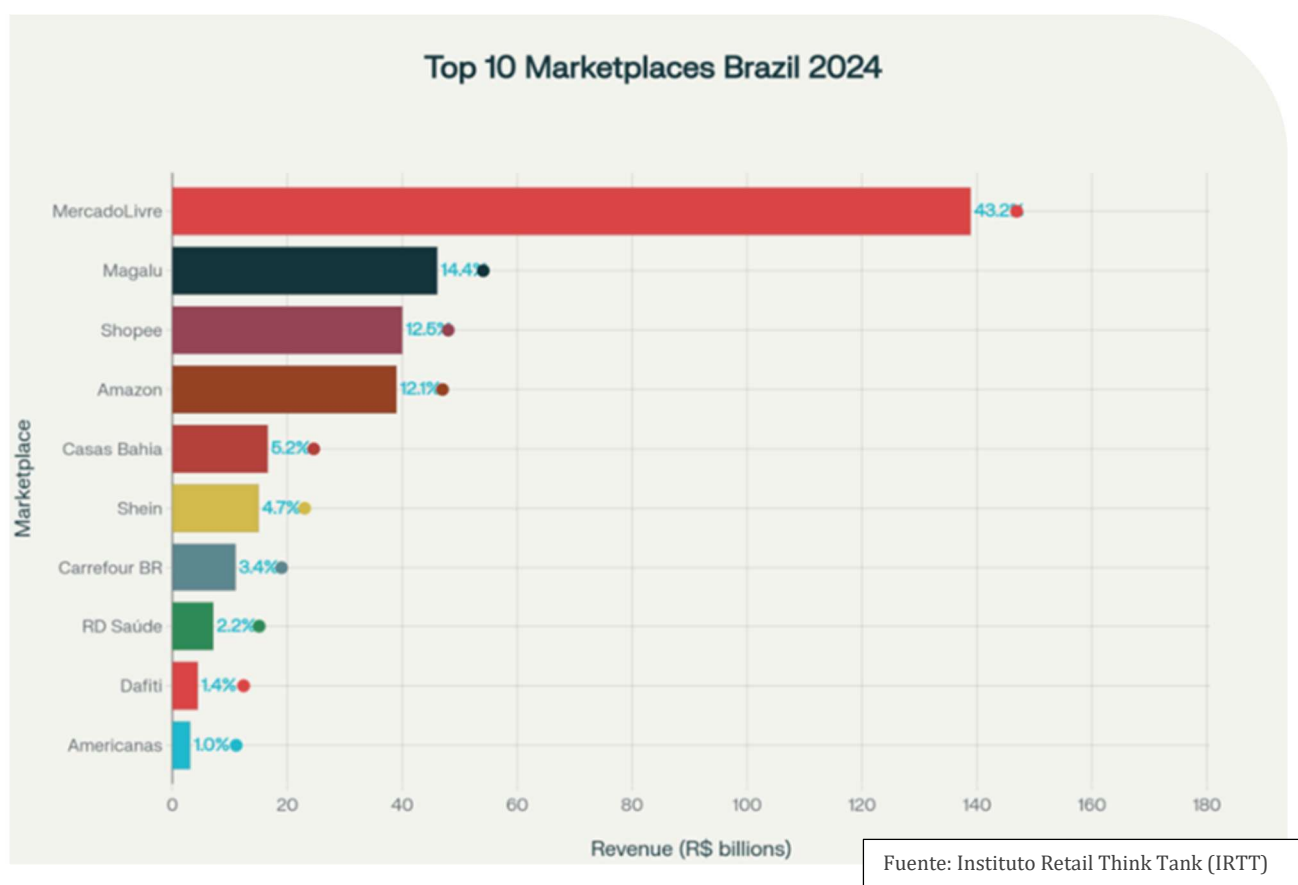
El combate contra la piratería por parte de Anatel se ha intensificado especialmente en relación con el llamado "mercado gris" de teléfonos móviles en Brasil, que involucra la comercialización de dispositivos importados sin homologación y sin garantía de conformidad con los estándares técnicos y de seguridad exigidos.



2.2. Combate a la Piratería en *Marketplaces*

Además de las acciones de fiscalización que involucran la colaboración con la Secretaría de la Receita Federal de Brasil, existe otro eje de actuación que ha adquirido especial relevancia en el PACP: el comercio electrónico, en particular las empresas que operan como *marketplaces*.

Con la pandemia de la Covid-19, la comercialización de mercancías por medios electrónicos aumentó de forma exponencial, y las plataformas de las grandes empresas de *marketplaces* presentes en el país como Mercado Libre, Amazon, Shopee, Casas Bahia, Carrefour, Americanas y Magalu cobraron protagonismo.



En este escenario, la Anatel instauró procedimientos de fiscalización regulatoria frente a dichos *marketplaces*, con el fin de buscar una composición amistosa para la regularización del comercio electrónico de productos de telecomunicaciones. Sin embargo, Anatel siempre se encontraba con la falta de disposición de los agentes económicos supervisados para aplicar sus conocimientos tecnológicos (a pesar de todos los esfuerzos del organismo regulador en proporcionar los insumos necesarios) para impedir la venta de productos no homologados en sus sitios electrónicos.

Considerando el universo de decenas o cientos de miles de anuncios en las plataformas de *marketplace*, el trabajo de fiscalización manual se mostró inviable o imposible de realizar. Para desarrollar soluciones a problemas de esta naturaleza, la Superintendencia de Fiscalización creó un Laboratorio de Innovación, compuesto por servidores dedicados a la producción de herramientas avanzadas de apoyo a las acciones de fiscalización. Uno de los

primeros productos desarrollados por el Laboratorio de Innovación fue la creación de un robot, con uso de Inteligencia Artificial, llamado “Regulatron”, para monitorear los anuncios en las plataformas e identificar productos de telecomunicaciones no homologados.

El análisis de los datos proporcionados por el “Regulatron”, realizado en junio de 2024, consistente en la verificación electrónica de anuncios publicados en plataformas de comercio electrónico en comparación con la información técnica de productos homologados en la base de datos de la Agencia, demostró un avance en la inclusión de los códigos de homologación en los anuncios de productos en las plataformas Mercado Libre, Amazon, Shopee, Carrefour, Magalu, Americanas y Casas Bahia. Sin embargo, quedó evidenciado que, pese a todos los esfuerzos realizados por Anatel desde 2018, seguía siendo elevado el porcentaje de productos cuyos códigos de homologación no están validados con la base de Anatel, incluso con códigos inexistentes o correspondientes a otros productos.



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

Los riesgos derivados de esta amplia comercialización de productos no homologados para los consumidores motivaron la expedición de una medida cautelar, materializada en los

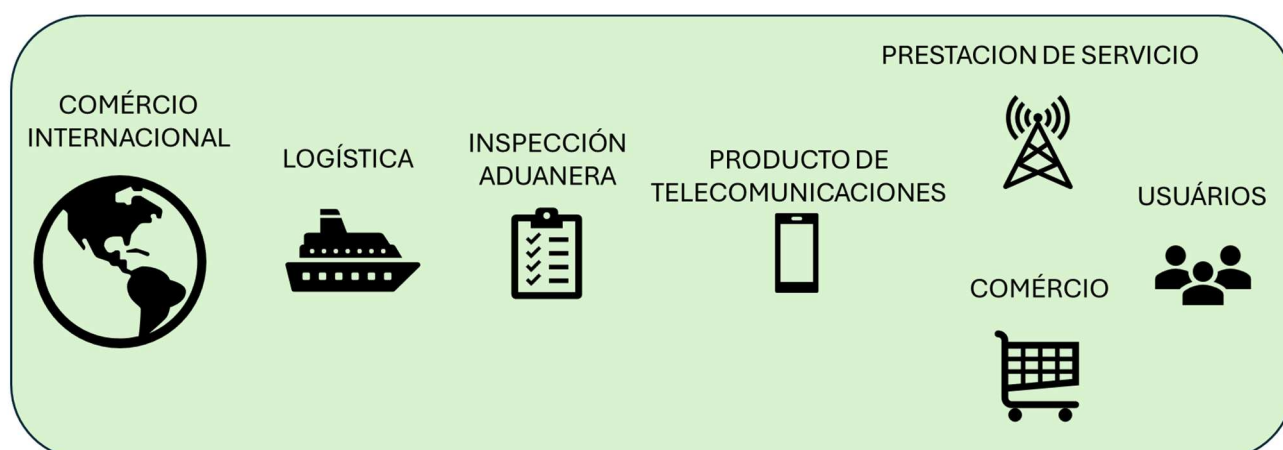
Despachos Decisorios n.º 5657/2024/ORCN/SOR¹⁹ (SEI n.º 12160352) e 5686/2024/ORCN/SOR²⁰ (SEI n.º 12163126), aún vigentes, lo cual constituye una señal importante para el mercado en línea de que el órgano fiscalizador monitorea sus actividades con el objetivo de impedir la comercialización de productos irregulares.

Además de la validación de los códigos de homologación, es fundamental que los *marketplaces* o cualquier otro involucrado en el proceso de comercialización verifiquen el origen al adquirir o poner a disposición un producto de telecomunicaciones. Esto se debe a que únicamente el titular del Certificado de Homologación puede vender o autorizar a otro a comercializar el producto de telecomunicaciones, dado que sobre él recae la responsabilidad derivada del producto frente al consumidor brasileño.

Desde el inicio del PACP, la Agencia ha realizado esfuerzos para convertirse en socia de otros órganos en las actividades de fiscalización, ya sea en las zonas fronterizas o en el mercado interno nacional. Los resultados presentados demuestran que, cuando existe cooperación entre los órganos, los efectos se potencian. No obstante, aún existen barreras por superar para que los organismos puedan trabajar de manera verdaderamente sinérgica, como se mostrará a continuación.

¹⁹AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL (Brasil). Superintendencia de Otorgamiento y Recursos a la Prestación, Superintendencia de Fiscalización. **Despacho Decisório n.º 5657/2024/ORCN/SOR**. Brasilia, 2024. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYmk7UOA8fj5jIUHIDwe0NhuPf9JzG-Uyip5lqqRmZXWq3_FHP60CDJBwjfirYwgLZsBySFp8Kq5_qlyt8sBgO. Acceso el: 23 jul. 2025.

²⁰AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL (Brasil). Superintendencia de Otorgamiento y Recursos a la Prestación, Superintendencia de Fiscalización, Superintendencia de Control de Obligaciones. **Despacho Decisório n.º 5686/2024/ORCN/SOR**. Brasilia, 2024a. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqZApP7PurlyWa1s0oaWqCwkV7A2ZHNvzF5QswTfpGIhwO97BwkTz78Z4IVzklfCymkA1dhf6kvAa4Vna4sXaT3. Acceso el: 23 jul. 2025.



2.3. Alianzas con los organismos de la administración pública

Secretaría de la Receita Federal de Brasil

Brasil posee una inmensa frontera terrestre de aproximadamente 16,9 mil kilómetros de extensión, limitando con 10 países vecinos. La mayor frontera es con Bolivia, con cerca de 3,4 mil kilómetros. A través de esta extensa franja fronteriza ingresa al país una gran cantidad de productos piratas de diversos segmentos, incluidos los de telecomunicaciones, tales como teléfonos celulares, cargadores de baterías, TV Boxes, baterías, drones, productos con tecnologías *wifi* y *bluetooth*, transceptores, así como equipos de uso restringido, como los inhibidores de señal (bloqueadores de señales).

La Secretaría Especial de la Receita Federal de Brasil (RFB) es un órgano de la administración pública federal responsable de administrar los tributos federales y ejercer el control aduanero. Además, la RFB actúa en el combate a la evasión fiscal, al descamino y al contrabando de mercancías que ingresan al territorio nacional.

En la estructura organizacional de la Receita Federal de Brasil, la Subsecretaría de Administración Aduanera (SUANA) se divide en la Coordinación General de Administración Aduanera (COANA), la Coordinación General de Combate al Contrabando y Descamino (COREP) y la Coordinación General de Riesgos Aduaneros (CORAD). Para lograr un mayor

control y fiscalización, la RFB definió dos grandes áreas de actuación: la zona primaria, bajo la responsabilidad de la COANA, y la zona secundaria, bajo la responsabilidad de la COREP.

La zona primaria, en el contexto del comercio exterior, se refiere a los lugares donde ocurren las operaciones de entrada y salida de mercancías del territorio nacional, como puertos, aeropuertos y regiones fronterizas con aduana, en los cuales se realizan las acciones de fiscalización aduanera en las actividades de importación y exportación. La zona secundaria, a su vez, corresponde a la parte del territorio aduanero que no forma parte de la zona primaria. Básicamente, es todo lo que no está incluido en la zona primaria, incluyendo aguas territoriales y espacio aéreo.

La alianza entre Anatel y la RFB se desarrolla en algunas zonas primarias ubicadas en puertos y aeropuertos, en los centros internacionales de tratamiento de envíos postales, que son áreas de Correos, pero bajo supervisión de la RFB, y en la zona secundaria, en determinados estados.



Fuente: Portal GOV.br

Los esfuerzos de la Agencia para ampliar la alianza con la RFB en todo el territorio nacional continúan. Más recientemente, la Agencia fue admitida como interviniente del Sistema de

Comercio Exterior (Siscomex). Esta integración permitirá que Anatel acceda a los datos del Siscomex y, de esta manera, realice un análisis previo de los registros de importación, garantizando la identificación de los equipos que se encuentren en conformidad con las reglas establecidas por la Agencia.

El borrador del Procedimiento Operativo para el Tratamiento Administrativo en el Sistema de Comercio Exterior de las Operaciones de Importación de Mercancías Sujetos a Homologación por la Anatel fue puesto en consulta pública bajo el número 17/2025, en el período del 17 de junio al 26 de agosto de 2025.

La propuesta busca sustituir el actual Procedimiento Operacional para la Importación de Productos de Telecomunicaciones, aprobado por el Resolución nº 4521, del 21 de julio de 2021. Dicho procedimiento define las condiciones para el tratamiento administrativo de las acciones de importación de productos y equipos sujetos a la homologación de Anatel en el Sistema Integrado de Comercio Exterior (SISCOMEX).

La Anatel, como órgano interviniente del Siscomex, aporta una gran experiencia técnica en la evaluación de la conformidad de los productos de telecomunicaciones dentro del proceso de despacho aduanero, permitiendo identificar y restringir que productos irregulares, es decir, no homologados, ingresen al mercado nacional. Este proceso fortalece la integración entre ambos organismos, cuyas tareas se complementan y se suman en el combate al ingreso de productos no homologados al país.

Polícia Federal de Carreteras – *Polícia Rodoviária Federal (PRF)*

La Agencia ha sido invitada a participar en acciones de fiscalización conjuntas con otros organismos, en operativos coordinados por la *Polícia Rodoviária Federal (PRF)*. El objetivo principal de estas acciones es capacitar a los policías rodoviarios federales para la ejecución de actividades de rutina que puedan ocurrir en las carreteras federales.

Las acciones se estructuran en operativos temáticos, con el fin de alinear y actualizar los conocimientos y competencias multidisciplinares de los efectivos locales; fortalecer la integración con los organismos públicos y entidades privadas de interés público, en especial con el Ministerio de Agricultura y Ganadería, otras Agencias, la Secretaría de Ingresos Federales de Brasil, las Secretarías de Hacienda estatales y otras Secretarías involucradas; promover el perfeccionamiento y el intercambio de información entre los PRFs y los servidores de las instituciones asociadas; e intensificar el enfrentamiento a la criminalidad, promoviendo la preservación del orden público y de la integridad de las personas y del patrimonio en las carreteras federales.



Fuente: Portal GOV.br

Polícia Federal

En el ámbito del Plan de Acción de Combate a la Piratería (PACP), las acciones de fiscalización han encontrado con frecuencia equipos no homologados que presentan altas restricciones de uso en el país. Es el caso de los bloqueadores de señales, conocidos como *jammers*, y más recientemente de los bloqueadores *antidrone*. Los *jammers* son utilizados casi siempre

por organizaciones criminales para la práctica de robos de mercancías en carreteras. Los bloqueadores *antidrone*, por su parte, fueron encontrados en operaciones realizadas en cooperación con la Secretaría de Ingresos Federales de Brasil y organismos policiales. En estos casos, los equipos tenían la finalidad de ser utilizados por organizaciones criminales para obstruir acciones policiales. Estos productos suelen ser importados e ingresan clandestinamente al país mediante bandas especializadas en el contrabando de mercancías.

Ante este escenario y la necesidad de profundizar las investigaciones para identificar a los destinatarios de estos equipos, así como su finalidad de uso y comercialización, Anatel busca compartir información de inteligencia con la Policía Federal, entendiendo que se trata de situaciones que involucran riesgos para la seguridad nacional, especialmente por la práctica de diversos ilícitos cometidos por organizaciones criminales.

En el mes de julio de 2025, la Policía Federal lideró una operación que contó con el apoyo de agentes de fiscalización de la Anatel para desarticular una sofisticada organización criminal especializada en la importación y comercialización de aparatos ilegales de IPTV, comúnmente conocidos como *TV BOX* y *Gatonet*.

La Policía Federal identificó que la organización movilizó grandes sumas de dinero, operaba con una estructura sofisticada de empresas fantasma y logística transnacional, con aparatos provenientes de la frontera con Paraguay, a través de la ciudad de Foz do Iguaçu/PR.

Se adoptaron medidas cautelares, como el bloqueo de R\$ 33 millones, el secuestro de vehículos e inmuebles y el bloqueo de sitios web utilizados para la comercialización de aparatos no homologados.

Los agentes de fiscalización identificaron cerca de 140 aparatos de TV BOX no homologados en posesión de la organización, con un valor estimado en R\$ 125.860,00. Además intercambio de información entre los organismos y de la cooperación en acciones conjuntas

enfocadas en los productos no homologados, la Policía Federal investiga delitos como



Fuente: Portal GOV.br

evasión fiscal, préstamos fraudulentos y lavado de dinero, contando con el apoyo de los equipos de fiscalización de la Anatel^{21,22}.

CNCP

El Consejo Nacional de Combate a la Piratería y a los Delitos contra la Propiedad Intelectual (CNCP) es una entidad gubernamental que forma parte del Ministerio de Justicia y Seguridad Pública (MJSP), compuesta por veinte representantes del poder público y de la Sociedad

²¹AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL (Brasil). **Anatel, Polícia Federal e Receita Federal realizam ação conjunta em Pelotas (RS)**. Brasília, DF: Anatel, 09 jul. 2025. Disponible en: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-policia-federal-e-receita-federal-realizam-acao-conjunta-em-pelotas-rs>. Acceso el: 27 jul. 2025.

²²AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL (Brasil). **Anatel e PF desarticulam esquema milionário de "TV Box" e "Gatonet" em Operação PRAEDO**. Brasília, DF: Anatel, 29 jul. 2025. Disponible en: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-e-pf-desarticulam-esquema-milionario-de-tv-box-e-gatonet-em-operacao-praedo>. Acceso el: 29 jul. 2025.

Civil Organizada, además de decenas de colaboradores.

El CNCP tiene como finalidad articular y ejecutar políticas públicas de combate a la piratería, al contrabando y a los demás delitos contra la propiedad intelectual. La unión del sector público y privado en la lucha contra la piratería y el contrabando es de fundamental importancia para combatir a las organizaciones criminales que introducen productos irregulares en la economía y generan perjuicios para toda la sociedad.

Anatel está representada en el Consejo por la Superintendencia de Fiscalización, como miembro titular, y por el Superintendente de Otorgamiento y Recursos para la Prestación, como miembro suplente.

2.4. Evolución del entendimiento jurídico (*marketplace*, redes sociales y cadena de distribución)

Como mencionado anteriormente, Anatel ha actuado en el combate a la piratería de productos de telecomunicaciones mediante un conjunto de acciones jurídicas y regulatorias, incluyendo la realización de acciones de fiscalización, la celebración de acuerdos de cooperación y el lanzamiento de campañas educativas. El objetivo es garantizar la seguridad de los consumidores, la confiabilidad de las redes, la calidad de los servicios de telecomunicaciones y la competencia justa en el mercado.

2.4.1. Responsabilización de los *marketplaces*

Como se indicó anteriormente, el modelo de certificación de productos para telecomunicaciones actualmente vigente, implementado por el Reglamento aprobado por la Resolución nº 715/2019, norma todo el proceso de certificación en el ámbito de Anatel y, junto con los procedimientos operativos y los requisitos técnicos, detalla la forma y los parámetros técnicos necesarios para la homologación de un producto.

A pesar de la existencia de dicha reglamentación, en el inicio de las actividades de fiscalización en plataformas de comercio electrónico, los *marketplaces* alegaban neutralidad (inspirándose en el Art. 19 de la Ley nº 12.965, de 23 de abril de 2014 — Marco Civil de Internet), argumentando que no podrían ser responsabilizados por el contenido de terceros.

Ante ello, Anatel solicitó el apoyo de la Procuraduría Federal Especializada (PFE-Anatel) con el fin de presentar una interpretación teleológica de las mencionadas normas, a fin de perfeccionar la actuación de la Agencia y la responsabilización de diversos agentes económicos — especialmente *marketplaces* y plataformas digitales — por la comercialización de productos para telecomunicaciones no homologados.

2015

Dictamen nº 1.580/2015/PFE ANATEL/PGF/AGU ²³

Consulta:

Responsabilidad administrativa de intermediadores (marketplace)

Respuesta:

No pasible de sanciones

Aun cuando fueron notificadas, las plataformas alegaban actuar únicamente como intermediarias, y no como vendedoras.

En 2018, se instauró un Pado contra una empresa que ofrecía productos de telecomunicaciones no homologados bajo el argumento de tratarse de pruebas de mercado. Ante ello, el área técnica de Anatel consultó a la PFE-Anatel si la oferta de productos no

²³ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 01580/2015/PFE ANATEL/PGF/AGU**. Brasília, 2015. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?Yj72kUioo_z14_E1ere_NErKAAYpCDMsB4uhQFHnURzICcsEezBx7gPUNtxU8bNUcaTcrOnBnveExhjlYaFQPg7w474YcqjoUmoQPS4yTNLNaIUCTtkxM0SgmZMjHGDh. Acceso el: 21 jul. 2025.

homologados, sin venta efectiva, configuraría comercialización.

2018

Dictamen nº 524/2018/PFE ANATEL/PGF/AGU ²⁴

Consulta:

Responsabilidad administrativa por oferta y divulgación (Marketplace)

Respuesta:

Caracteriza comercialização sendo passível de autuação

A la luz de tales conclusiones, la responsabilidad administrativa de los *marketplaces* en la comercialización de productos irregulares siempre estuvo marcada por debates jurídicos sobre la extensión de la responsabilidad de los intermediadores de ventas en línea. La jurisprudencia y la doctrina oscilaban entre la responsabilización objetiva, con base en el Código de Defensa del Consumidor, y la necesidad de delimitar el alcance de dicha responsabilidad, considerando la naturaleza de la actuación del *marketplace* como mero intermediario.

Sin embargo, el mencionado escenario digital ha evidenciado la limitación del tradicional deber de protección estatal —históricamente concebido como criterio de control y conformación de la actividad legislativa— frente a los nuevos desafíos impuestos por las dinámicas propias del entorno informacional contemporáneo.

Como destacan Gilmar Mendes y Victor Oliveira Fernandes, dicho paradigma se muestra insuficiente para la adecuada resolución de conflictos entre derechos fundamentales en el

²⁴ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 00524/2018/PFE-ANATEL/PGF/AG**. Brasília, 2018. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5Aq93gDCiAKZgfvdufplsL2yUPD34g1U-JBQb1D9R_dacgaUTkfl4JNVnd23QsN5FoeTx1MPAZEgSqZRwJaIOS. Acceso el: 21 jul. 2025.

contexto digital.²⁵ Ello se debe a que, en las plataformas digitales, la estructuración del espacio público informacional ha sido, en gran medida, definida por agentes privados, que detentan una creciente capacidad de condicionar el ejercicio de libertades constitucionales.

En este entorno, prácticas relacionadas con la curaduría algorítmica, los sistemas de recomendación y la arquitectura de la elección permiten que tales agentes ejerzan una influencia relevante sobre los flujos de información, afectando el alcance, la visibilidad y el contenido de la comunicación realizada por los usuarios. Esta realidad impuso al Poder Público el desafío de desarrollar instrumentos normativos y regulatorios capaces de garantizar, de manera eficaz, la protección de los derechos fundamentales en el ecosistema digital.

En este escenario, el deber estatal de protección asumió múltiples dimensiones, como la obligación de interpretar las normas en conformidad con la Constitución, considerando la vulnerabilidad estructural del consumidor; el deber de actuación administrativa, mediante regulación y fiscalización eficaces; y la responsabilidad de formulación normativa, mediante la construcción de una arquitectura regulatoria que asegure la efectividad de la protección frente a las nuevas dinámicas de mercado y a los riesgos tecnológicos emergentes²⁶.

En el año 2020, la Secretaría Nacional del Consumidor (Senacon) enfrentó la cuestión de la comercialización de productos prohibidos y piratas que generan riesgo a la vida, la salud y la seguridad de los consumidores, y emitió una Nota Técnica.

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.º 1, p. 1–33, 2020. DOI: 10.18256/2238-0604.2020.v16i1.4103. Disponible en: <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103>. Acceso el: 10 ago. 2025.

²⁶ En este sentido, 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.

2019

Nota Técnica nº 610/2019/SENACON/MJ²⁷**Contexto Legal**

Se fundamenta en el Código de Defensa del Consumidor (CDC) y en la Constitución Federal, que prohíben la comercialización de productos ilegales y falsificados, incluso en plataformas digitales.

El derecho a la vida, la salud y la seguridad del consumidor es prioritario e inalienable.

Prohibición y Responsabilidad:

Los productos **ilegales o falsificados no pueden ser comercializados** bajo ninguna circunstancia.

Las plataformas **pueden ser responsabilizadas**:

Por la **falta de registro o identificación** de los vendedores;

Por la **ausencia de información clara** sobre los proveedores;

Por la **omisión en relación con los límites de su propia responsabilidad**.

Protección del Consumidor:

El CDC impone un **deber de prevención y cuidado** por parte de las plataformas.

Existe la posibilidad de **responsabilidad objetiva y solidaria** por los daños ocasionados.

Libertad Económica vs. Responsabilidad:

La **libertad de expresión no se aplica** como justificación para mantener anuncios de productos ilícitos.

Se trata del **ejercicio de la libertad económica, subordinada a la ley y al interés público**.

Las plataformas **deben remover** anuncios de productos irregulares y **no pueden alegar neutralidad**.

Conclusion:

Las plataformas de comercio electrónico **deben adoptar mecanismos eficaces de control, prevención y retiro de anuncios** de productos ilegales o falsificados, bajo pena de **responder solidariamente** con los vendedores, en conformidad con los principios del CDC y de la Constitución.

A su vez, una nueva Nota Técnica de la Secretaría Nacional del Consumidor consignó:

²⁷ MINISTERIO DE JUSTICIA Y SEGURIDAD PÚBLICA. SECRETARÍA NACIONAL DEL CONSUMIDOR. COORDINACIÓN DE CONSUMO SEGURO Y SALUD. **Nota Técnica n.º 610/2019/CCSS/CGCTSA/DPDC/SENACON/MJ**. Disponible en: <https://www.gov.br/mj/pt-br/assuntos/noticias/senac-con-questiona-sites-sobre-politica-para-evitar-anuncio-e-venda-de-produtos-falsificados/NTPirataria.pdf>. Acceso el: 10 ago. 2025.

2019**Nota Técnica nº 91/2020/SENACON/MJ**²⁸**Contexto Legal**

Analiza las respuestas de plataformas de comercio electrónico sobre las medidas adoptadas para combatir la venta de productos falsificados, destacando la necesidad de una actuación proactiva en la protección de los consumidores y en la prevención de ilícitos en las transacciones en línea.

Postura de las Plataformas y Responsabilidad:

Negar responsabilidad por la **publicidad, el anuncio o la oferta de productos falsificados** puede resultar en:

Procedimientos sancionadores;

Sanciones administrativas, con base en el **art. 55 del Código de Defensa del Consumidor (CDC)**.

La **omisión de las plataformas** se considera una **conducta potencialmente lesiva** para los consumidores.

Desafíos Regulatorios:

Las autoridades y los organismos de defensa del consumidor, **tanto en Brasil como en el exterior**, enfrentan **dificultades para adoptar medidas eficaces** contra productos **pirateados o falsificados**.

Se vuelve esencial la **adopción de medidas preventivas y de colaboración** por parte de las plataformas.

Conclusion:

Las conductas omisivas pueden generar responsabilidad civil y de consumo, a la luz de:

El **Código Civil**, y

El **Código de Defensa del Consumidor (CDC)**.

Las plataformas digitales **no pueden alegar ausencia de responsabilidad** por la presencia de productos falsificados en sus entornos. Deben **actuar preventivamente**, garantizando **transparencia, trazabilidad y seguridad** en las relaciones de consumo, bajo pena de **responsabilidad solidaria**.

Ante ello, y considerando la evolución de las prácticas de los *marketplaces*, la PFE-Anatel fue nuevamente consultada en 2021.

²⁸ MINISTERIO DE JUSTICIA Y SEGURIDAD PÚBLICA. SECRETARÍA NACIONAL DEL CONSUMIDOR. COORDINACIÓN DE CONSUMO SEGURO Y SALUD. **Nota Técnica n.º 91/2020/CCSS/CGCTSA/DPDC/SENACON/MJ**. Disponible en: <https://www.gov.br/mj/pt-br/acesso-a-informacao/perguntas-frequentes/consumidor/consumo-seguro-e-saude#:~:text=Nota%20%C3%A9cnica%20n%C2%BA%2091/2020,Permanentes%20de%20Acidentes%20de%20Consumo>. Acceso el: 10 ago. 2025.

2021**Dictamen nº 453/2021/PFE ANATEL/PGF/AGU**²⁹**Consulta:**

Evolución de las prácticas de los marketplaces -que pasaron a ofrecer servicios como almacenamiento, embalaje y despacho.

Respuesta:

Caracteriza una comercialización, siendo susceptible de sanción y de medidas cautelares, como la clausura y la incautación

Con ello, se hicieron posibles fiscalizaciones presenciales, incautaciones de productos irregulares y la instauración de Procedimientos de Fiscalización Regulatoria (PFR), con fundamento en el Reglamento de Fiscalización Regulatoria (RFR), aprobado por la Resolución nº 746, de 22 de junio de 2021, así como la apertura de PADOs directamente contra los *marketplaces*.

Tras la emisión del Dictamen nº 453/2021/PFE-ANATEL/PGF/AGU y la entrada en vigor del nuevo Reglamento de Fiscalización Regulatoria (RFR), actualmente por la Portaria nº 2.431/2022 (SEI nº 8941316), se aprobó una nueva Instrucción de Fiscalización sobre la comercialización de productos por comercio electrónico.

A pesar de dichas conclusiones, la tesis neutralista de los *marketplaces* colisionaba con el PACP y aún existían tribunales que la adoptaban. Sin embargo, la jurisprudencia fue evolucionando hacia la atribución de deberes de diligencia proactiva a las plataformas, lo que fue pacificado por una decisión reciente del Supremo Tribunal Federal (STF), con

²⁹ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 00453/2021/PFE-ANATEL/PGF/AGU**. Brasília, 2021. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO4t0UuV0d7ERjywGrRjfwWiwaEv5qDiucqzOSkmGuYZGIA6a-B118QiuypPF9Bdki34wmGMyB6GhHGdoEUeFV5_. Acceso en 21 jul. 2025.

repercusión general, dictada en junio de 2025³⁰. El STF decidió que las plataformas de contenido deben crear mecanismos de autorregulación y que los *marketplaces* responden civilmente conforme al Código de Defensa del Consumidor (Ley nº 8.078/1990). El juicio sobre el Art. 19 del Marco Civil de Internet marcó un hito en la responsabilidad de las plataformas digitales por contenidos de terceros, ya que amplió las responsabilidades y obligaciones de las plataformas en cuanto a la moderación y rendición de cuentas sobre las publicaciones realizadas por terceros. Este entendimiento legitima directamente la postura preventiva de Anatel en su actuación frente a los *marketplaces*, otorgando seguridad jurídica a la Agencia en la protección del consumidor y garantizando la equidad competitiva en el sector de telecomunicaciones.

El 1º de agosto de 2025, fundamentada en los dictámenes jurídicos de la Abogacía General de la Unión y alineada con el entendimiento del Supremo Tribunal Federal, Anatel aprobó la revisión del Reglamento de Evaluación de la Conformidad y de Homologación de Productos para Telecomunicaciones mediante la Resolución nº 780, formalizando la responsabilidad solidaria de los *marketplaces* y de las demás plataformas digitales involucradas en el proceso de comercialización, aun cuando actúen únicamente en la divulgación y publicidad, por la oferta de productos para telecomunicaciones no homologados o en desacuerdo con los requisitos técnicos de Anatel. La medida incluye la obligación de divulgar el código de homologación en los anuncios y de verificar la regularidad de los artículos ofertados.

De este modo, los *marketplaces* pasan a responder solidariamente con los vendedores por las infracciones relacionadas con la oferta de productos irregulares, normatizando un entendimiento ya consolidado en decisiones de Anatel y dejando claro que la actuación de estas plataformas va mucho más allá de un simple “escaparate virtual”, constituyendo parte

³⁰ SUPREMO TRIBUNAL FEDERAL (STF) (Brasil). **STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros.** Brasília, 26 jun. 2025. Disponible en: <https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/>. Acceso en: 29 jul. 2025. Nota: acórdão ainda pendente de lavratura em 10 de outubro de 2025.

efectiva de la cadena de comercialización.

2.4.2. Responsabilización de las redes sociales (YouTube y Facebook)

Además de las iniciativas mencionadas dirigidas a la actuación de los *marketplaces*, en el año 2019, ante denuncias de que canales y páginas de YouTube y Facebook estarían difundiendo tutoriales que incentivaban el uso y/o la comercialización de equipos de telecomunicaciones no homologados, la SFI realizó una consulta jurídica a la PFE-Anatel acerca de la posibilidad de actuación.

2019

Dictamen nº 695/2019/PFE ANATEL/PGF/AGU³¹

Consulta:

Fiscalización y sanción de sitios web y youtubers que incentivan el uso y la comercialización de productos no homologados.

Respuesta:

Sí, dado que su competencia está relacionada con la seguridad de los usuarios y con el mantenimiento de un mercado sectorial saludable y competitivo.

Con fundamento en dicho entendimiento, los sitios web, influenciadores digitales y canales de contenido denunciados fueron formalmente notificados para que removieran las publicidades irregulares y publicaran una retractación relativa a la divulgación de mensajes que incentivaban el uso y la comercialización de productos no homologados por Anatel.

³¹ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 00695/2019/PFE-ANATEL/PGF/AGU**. Brasília, 2019. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5Sb4M9fy78errTgNmS1KvYO6MDBaTC20TJyVcVGyXzrRmS0t-IDw7p9ZA-wiumFQdmhpVP6MIDcdohmso_Flu_%20%20. Acceso en 21 jul. 2025.

2.4.3. Responsabilización de la cadena de distribución de productos

Distinción entre correspondencia y encomienda

Otra línea de actuación del Plan de Acción de Combate a la Piratería de Anatel deriva de la cooperación con las actividades de la RFB y de Correos, en la inspección de la importación de productos de telecomunicaciones.

La RFB y Correos, al identificar la tentativa de importación de productos de telecomunicaciones sujetos a homologación, notifican a Anatel para su inspección (por correo electrónico o *WhatsApp*). Tras la selección de los paquetes mediante rayos X (realizada por los empleados de Correos), los envíos escogidos para el análisis de Anatel son abiertos, verificados, fotografiados y evaluados en cuanto a la posibilidad de homologación. En seguida, los embalajes son nuevamente sellados por el fiscal de Anatel y se completa el “formulario de verificación de productos”, que registra los datos de los artículos, el código de rastreo del objeto y su regularidad. Los productos irregulares son comunicados a la RFB respecto a la eventual posibilidad de regularización.

Según la naturaleza del equipo, la Anatel puede emitir un dictamen para autorización de importación, devolución al remitente, retención para regularización o pérdida. Los productos de Categoría I y aquellos que operan conectados a la red eléctrica son generalmente devueltos al origen, mientras que los productos que pueden ser homologados mediante declaración de conformidad reciben un plazo para la regularización. Los productos ilegales, como bloqueadores de señal y decodificadores piratas, son declarados como perdidos.

Es importante destacar que Anatel actúa en nombre de la RFB en este caso, limitándose a verificar la conformidad regulatoria de los equipos, sin realizar actuaciones administrativas.

Ocorre que, tras el inicio de dichas actividades, surgieron dudas jurídicas en relación con la

regularidad del procedimiento adoptado, lo que motivó una consulta jurídica a la PFE-Anatel.

2019

Dictamen nº 770/2019/PFE ANATEL/PGF/AGU³²

Consulta:

Regularidad del procedimiento de apoyo en la inspección de encomiendas.

Respuesta:

Sí, ya que existe una distinción entre correspondencia y encomienda, no habiendo violación del secreto de correspondencia. Además, la Anatel actúa como apoyo técnico a la AFIP-RFB.

La consolidación de las acciones de fiscalización de Anatel, en articulación con la RFB, se ha mostrado un instrumento fundamental en el enfrentamiento a la piratería de productos de telecomunicaciones. El enfoque técnico-operacional basado en inspecciones *in loco*, análisis de conformidad y clasificación sistemática de envíos postales y exprés contribuye a inhibir la entrada, comercialización y uso de equipos irregulares en el país.

Además de proteger a los consumidores frente a los riesgos derivados de productos no certificados, estas acciones fortalecen el mercado formal, garantizan el cumplimiento de las normas técnicas y promueven la competencia leal en el sector de telecomunicaciones. El perfeccionamiento continuo de estos procedimientos —junto con el desarrollo de normas más claras y mecanismos interinstitucionales eficaces— es esencial para la efectividad de la política pública de combate a la piratería tecnológica en Brasil.

³² ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 00770/2019/PFE-ANATEL/PGF/AGU**. Brasília, 2019a. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO7vcSiACcxViZXBtJEqIYo_G5oZ0GTWldJ5bFQIdK3XB0qatznYBYSXvUPbLchNV9NPF5Fr5wuknNblsCUZqEXN. Acceso en 21 jul. 2025.

Responsabilidad por la importación

Aún como resultado de las actividades de fiscalización realizadas en cooperación con la RFB, en el año 2023 se consultó a la PFE-Anatel acerca de la responsabilidad por la operación de importación, en los casos de importación por cuenta y orden de terceros.

2023

Dictamen nº 385/2023/PFE ANATEL/PGF/AGU³³

Consulta:

Responsabilidad por la operación de importación en los casos de importación por cuenta y orden de un tercero.

Respuesta:

La responsabilidad por la infracción de importación de productos no homologados recae sobre el adquirente de la mercadería, y no sobre la empresa importadora contratada.

Relaciones comerciales

Otra cuestión que surgió en las actividades de fiscalización y que demandó un pronunciamiento jurídico de la PFE-Anatel fue la relacionada con las alianzas comerciales celebradas por las empresas titulares de los certificados de homologación expedidos por Anatel, con el fin de permitir la comercialización, en el país, de productos de telecomunicaciones por parte de terceros.

³³ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 00385/2023/PFE-ANATEL/PGF/AGU**. Brasília, 2023. Disponible en: sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqa6i8M5H4M2ICd-In0Ov5885pJq4NQwRwrORFIXmO-AeuSMT701C3h8Xc2ljkSS0nxN_TT-x1yflY6U6Z-DPLZK . Acceso en 21 jul. 2025.

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

Acuerdos comerciales firmados por las empresas titulares de los certificados de homologación emitidos por Anatel.

Respuesta:

No pueden ser utilizados por terceros cuando ello perjudique las responsabilidades del representante comercial en Brasil.
Declaración particular de autorización sometida a registro público.

Posteriormente, la Gerencia de Certificación y Numeración de Anatel (ORCN), de la Superintendencia de Otorgamiento y Recursos a la Prestación (SOR), expidió el Memorando nº 52/2022/ORCN/SOR3535, de 5 de julio de 2022 (SEI nº 8304709), en el que reforzó el entendimiento de la PFE-Anatel manifestado en el Dictamen nº 329/2020/PFE-ANATEL/PGF/AGU y añadió que deberían considerarse válidos cualesquiera medios de prueba (admitidos en derecho) de autorización para la comercialización de productos emitidos por el titular de la homologación al tercero fiscalizado (en posesión del producto comercializado), presentados durante la acción de inspección por la fiscalización de telecomunicaciones, en observancia de la presunción de buena fe del fiscalizado.³⁵

En 2022, una nueva consulta abordó la inclusión del arrendamiento de equipos en el concepto de comercialización.

³⁴ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 00329/2020/PFE-ANATEL/PGF/AGU**. Brasília, 2020. Disponible en:

https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5BzURuP5bhnuacdW_NWcJqJATu7fxFbPmmPsQQNOp8Spe2mTWP5nRw2ylwB4yQmuqdkfNHT6EjUJB25_jBtPM7. Acceso en: 21 jul. 2025.

³⁵ AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendencia de Otorgamiento y Recursos a la Prestación. Gerencia de Certificación y Numeración. **Memorando n.º 52/2022/ORCN/SOR**. Brasília, 2022. Disponible en:

https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO6twY5HXXccmxWop68eTQTqTn9ixgaLS49XCr64tUHCc5brumli3HaJDIhwKGOzPY-2iCX7HynMovVtKoW_wErB. Acceso en: 23 jul. 2025.

2022**Dictamen n° 223/2022/PFE ANATEL/PGF/AGU**³⁶**Consulta:**

Inclusión del alquiler de equipos dentro del concepto de comercialización.

Respuesta:

Sí, encuadrándose en el art. 83, inciso I, del Reglamento (Resolución n.º 715/2019).

Almacenamiento de equipos no homologados

Cuestión que igualmente demandó pronunciamiento de la PFE-Anatel fue la relacionada con el alcance del Art. 83, I, del Reglamento de Evaluación de la Conformidad y de Homologación de Productos para Telecomunicaciones, aprobado por la Resolución n° 715/2019, a la época, en vista de la posesión de equipos no homologados en stock por prestadoras de servicios, aun cuando no estuvieran en uso ni conectados a la red de telecomunicaciones.

³⁶ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 00223/2022/PFE-ANATEL/PGF/AGU**. Brasília, 2022a. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5ax4ZZUq2xuaXLoaMiATdWGelxczd1TqyaqC0PDsQ2KQBdeJJETr0mD_5EQjZWmZoQcKGDxWFWugbgv77UV3fU. Acceso en 21 jul. 2025.

2021**Dictamen nº 454/2021/PFE ANATEL/PGF/AGU**³⁷**Consulta:**

La tenencia de equipos no homologados en stock por prestadoras de servicios, aun cuando no estuvieran en uso o conectados a la red de telecomunicaciones, es pasible de sanción.

Respuesta:

El término “uso” no se limita a la “utilización efectiva”, sino que abarca la función o utilidad potencial de los equipos en stock, generando un beneficio para la prestadora.

Obstrucción a la fiscalización

Otro cuestionamiento formulado a la PFE-Anatel se relacionó con la capacidad de las entidades que fabrican, importan, suministran, distribuyen o comercializan productos para telecomunicaciones de incurrir en la infracción de obstrucción a la actividad de fiscalización de la Agencia, prevista en los Arts. 39 a 41 del Reglamento de Fiscalización Regulatoria, aprobado por la Resolución nº 746, de 22 de junio de 2021.

³⁷ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 00454/2021/PFE-ANATEL/PGF/AGU**. Brasília, 2021a. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLqrlYJw_9INcO68ltWJtJ7YHhYP85DAYRwXLVYefsWGyUfp3DobEpcyWtximBn8o7NqLIGfbu_cwgEdo_tujUfwlH-bKJxFpKKZ. Acceso en 21 jul. 2025.

2022**Dictamen nº 103/2022/PFE ANATEL/PGF/AGU**³⁸**Consulta:**

Práctica de la infracción de obstrucción por distribuidores y comerciantes de productos de telecomunicaciones.

Respuesta:

Sí, dado que la sujeción especial no es imprescindible para el ejercicio de las competencias de Anatel.

Los proveedores pueden obstruir la fiscalización, conforme lo establecido en el Reglamento de Fiscalización Regulatoria.

Inaplicabilidad del principio de consunción

Por último, en el año 2024 se realizó una consulta a la PFE-Anatel sobre la aplicación del principio de consunción en los casos de importación y comercialización de productos para telecomunicaciones no homologados por Anatel. La duda jurídica consistía en determinar si la conducta de importación podría ser jurídicamente absorbida por la de comercialización —considerada una etapa subsecuente del mismo proceso— o si ambas deberían ser tratadas como infracciones autónomas, sujetas a sanciones acumulativas.

³⁸ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 00103/2022/PFE-ANATEL/PGF**. Brasília, 2022. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5sBHBmJmM0fxKRu2a4Qr-PGPvBLNbHPOOdoC0BU3-3lvzfZw6OxT9C7mfgGXwntQyXc5eX5wVKWjddc0HI21S. Acceso en 21 jul. 2025.

2024**Dictamen nº 63/2024/PFE ANATEL/PGF/AGU**³⁹**Consulta:**

Si la conducta de importación podría ser jurídicamente absorbida por la de comercialización.

Respuesta:

No, dado que la importación configura una conducta autónoma, con potencial lesivo propio, y no constituye una etapa necesariamente vinculada a la comercialización.

La imposición acumulativa de ambas conductas no caracteriza “bis in idem”.

Esta interpretación refuerza la actuación regulatoria de Anatel, permitiendo la responsabilización plena de importadores y comerciantes que introducen productos irregulares en el mercado, ampliando la eficacia de los mecanismos de control y represión.

Sinopsis

La actuación de Anatel en el combate a la piratería de productos para telecomunicaciones ha estado fuertemente respaldada por los dictámenes de la PFE-Anatel, los cuales otorgan seguridad jurídica a las acciones de la Agencia.

Inicialmente, los *marketplaces* alegaban neutralidad con base en el Marco Civil de Internet. Sin embargo, con el paso del tiempo, la PFE-Anatel consolidó el entendimiento de que dichas plataformas, al prestar servicios como almacenamiento y entrega, integran la cadena de comercialización y pueden ser responsabilizadas por la oferta de productos no homologados.

³⁹ ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. **Parecer n.º 00063/2024/PFE-ANATEL/PGF/AGU**. Brasília, 2024. Disponible en:

https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqZPZr_MlidKv2NAOXJQ69gtBrT0pFzcupimr_D0SIJIM4dMMIefb5Nlui0BcjfUnUpz93sTE18zCmc569falTP7. Acceso en 21 jul. 2025.

Otros hitos relevantes incluyen el reconocimiento de que la simple oferta o alquiler de productos no homologados constituye comercialización; que minoristas e influenciadores digitales pueden ser responsabilizados; y que el almacenamiento de equipos irregulares igualmente puede dar lugar a sanciones.

La actuación conjunta con la RFB, especialmente en la inspección de envíos postales, también fue jurídicamente legitimada.

Además, la PFE-Anatel descartó la aplicación del principio de consunción entre importación y comercialización, por entender que se trata de conductas distintas, con niveles propios de lesividad.

Con base en estos entendimientos, Anatel estructuró una actuación fiscalizadora proactiva, eficaz y jurídicamente sólida, reforzando su papel en la protección de los consumidores, en la integridad de las redes y en la defensa de la competencia leal en el sector de telecomunicaciones.

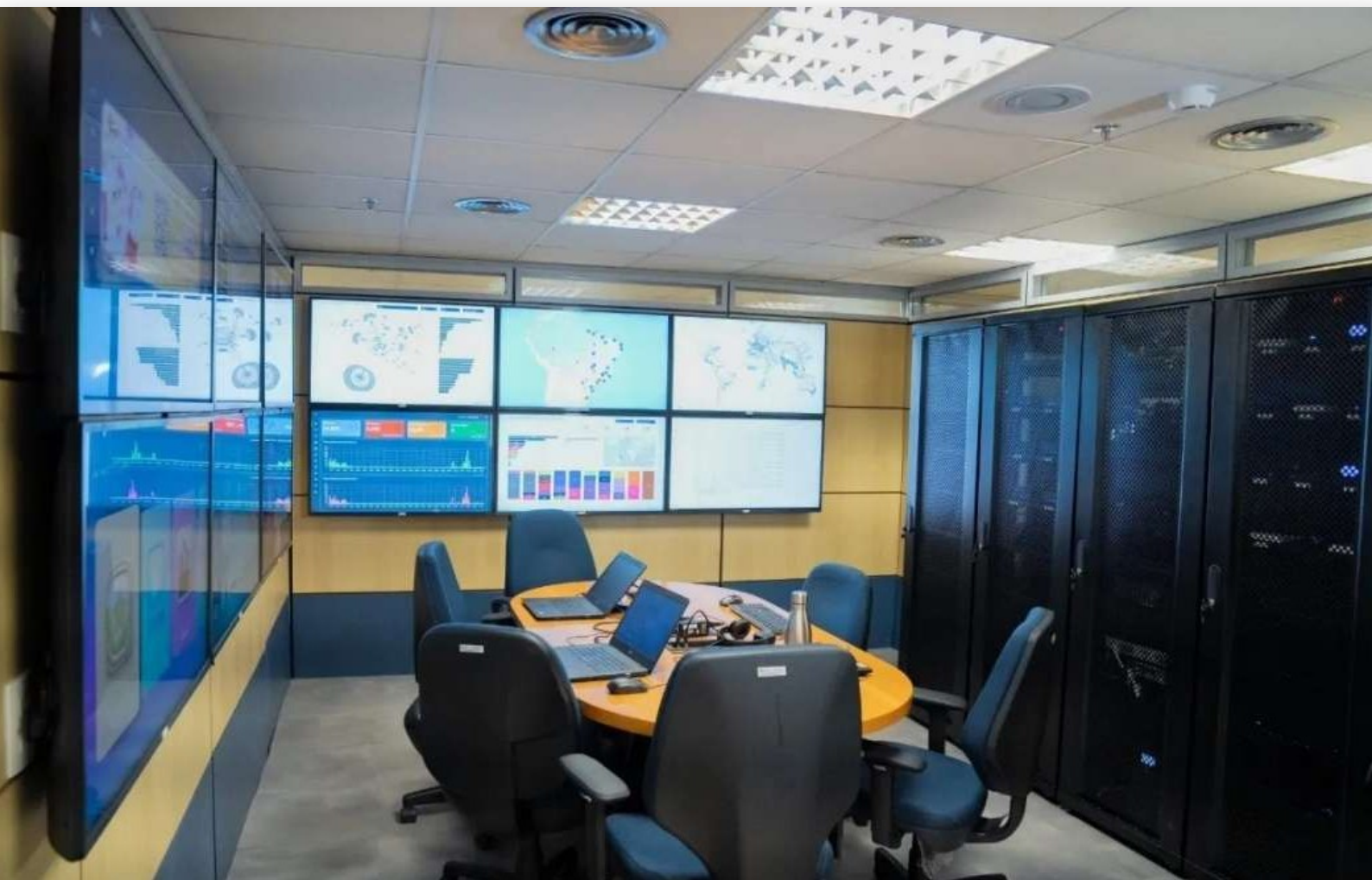
2.5. Plan de Combate al Uso de Decodificadores Clandestinos

La creciente proliferación de decodificadores clandestinos —dispositivos utilizados para acceder ilegalmente a señales de TV por suscripción, contenidos de *streaming* y otros servicios protegidos— constituye uno de los principales desafíos para la integridad del sector de telecomunicaciones en Brasil. Frente a este escenario, la Agencia Nacional de Telecomunicaciones lanzó, en 2023, una iniciativa estratégica de alcance nacional para enfrentar de manera sistemática el uso y la comercialización de estos equipos, ampliando significativamente el alcance y la efectividad de las acciones iniciadas en años anteriores.

La preocupación de Anatel reside en la vulnerabilidad de la red generada por equipos no homologados y en la prestación del Servicio de Acceso Condicionado (nombre técnico para

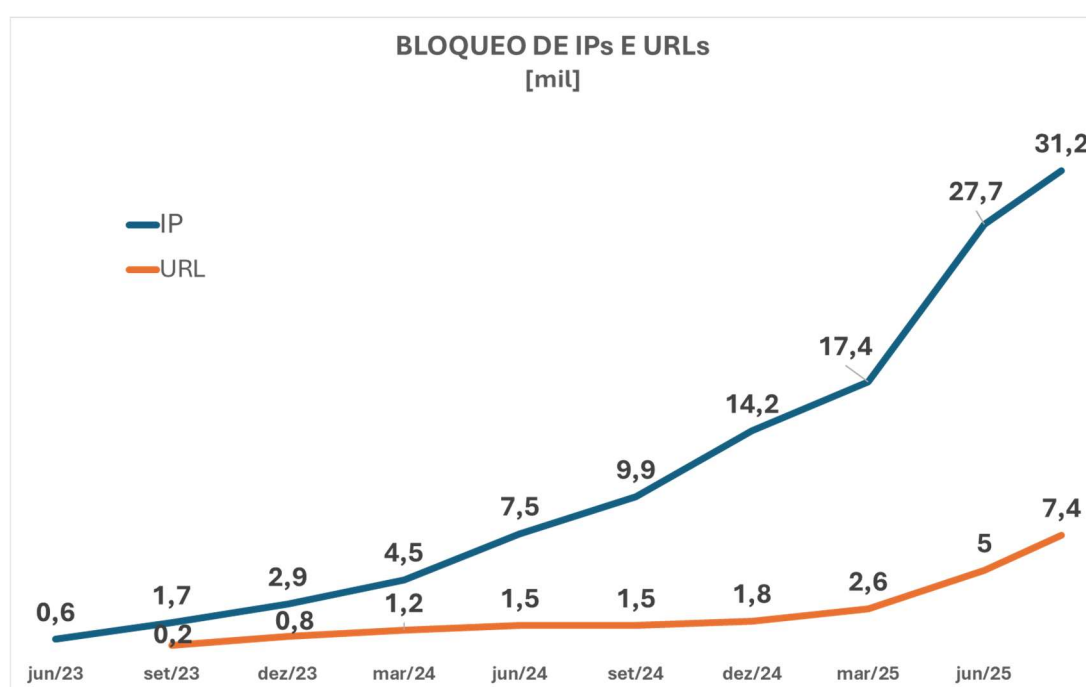
TV por suscripción) sin autorización. Esas preocupaciones llevaron a la celebración del Acuerdo de Cooperación n° 2/2023 entre la Agencia y la ABTA, destinado a estructurar laboratorios para realizar análisis técnicos sobre equipos y otros medios ilegales de oferta audiovisual pirata, con intercambio de información, instituyendo el plan de combate a los decodificadores clandestinos mediante un enfoque integrado que abarca acciones normativas, operativas, preventivas y represivas, protegiendo la infraestructura crítica de telecomunicaciones, la seguridad digital de los consumidores y el equilibrio económico del sector.

El laboratorio cuenta con recursos tecnológicos para realizar y acompañar análisis técnicos sobre equipos y medios ilegales de oferta audiovisual pirata, en cumplimiento del Plan de Acción para Combatir el Uso de Decodificadores Clandestinos del Servicio de Acceso Condicionado (SeAC). La estructura dispone de 12 pantallas de monitoreo, seis puestos de trabajo presencial y acceso remoto.



Además del laboratorio central, hay más de 15 *probes* distribuidos estratégicamente por Brasil, con al menos dos en cada región del país. Esta capilaridad es esencial para acompañar la dinámica operativa de los sistemas piratas, que utilizan tecnologías como CDN (*Content Delivery Network*), servidores *proxy* y redes P2P (*peer-to-peer*) tanto para la autenticación de dispositivos como para la distribución de contenido. La amplia dispersión geográfica de los *probes* permite detectar variaciones regionales en el tráfico, identificar patrones de actuación y garantizar una mayor eficiencia en la recolección de datos para las acciones de combate a la piratería.

El Plan de Acción para el Combate a los Decodificadores Clandestinos monitorea actualmente cerca de 34,1 mil direcciones IP y 8,2 mil URL, mantiene alrededor de 2,7 mil direcciones IP bloqueadas durante determinado período (datos actualizados hasta el 23/08/2025) por estar directamente vinculadas a actividades ilegales, y supervisa decenas de modelos de dispositivos. Este procedimiento se debe al hecho de que las direcciones IP pueden reutilizarse para otros fines lícitos, por lo que se mantienen bajo monitoreo en caso de que vuelvan a emplearse con fines ilegales.



Actualmente, la Agencia está implementando medidas para ampliar el Plan de Acción para el Combate a los Decodificadores Clandestinos, como la automatización de las órdenes de bloqueo para los proveedores de Internet y los proveedores de cables submarinos (que pasarán a recibir el comando en tiempo real, tan pronto como las direcciones sean identificadas por la Agencia).

Las acciones de combate a la piratería en Brasil cuentan con un respaldo jurídico relevante, lo que permite que denuncias fundamentadas sean acogidas por el Ministerio Público y resulten en acciones efectivas, como la retirada del aire de grupos en aplicaciones de mensajería (como Telegram y WhatsApp), canales en plataformas de video (como YouTube) y sitios web que promueven la actualización y el uso de decodificadores clandestinos de IPTV.

Estas denuncias se sustentan en disposiciones legales que tipifican como delito la realización de actividades destinadas a la distribución no autorizada de contenido protegido por derechos de autor, así como el favorecimiento del uso de equipos clandestinos que violan el sistema jurídico establecido y mantenido por Anatel. Entre los principales fundamentos jurídicos utilizados, se destacan:

Ley n.º 9.472/1997 (Ley General de Telecomunicaciones)

Prohíbe la explotación de servicios de telecomunicaciones sin la debida autorización, siendo aplicable a los casos de uso de decodificadores no homologados o manipulados para captar señales de TV por suscripción de forma ilegal.

Ley n.º 12.965/2014 (Marco Civil de Internet)

Responsabilidad de los intermediarios y obligación de cumplir órdenes judiciales para la remoción de contenidos ilícitos.

Ley n.º 8.078/1990 (Código de Defensa del Consumidor)

Protección del consumidor como uno de los desdoblamientos de los derechos fundamentales constitucionales (decisión reciente del STF en los RE 1037396 y RE 1057258, que determina que los marketplaces responden civilmente de acuerdo con el CDC, incluso por actos de terceros que utilizan sus plataformas).

El Ministerio Público, al recibir representaciones técnicas y pruebas documentadas —como capturas de pantalla, informes de tráfico, registros de ventas y tutoriales ilegales— puede solicitar judicialmente el bloqueo o la retirada del contenido, con el apoyo técnico de Anatel para la identificación de servidores, dominios y dispositivos involucrados.

Esta cooperación fortalece las acciones de Anatel en el marco de su Plan de Acción para el Combate al Uso de Decodificadores Clandestinos del SeAC, garantizando que las medidas administrativas, como la incautación de equipos y la suspensión de homologaciones, sean complementadas por medidas judiciales que alcancen las redes de apoyo y difusión de la piratería, tanto en el entorno físico como digital.

La combinación de estas estrategias —jurídicas, técnicas y operativas— ha demostrado ser eficaz para debilitar las estructuras de la piratería y proteger el ecosistema audiovisual legal, preservando los derechos de los productores, distribuidores y operadores de contenido.

Investigaciones han demostrado⁴⁰ que acciones que hacen que el contenido legal sea más atractivo para los usuarios o que hacen que el contenido ilegal sea menos atractivo pueden llevar a que los piratas migren hacia el contenido legal. A pesar de la dificultad para cuantificar el mercado de los *set-top boxes* irregulares, ya se observan efectos de las acciones de Anatel, con los principales modelos de dispositivos ilegales comenzando a cobrar por el acceso al contenido pirata, y con empresas de *set-top boxes* certificadas por Anatel invirtiendo en el desarrollo y producción de equipos⁴¹.

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. Disponible en: <https://www.journals.uchicago.edu/doi/full/10.1086/674020>. Acceso en: 19 may 2025.

⁴¹ Proeletronic expõe o SmartPRO 4K, TV box com homologação da Anatel para provedores e IPTV. **Revista RTI (Aranda Net)**, São Paulo, actualizado en 14 jun. 2024. Disponible en: <https://www.arandanet.com.br/revista/rTI/noticia/8998-Proeletronic-expoe-o-SmartPRO-4K,-TV-box-com-homologacao-da-Anatel-para-provedores-e-IPT>. Acceso en: 07 jul. 2025.

A lo largo del tiempo, Anatel ha recibido 5 premios de Combate a la Piratería otorgados por el Consejo Nacional de Combate a la Piratería (CNCP), entregados por el Ministerio de Justicia y Seguridad Pública, en reconocimiento a sus acciones de combate a la piratería en el sector de telecomunicaciones.

En 2024, Anatel recibió un premio de reconocimiento de la Unión Internacional de Telecomunicaciones. El proyecto del Plan de Acción para el Combate a los Decodificadores Clandestinos fue inscrito en la categoría “Entorno Habilitador” (*Enabling Environment*) del Premio WSIS 2024 – World Summit on the Information Society, quedando entre los cuatro ganadores de la categoría, compitiendo con proyectos de todo el mundo presentados por empresas, reguladores y gobiernos.



Ancine

En 2025, se firmó un nuevo Acuerdo de Cooperación Técnica entre la Agencia Nacional de Cine (Ancine) y la Anatel, con el objetivo de establecer un flujo de comunicación ágil y

directo, por medio electrónico, entre ambos organismos, para el envío por parte de la Anatel de decisiones emitidas por la Ancine que determinan la suspensión y el cese del uso no autorizado de obras brasileñas y extranjeras protegidas, a través de sitios web.

Desde la celebración del acuerdo, ya se han bloqueado 684 direcciones IP durante un período determinado (datos actualizados hasta el 12 de julio de 2025) y 159 dominios que promovían el uso no autorizado de obras brasileñas y extranjeras protegidas, en desacuerdo con la legislación aplicable.



3. ACCIONES DE COMBATE A LA PIRATERÍA EN OTRAS ADMINISTRACIONES

El combate a la piratería de productos de telecomunicaciones es una preocupación creciente y compartida por administraciones y organismos reguladores de todo el mundo. El avance tecnológico, la digitalización de los servicios y la expansión del comercio electrónico internacional han creado un ambiente propicio para la proliferación de dispositivos irregulares y redes clandestinas de distribución de contenido, exigiendo respuestas coordinadas, modernas y eficaces por parte de las autoridades regulatorias.

Diversos países han desarrollado estrategias sólidas para contener la circulación de productos robados, falsificados y no certificados, así como el acceso ilegal a contenidos protegidos por derechos de autor y la manipulación de infraestructuras críticas de telecomunicaciones. Estas experiencias internacionales ofrecen referencias valiosas para la actuación de la Anatel y demuestran el papel fundamental de las agencias reguladoras en la defensa del interés público y la integridad del ecosistema digital.

3.1. Combate a la piratería en *e-commerce*

En los últimos años, el crecimiento exponencial del comercio electrónico, combinado con la complejidad de la cadena logística global, ha impulsado la proliferación de productos falsificados y no certificados en diversas plataformas digitales. Frente a este escenario, distintas autoridades internacionales han desarrollado mecanismos de cooperación y fiscalización para mitigar los impactos de la piratería sobre la economía, la seguridad del consumidor y la integridad de sectores estratégicos. En este contexto, se destacan las iniciativas lideradas por el Departamento de Seguridad Nacional de los Estados Unidos (Homeland Security Investigations – HSI) y por Europol, en Europa.

Estados Unidos

En Estados Unidos, Homeland Security, por medio de su brazo de Investigaciones de Seguridad Nacional (HSI), ha actuado de forma sistemática en operaciones conjuntas con el sector privado, autoridades aduaneras y agencias reguladoras. Entre las principales acciones adoptadas se encuentran el refuerzo de la responsabilización de las plataformas en línea, exigiendo que implementen políticas de verificación de vendedores, trazabilidad de la cadena de suministro, eliminación proactiva de anuncios ilegales y mayor cooperación con las autoridades aduaneras. El informe también recomienda medidas como inspecciones aduaneras más rigurosas, bloqueo de remesas de productos falsificados y sanciones contra vendedores reincidentes, promoviendo un enfoque integrado entre gobierno y sector privado para proteger a los consumidores y fortalecer la integridad del comercio digital⁴².

Europa

En Europa, Europol coordina operaciones transnacionales como la Operation Fake Star, dirigida a reprimir la piratería digital y física en múltiples sectores, incluidos los electrónicos y de telecomunicaciones. A través de asociaciones con aduanas, plataformas en línea y autoridades nacionales, estas operaciones han resultado en incautaciones significativas, eliminación de contenido ilícito y bloqueo de redes de distribución. Las acciones europeas también enfatizan el uso de inteligencia artificial para identificar patrones de fraude, ampliando la capacidad de respuesta de las agencias involucradas.

La Operación Fake Star fue lanzada en 2022 en el ámbito de la Acción Operativa (A.O.) 3.4 de EMPACT. La Acción Operacional 3.4 forma parte de un plan de acción específico dentro

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.** Disponible en: https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf. Acceso en: 14 jun. 2025.

de la Plataforma Multidisciplinar Europea contra las Amenazas Criminales^{43,44} (EMPACT), centrado en la cooperación policial. EMPACT es una iniciativa de la Unión Europea que reúne a diversas autoridades policiales, agencias y socios para combatir el crimen organizado y grave.

Las operaciones de EMPACT están previstas en el Documento de Programación de Europol, elaborado con base en el artículo 12 del Reglamento de Europol⁴⁵ y en los artículos 32 y 33 del Reglamento Financiero^{46,47} aplicable a Europol.

Pionerismo de Anatel en Brasil

Si bien estas acciones internacionales son, en su mayoría, amplias y aplicadas a distintos segmentos del mercado, Brasil se ha destacado mediante un enfoque pionero y sectorial, liderado por la Agência Nacional de Telecomunicações (Anatel). Anticipándose a una actuación aún incipiente en el enfrentamiento a la piratería en el comercio electrónico en el país, Anatel ha promovido acciones específicas para combatir la comercialización irregular de productos de telecomunicaciones, especialmente en plataformas digitales.

Por medio del Plan de Acción de Combate a la Piratería, lanzado en 2018, Anatel ha

⁴³ ESTADOS UNIDOS DA AMÉRICA (EUA). **United States Code. Title 18. Part I. Chapter 1. Section 18 - Organization defined.** Disponible en : <https://www.law.cornell.edu/uscode/text/18/18>. Acceso en: 19 jun. 2025.

⁴⁴ COUNCIL OF THE EUROPEAN UNION (União Europeia). **EMPACT Terms of Reference.** Bruselas: 2023. Disponible en: <https://data.consilium.europa.eu/doc/document/ST-8975-2023-INIT/en/pdf>. Acceso en: 19 jun. 2025.

⁴⁵ EUROPOL (União Europeia). **Europol Programming Document 2025 – 2027.** Haia: 2024. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2025-2027.pdf. Acceso en: 14 jun. 2025.

⁴⁶ UNIÃO EUROPEIA (UE). **Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022.** Estrasburgo: 2022. Disponible en: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2022.169.01.0001.01.ENG. Acceso en: 14 jun. 2025.

⁴⁷ UNIÃO EUROPEIA (UE). **Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012.** Estrasburgo: 2012. Disponible en: https://www.epo.org/en/legal/up-upc/2022/upcaannexi_ciii.html. Acceso en: 14 jun. 2025.

articulado una estrategia integrada que involucra monitoreo automatizado de *marketplaces*, notificación a vendedores, remoción de anuncios irregulares, incautaciones en puntos físicos y alianzas con órganos como la *Secretaría de Ingresos Federales de Brasil*, Policía Federal, Procons y plataformas de comercio electrónico. Estas iniciativas colocan a Brasil en una posición de vanguardia en la regulación sectorial frente al desafío de la piratería digital, con resultados expresivos tanto en la protección del consumidor como en la garantía de calidad y conformidad de los productos comercializados.

Así, aunque EE.UU y Europa presentan estructuras sólidas y articuladas en el combate a la piratería en ambientes digitales, la actuación de Anatel se diferencia por su especialización, enfoque técnico y coordinación interinstitucional orientada al sector de telecomunicaciones. Este carácter pionero brasileño demuestra la importancia de iniciativas regulatorias específicas, reforzando la necesidad de fortalecer la gobernanza digital en mercados clave, con miras a la protección del interés público, la innovación tecnológica y la seguridad de las redes de telecomunicaciones en el país.

3.2. Combate al uso de equipos no homologados

En cuanto al combate al uso y comercio de productos no homologados y equipos de telecomunicaciones falsificados, se presentan a continuación algunas de las acciones adoptadas por diferentes administraciones.

Estados Unidos

En Estados Unidos, la fiscalización de equipos de telecomunicaciones es realizada principalmente por la Federal Communications Commission (FCC), que es el organismo regulador del sector. La FCC establece normas y reglamentos para garantizar la seguridad, la compatibilidad y la calidad de los equipos utilizados en el país. Además, otras agencias y leyes desempeñan un papel en la fiscalización, en conformidad con la Ley de Asistencia en

Comunicaciones para la Aplicación de la Ley⁴⁸ (CALEA) y la Ley de Telecomunicaciones de 1996⁴⁹.

La certificación FCC es un proceso obligatorio en Estados Unidos para garantizar que los equipos de telecomunicaciones, incluidos los dispositivos inalámbricos, cumplan con los estándares técnicos y las regulaciones establecidas por la FCC⁵⁰. Esta certificación tiene como objetivo asegurar la seguridad, la compatibilidad con otros dispositivos y la ausencia de interferencias con las redes de comunicación. La certificación FCC es esencial para que los fabricantes puedan comercializar sus productos en los EE.UU.

La FCC supervisa el cumplimiento continuo de los equipos certificados y puede adoptar medidas contra empresas que no respeten los estándares y tienen autoridad para bloquear la venta de equipos de empresas extranjeras que representen riesgos para la seguridad nacional. Cada equipo certificado recibe un código FCC ID, que permite identificar al fabricante y al modelo del dispositivo.

La FCC también desempeña un papel en la garantía de la neutralidad de la red y en la fiscalización de interrupciones en los servicios de internet, con el fin de asegurar la adecuada prestación de los servicios.

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. Disponible en: <https://www.govinfo.gov/content/pkg/COMPS-937/uslm/COMPS-937.xml>. Acceso en: 14 jun. 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. Disponible en: <https://www.govinfo.gov/content/pkg/COMPS-959/uslm/COMPS-959.xml>. Acceso en: 14 jun. 2025.

⁵⁰ FEDERAL REGISTER (Estados Unidos da América). **Code of Federal Regulations**. Title 47 - Telecommunication, as of June 14th, 2025. Washington (DC): 2025. Disponible en: <https://www.ecfr.gov/on/2025-06-14/title-47>. Acceso en: 14 jun. 2025.

Japón

La legislación aplicable a la certificación de equipos de telecomunicaciones en Japón se basa principalmente en dos leyes: la Ley de Radio⁵¹ y la Ley de Telecomunicaciones⁵². La certificación es emitida por el Ministerio de Asuntos Internos y Comunicaciones (MIC). Dependiendo de las características del equipo, se puede aplicar uno o ambos regímenes de certificación. La certificación garantiza que los equipos cumplan con las leyes y los reglamentos japoneses, incluidos los requisitos de seguridad y de compatibilidad electromagnética (EMC). La falta de certificación impide la comercialización legal de los equipos en el mercado japonés.

La fiscalización de equipos de telecomunicaciones en Japón es realizada por el Ministerio de Asuntos Internos y Comunicación (MIC). Este ministerio es responsable de garantizar el cumplimiento de la Ley de Radio y de la Ley de Telecomunicaciones de Japón. Los equipos de radio y telecomunicaciones destinados al mercado japonés deben someterse a un proceso de certificación obligatorio.

Japón también mantiene una atención especial sobre cuestiones de seguridad cibernética y privacidad de los datos, especialmente en relación con equipos de telecomunicaciones de origen extranjero. En algunos casos, el gobierno puede solicitar a las empresas adopten precauciones adicionales en la adquisición de equipos que puedan representar riesgos de seguridad.

⁵¹ JAPÓN. **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. Disponible en: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_5.pdf. Acceso en: 14 jun. 2025.

⁵² JAPÓN. **Telecommunications Business Law** (Law No. 86 of December 25, 1984) - as amended last by: Law No. 125 of July 24, 2003. Tóquio, 2003. Disponible en: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/TBL/TBL-index.html. Acceso en: 14 jun. 2025.

Europa

La Directiva de Equipos Radioeléctricos (RED) 2014/53/UE⁵³ establece un marco regulatorio para la introducción de equipos radioeléctricos en el mercado. Garantiza un mercado único para estos equipos, estableciendo requisitos esenciales de seguridad y salud, compatibilidad electromagnética y uso eficiente del espectro radioeléctrico. También proporciona la base para reglamentaciones adicionales que rigen otros aspectos, incluidos requisitos técnicos para la protección de la privacidad, de los datos personales y contra fraudes. Además, se abordan otros aspectos como la interoperabilidad, el acceso a los servicios de emergencia y la conformidad en la combinación de equipos radioeléctricos y *software*.

La certificación de equipos de telecomunicaciones en Europa es un proceso regulado para garantizar la seguridad, el desempeño y el cumplimiento de las normas europeas. La marca CE, junto con la Directiva de Equipos Radioeléctricos (RED), desempeña un papel crucial en la certificación de dispositivos de comunicación y de equipos que utilizan radiofrecuencia.

El artículo 45 de la RED crea el comité de evaluación de la conformidad y de fiscalización del Mercado de las telecomunicaciones (TCAM), un comité relacionado con el Reglamento (UE) n.º 182/2011.⁵⁴ El TCAM emite dictámenes sobre los actos de ejecución propuestos en el marco de la RED.

África

En Botsuana, la Ley de Regulación de las Comunicaciones de 2012 exige que todos los

⁵³ UNIÓN EUROPEA (UE). **Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014**. Estrasburgo, 2014. Disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053>. Acceso en: 14 jun. 2025.

⁵⁴ UNIÓN EUROPEA (UE). **Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011**. Estrasburgo, 2011. Disponible en: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32011R0182>. Acceso en: 14 jun. 2025.

autorizados, fabricantes y distribuidores aprueben sus dispositivos de comunicación electrónica antes de su conexión a la red pública.⁵⁵

En Ghana, el organismo regulador está legalmente obligado a certificar y probar los equipos de comunicación para verificar su conformidad con las normas internacionales de salud y seguridad.⁵⁶

3.3. Combate a la conexión de equipos no homologados y al acceso a contenido

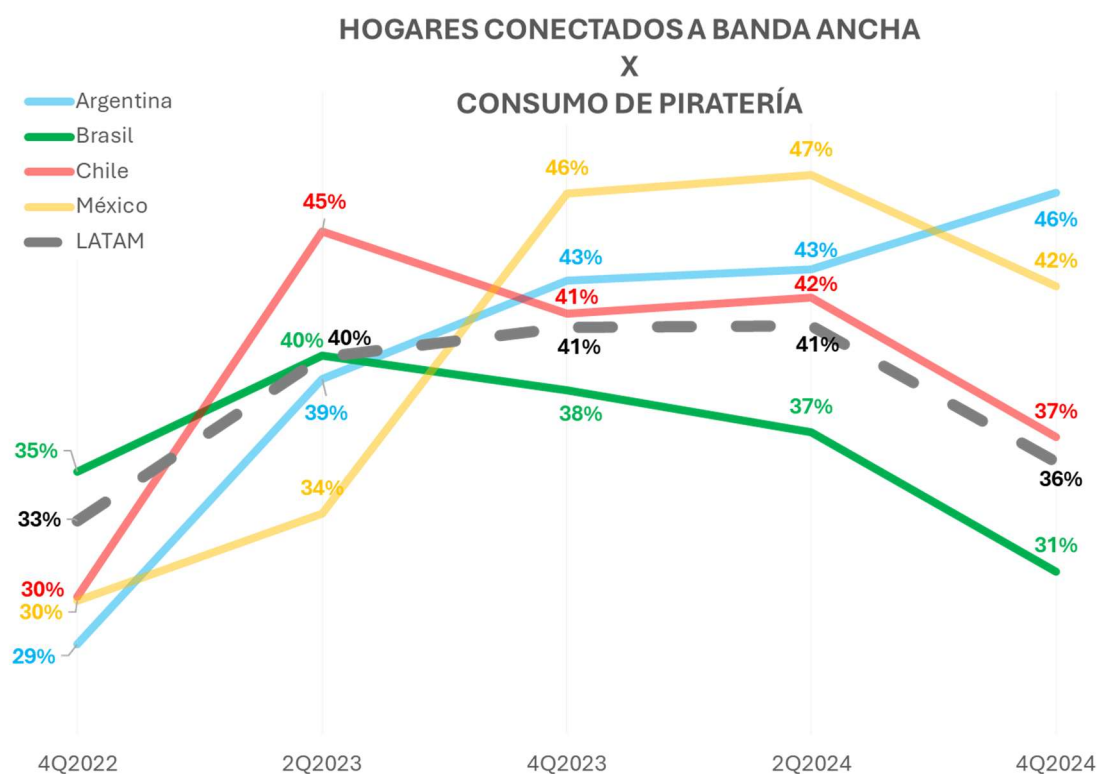
La Anatel actúa en el bloqueo de *set-top boxes* irregulares, con el objetivo de proteger la infraestructura nacional de telecomunicaciones y a los usuarios de telecomunicaciones frente a amenazas cibernéticas. El bloqueo de *set-top boxes* irregulares se lleva a cabo en línea con el Plan de Combate a la Piratería, ya que se realiza sobre dispositivos fiscalizados por el PACP.

Brasil redujo el consumo de piratería audiovisual en línea en hogares conectados por banda ancha a internet en el año 2024. De acuerdo con el último informe de la Alianza contra la Piratería Audiovisual (Alianza), el índice de hogares que accedieron a contenido ilegal cayó del 39,7% en el segundo trimestre de 2023 al 36,8% en el mismo período de 2024, entre los 43,9 millones de residencias conectadas a internet⁵⁷.

⁵⁵ UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES (UIT). **Agreement - draft Supplement Q.Suppl.75. 2021**. Disponible en: <https://www.itu.int/md/T17-SG11-211201-TD-GEN-1800/en>. Acceso en: 23 jul. 2025.

⁵⁶ UIT, 2021.

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



Administraciones de otros países realizan el bloqueo de piratería de contenido ilegal que, además, afecta a *set-top boxes* que transmiten dicho contenido; sin embargo, Anatel es pionera en este tipo de acción, ya que actúa únicamente sobre los dispositivos, impidiéndoles conectarse a los servidores, sin bloquear nunca el contenido que circula a través de ellos. Estudios internacionales, como el realizado por Human Security⁵⁸, confirman que diversas administraciones de otros países se interesan en el trabajo desarrollado en Brasil.

A continuación, se presentan las formas de actuación de otras administraciones que comparten el mismo objetivo de la Anatel de proteger la red de telecomunicaciones nacional

⁵⁸ SATORI THREAT INTELLIGENCE AND RESEARCH TEAM, 2025.

Estados Unidos

A ACE (Alliance for Creativity and Entertainment) lleva a cabo acciones contra empresas que facilitan el acceso a señales de TV por suscripción sin licencia, imponiendo multas millonarias, cancelación de licencias y bloqueos judiciales^{59,60}.

Reino Unido

En el Reino Unido, el combate a la piratería se realiza mediante la colaboración entre Office of Communications – Ofcom (el órgano regulador de comunicaciones) y la Unidad de Delitos contra la Propiedad Intelectual (PIPCU), vinculada a la Policía Metropolitana de Londres. Las acciones combinan fiscalización física, operaciones contra redes ilegales de IPTV, bloqueo de dominios y campañas públicas de concienciación.

Los tribunales del Reino Unido conceden medidas cautelares para bloquear eventos deportivos en directo, *cyberlockers* piratas y sitios de *streaming*^{61,62} desde 2011. Un *cyberlocker* es, esencialmente, un servicio de alojamiento de archivos similar a un servicio legítimo de almacenamiento en la nube, como Dropbox, pero que operadores de piratería utilizan para permitir a los usuarios cargar y descargar contenido que viola derechos de

⁵⁹ BROADBAND TV NEWS CORRESPONDENT. Anti-piracy alliance ACE settles copyright infringement cases with IPTV operators. **Broadband TV News**, 17 ago. 2024. Disponible en: <https://www.broadbandtvnews.com/2024/ago.17/anti-piracy-alliance-ace-settles-copyright-infringement-cases-with-iptv-operators/>. Acceso en: 07 jul. 2025.

⁶⁰ BRIEL, Robert. ACE takes legal action against IPTV pirates. **Broadband TV News**, 11 mar. 2025. Disponible en: <https://www.broadbandtvnews.com/2025/03/11/ace-takes-legal-action-against-iptv-pirates/>. Acceso en: 07 jul. 2025.

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

⁶² ENGLAND AND WALES HIGH COURT (Reino Unido). Chancery Division. **Matchroom Boxing Ltd & Anor v British Telecommunications Plc & Ors** (Decision). Londres, 20 set. 2018. Disponible en: <https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2018/2443.html&query=IL-2018-000155+>. Acceso en: 23 jul. 2025.

autor. Los *cyberlockers* de piratería permiten cargar/descargar material ilegal de forma gratuita y recompensan a los usuarios que suben contenido ilegal, permitiéndoles ganar dinero cada vez que su archivo es descargado. Los operadores de piratería permiten que los usuarios creen enlaces URL compartibles para facilitar el acceso de terceros al contenido pirateado.⁶³.

Según estudios de Danaher *et al.*⁶⁴, cuando 19 de los principales sitios de piratería fueron bloqueados simultáneamente entre octubre y noviembre de 2013, hubo una fuerte reducción en los niveles totales de piratería, lo que llevó a los usuarios de esos sitios bloqueados a aumentar el uso de plataformas legales de *streaming* de pago en un 11%. El bloqueo de 53 sitios en 2014 provocó que los usuarios disminuyeran la piratería y aumentaran el uso de sitios legales de suscripción entre un 7% y un 12%.

Europa

La Unión Europea promueve una actuación integrada a través del EUIPO (European Union Intellectual Property Office) y del Europol (*Agência da União Europeia para Cooperação Policial*), coordinando campañas conjuntas con administraciones nacionales para combatir la piratería digital. El proyecto "*IPTV Crime and Enforcement*" es un ejemplo de iniciativa transfronteriza que abarca incautación de equipos, rastreo de transacciones financieras y desarticulación de redes organizadas que operan IPTV pirata en varios países de la UE.

El bloqueo de sitios web para aplicar derechos de autor es legalmente posible en toda la

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

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

UE⁶⁵, pero utilizado activamente sólo en un subconjunto de Estados miembros. Diversas decisiones del Tribunal de Justicia de la Unión Europea (TJUE), a máxima instancia judicial de la UE, han aclarado su uso como herramienta válida contra la piratería. Aunque estas decisiones judiciales respaldan la disponibilidad del bloqueo dinámico —bloqueando sitios espejo y *proxies*, así como la dirección IP principal—, solo están disponibles las medidas cautelares estáticas en todos los Estados miembros. Irlanda, España y el Reino Unido llevaron esta práctica un paso más allá e implementaron medidas cautelares de bloqueo en tiempo real.

En 2021, Alemania creó la Clearingstelle Urheberrecht im Internet (CUII), una iniciativa conjunta de titulares de derechos de autor (de los sectores de música, cine, juegos y publicaciones científicas), asociaciones industriales, proveedores de internet (ISP), expertos jurídicos y el gobierno, destinada a gestionar de manera más eficiente el bloqueo de sitios que infringen sistemáticamente los derechos de autor, además de tener en cuenta los requisitos de neutralidad de la red. Todas las decisiones están sujetas a revisión judicial y a la revisión por parte de la *Bundesnetzagentur* (BNetzA), la Agencia Federal de Redes de Alemania, responsable de aplicar los requisitos de neutralidad de la red. Esto refuta otra crítica infundada: la de que el bloqueo de sitios perjudica la neutralidad de la red. La BNetzA considera las implicaciones relativas a la neutralidad de la red en cada solicitud de bloqueo⁶⁶.

En diciembre de 2024, la Oficina Federal de Seguridad de la Información de Alemania (BSI) llevó a cabo una operación contra la *botnet* BadBox 2.0, que infectaba dispositivos Android y *smart* TVs. La *botnet*, ya presente de forma preinstalada en diversos aparatos como set-

⁶⁵ UNIÓN EUROPEA (UE). **Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019**. Estrasburgo, 2019. Disponible en: <https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng>. Acceso en: 16 jun. 2025.

⁶⁶ HOMANN, Jochen. **Online Copyright Clearance System arranges block of streaming site**. Bonn: Bundesnetzagentur, 11 mar. 2021. Disponible en: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2021/20210311_Clearingstelle.html. Acceso en: 23 jul. 2025.

top boxes, tabletas y sistemas vehiculares, tuvo su comunicación interrumpida en aproximadamente 30 mil dispositivos durante la primera fase de la operación.⁶⁷

La Sección 60c de la Ley de Derechos de Autor de Finlandia proporciona el marco legal para que un ISP bloquee el acceso a sitios infractores.⁶⁸ Finlandia bloqueó *The Pirate Bay* por primera vez en 2011.

En Italia, el bloqueo de sitios se hizo posible con la implementación del Artículo 8.3 de la Directiva de Derechos de Autor de la UE⁶⁹, de la ley penal y de un procedimiento administrativo especial (Reglamento de la AGCOM), que entró en vigor a finales de marzo de 2014. De acuerdo con el reglamento, la AGCOM (la autoridad reguladora nacional de comunicaciones) tiene la facultad de ordenar a los ISP que bloqueen el acceso a sitios infractores tras considerar una denuncia presentada por un titular de derechos, y existe un procedimiento "acelerado" para los sitios responsables de violaciones masivas de derechos de autor.

Canadá

El CRTC (*Canadian Radio-television and Telecommunications Commission*) mantiene una actuación firme en defensa de la propiedad intelectual y de la integridad de las redes de telecomunicaciones. El organismo tiene autoridad para determinar el bloqueo de sitios piratas y coordinar con los ISP (*Internet Service Providers*) las acciones de desactivación de servicios clandestinos. El programa "*FairPlay Canada*", lanzado con el apoyo de empresas de medios, operadoras y entidades civiles, tiene como objetivo combatir el *streaming* ilegal

⁶⁷ SATORI THREAT INTELLIGENCE AND RESEARCH TEAM, 2025.

⁶⁸ FINLANDIA. **Copyright Act (Act No. 404/1961 of July 8, 1961, as amended up to Act No. 608/2015 of May 22, 2015)**. 2015. Disponible en: <https://www.wipo.int/wipolex/en/legislation/details/15992>. Acceso en: 23 jul. 2025.

⁶⁹ UE, 2019.

mediante listas de bloqueo mantenidas por decisión judicial y con el apoyo técnico de los proveedores.

Ásia

Japón aplica sanciones severas a quienes compartan o comercialicen dispositivos capaces de vulnerar sistemas de encriptación de contenido.

En Corea del Sur, el bloqueo de sitios es posible mediante un procedimiento administrativo que involucra a autoridades gubernamentales. De acuerdo con las informaciones disponibles por *World Intellectual Property Organization* (WIPO)⁷⁰. A principios de 2021, más de 180 dominios se habían bloqueado, incluidos sitios populares de BitTorrent y *cyberlockers*. En enero de 2019, la Comisión de Normas de Comunicación de Corea (KCSC) lanzó un nuevo centro para gestionar más rápidamente las solicitudes de bloqueo de sitios, como parte de su misión general de combatir la pornografía infantil, la piratería de vídeos y los juegos de azar ilegales.

Australia

El 22 de junio de 2015, el gobierno australiano promulgó la Enmienda de Derechos de Auto^{71,72} (Infracción en Línea). La Sección 115A de la Enmienda otorga al tribunal federal de Australia el poder de emitir una orden cautelar para exigir que un ISP bloquee el acceso a "ubicaciones en línea", incluso fuera de Australia, cuyo objetivo principal sea infringir o facilitar la violación de derechos de autor. "Localización en línea" se utilizó como un término

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. Disponible en: <https://www.legislation.gov.au/C2015A00080/latest/text>. Acceso en: 23 jul. 2025.

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

intencionalmente amplio que incluye, pero no se limita a, sitios web, además de adaptarse a tecnologías futuras. Actualmente, los titulares de derechos de autor y los ISP pueden acordar, de forma privada, ampliar la medida cautelar para incluir cualquier nuevo sitio que aloje el mismo material infractor de la orden judicial original, sin necesidad de acudir nuevamente a los tribunales para obtener una nueva medida. Del mismo modo, las herramientas de búsqueda como Google y Bing son responsables de eliminar los enlaces a los sitios bloqueados, así como a sus espejos y *proxys*.

Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior: December 2018⁷³, el tráfico hacia los sitios de visualización de contenido legal aumentó un 5% en el período posterior a los bloqueos.

3.4. Alianzas multilaterales y Foro Global

Organismos internacionales como la Unión Internacional de Telecomunicaciones (UIT) y la Organización Mundial de la Propiedad Intelectual (OMPI) promueven el intercambio de buenas prácticas entre administraciones y fomentan el desarrollo de normas técnicas comunes. La UIT, en particular, reconoce la piratería como un riesgo para la resiliencia de las redes y para la soberanía digital de los países, y recomienda la adopción de políticas nacionales integradas para combatir la circulación de equipos no conformes.

La Anatel, en el ejercicio de su competencia de representar internacionalmente a Brasil en los temas de telecomunicaciones, actúa de manera activa ante la UIT, incluso liderando el debate a nivel internacional con la elaboración del Informe Técnico ITU-T QSTR-MCM-UC⁷⁴, que aborda los casos de uso para combatir la apropiación indebida de contenido

⁷³ MPA, 2020.

⁷⁴ UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). **LS on the agreement of Technical Report ITU-T QSTR-MCM-UC "Use Cases on the combat of Multimedia Content Misappropriation"**. 2024. Disponible en: <https://www.itu.int/md/T22-SG16-240415-TD-GEN-0295/en>. Acceso en: 23 jul. 2025.

multimedia, y con la propuesta de la nueva Recomendación sobre el combate contra la apropiación indebida de contenido multimedia (Rec. ITU-T Q.FC-MCM), en el ámbito de la Comisión de Estudios 11 del Sector de Normalización de la UIT⁷⁵.

Diversos países miembros de la Unión Internacional de Telecomunicaciones (UIT) están buscando implementar métodos y soluciones regulatorias para combatir los teléfonos móviles robados y falsificados. Estas iniciativas se basan en gran medida en las Recomendaciones UIT-T Q.5050 y Q.5051, que contaron con la participación activa de la administración brasileña en su elaboración, especialmente con las contribuciones de Anatel.

De esta forma, lo que se observa a partir de los estudios y de los trabajos realizados por otros países es que existen esfuerzos con similitudes de procesos en el combate a los teléfonos móviles robados o falsificados y al contenido. Sin embargo, la experiencia brasileña en la lucha contra la piratería es más amplia que la de cualquier otro país, debido a la fuerte actuación de Anatel en la conducción del PACP, que abarca los más variados segmentos de la cadena de comercialización y cuenta con la integración de diversos organismos públicos y privados, en especial el órgano aduanero.

En cuanto al combate al uso indebido de contenido protegido por derechos de autor, la actuación de Anatel se concentra en impedir la conexión de los equipos utilizados para tal fin ilícito a las redes de telecomunicaciones, mientras que algunos países actúan directamente en el bloqueo del contenido protegido. Ambas perspectivas abren posibilidades a las administraciones y a los organismos reguladores para la protección de los derechos de autor y para la utilización adecuada de las redes de telecomunicaciones, de acuerdo con la interpretación jurídica de la legislación de cada país.

⁷⁵ UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). **Output - Updated text of the draft Recommendation ITU-T Q.FC-MCM: Framework for combating Multimedia Content Misappropriation**. Ginebra, 2024. Disponible en: <https://www.itu.int/md/T22-SG11-240501-TD-GEN-0993/en>. Acceso en: 23 jul. 2025.

4. DESAFÍOS Y OPORTUNIDADES FUTURAS

El combate contra la piratería en las telecomunicaciones es un frente estratégico de la actuación regulatoria de Anatel, que exige una constante actualización tecnológica, articulación institucional y alineamiento con la dinámica del mercado digital. Aunque se han logrado avances significativos —como las incautaciones de equipos no homologados, el bloqueo remoto de dispositivos clandestinos, la represión a las redes de IPTV ilegal y el fortalecimiento de la fiscalización—, el escenario aún impone desafíos complejos y multifactoriales, al mismo tiempo que ofrece oportunidades de innovación regulatoria y de colaboración intersectorial.

4.1. Principales Desafíos

Desinformación y Atracción por el Bajo Costo – Muchos consumidores aún no perciben los riesgos asociados al uso de dispositivos no homologados. La atracción del bajo costo, junto con la falsa sensación de legalidad en algunos canales de venta, contribuye a la demanda continua de productos piratas.

Capilaridad y Logística del Comercio Ilegal – La estructura de distribución de dispositivos clandestinos involucra múltiples canales —físicos y virtuales—, lo que hace que la fiscalización sea más costosa y reactiva. Una actuación eficaz requiere ampliar la capacidad de respuesta en tiempo real y reforzar la inteligencia preventiva.

Limitaciones Jurídico-Normativas – Aunque existen instrumentos normativos que otorgan a la Anatel competencia para actuar en la represión de la piratería, aún hay vacíos regulatorios y jurídicos que dificultan la responsabilización de los infractores, especialmente en los casos en que los servicios ilegales son ofrecidos por entidades ubicadas fuera del país.

Fragmentación y Anonimato de la Distribución Digital – La comercialización de decodificadores y servicios piratas se realiza, en gran parte, a través de plataformas digitales internacionales, grupos en redes sociales y *marketplaces* que operan fuera de la jurisdicción brasileña. Esto exige soluciones multilaterales y cooperación con intermediarios digitales y organismos internacionales.

Sofisticación Tecnológica de los Dispositivos Piratas – La tecnología aplicada a los equipos ilegales se adapta y avanza rápidamente, con capacidades de ofuscación, actualización remota e integración con plataformas descentralizadas, lo que dificulta su identificación y bloqueo. Muchos dispositivos cuentan con mecanismos de *firmware over-the-air* (tecnología que permite la actualización del *software* de control del equipo mediante conexión por radio, como Wi-Fi o datos móviles), que logran evadir los sistemas convencionales de detección.

4.2. Oportunidades Futuras

Avance en la Cooperación con Plataformas Digitales – Existe margen para consolidar acuerdos de cooperación con grandes *marketplaces* y redes sociales para posibilitar la eliminación proactiva y automatizada de anuncios y perfiles involucrados en la comercialización de productos irregulares, utilizando criterios técnicos definidos por la Anatel.

Integración con Sistemas Aduaneros y de Inteligencia Artificial – La Anatel puede ampliar el uso de tecnologías de IA y *machine learning* en conjunto con la Secretaría de la Receita Federal de Brasil y organismos de seguridad, para la identificación automática de cargas sospechosas y bloqueo en el origen, aún en los puntos de entrada del país.

Revisión y Modernización del Marco Regulatorio – El combate contra la piratería puede fortalecerse mediante propuestas legislativas que criminalicen de manera más objetiva la

importación, comercialización y operación de dispositivos ilegales y el consumo de contenido multimedia que infrinja los derechos de autor y la propiedad intelectual, así como mediante la actualización de resoluciones para permitir respuestas más rápidas e interoperables.

Fortalecimiento de Campañas Educativas – La concienciación del consumidor es uno de los pilares de la eficacia a largo plazo de las estrategias contra la piratería. La Anatel puede ampliar sus acciones de educación digital y ciudadanía, en colaboración con escuelas, Procons, operadoras y medios de comunicación, reforzando los riesgos para la seguridad, la privacidad y la legalidad.

Participación Activa en Foros Internacionales – El compromiso en iniciativas como las de la UIT, OCDE, OMPI y redes de administradores de telecomunicaciones puede aportar aprendizajes, estandarizaciones técnicas y buenas prácticas transnacionales que contribuyan a acciones más efectivas en territorio nacional.

Adopción de Infraestructuras de Respuesta Automatizada – La creación de sistemas integrados de respuesta a incidentes, con la participación de proveedores de acceso, operadoras y empresas de tecnología, puede permitir bloqueos automatizados en tiempo real de dispositivos y servidores irregulares, basados en datos regulatorios y de seguridad.

Fortalecimiento de asociaciones con otros órganos de la administración pública – En 2025 se concretó un acuerdo con Ancine, que permitirá el bloqueo no solo de los *set top boxes*, sino también de sitios web y aplicaciones de distribución de contenido pirata.

Además, continúan las negociaciones con la RFB para ampliar la actuación conjunta con Anatel en puertos y aeropuertos, con el fin de impedir la importación de equipos no homologados. El escenario de piratería en telecomunicaciones está en constante transformación, lo que exige que Anatel adopte una postura proactiva, adaptable y

tecnológica. La conjugación de desafíos regulatorios, operativos y culturales debe enfrentarse con una visión sistémica, compromiso interinstitucional e innovación continua.

Las oportunidades para fortalecer la lucha contra la piratería en Brasil son significativas, desde el uso estratégico de datos e inteligencia artificial hasta el desarrollo de políticas públicas integradas con el sector privado y la sociedad civil. Al liderar este movimiento con rigor técnico y compromiso público, Anatel contribuye a la protección de la legalidad, la soberanía digital y los derechos del consumidor brasileño.

REFERENCIAS

1. En el argot técnico, la conexión o interconexión es el enlace del terminal o red del usuario con las redes públicas de telecomunicaciones. Disponible en: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2018/1142-resolucao-693>. Acceso en: 07 jul. 2025.
2. BRAGA, Lucas; FAVRETTO, Everton. Anatel multa clínica veterinária por usar produto sem homologação. Tecnoblog, 23 feb. 2021. Actualizado el 14 nov. 2023. Disponible en: <https://tecnoblog.net/noticias/anatel-multa-clinica-veterinaria-por-usar-produto-sem-homologacao/>. Acceso en: 07 jul. 2025.
3. Polícia apreende bloqueador de sinal de GPS usado por quadrilha de roubos de cargas no Rio. G1, Río de Janeiro, 14 feb. 2019. Disponible en: <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>. Acceso en: 07 jul. 2025.
4. ALMEIDA, Esther. Dono de construtora morto em SP: saiba como evitar clonagem de controle de portão. O Globo, Río de Janeiro, 7 jun. 2025. (Actualizado en 7 ago. 2025.). Disponible en: <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>. Acceso en: 07 jul. 2025.
5. Bandidos em dupla já clonam chave a distância e levam carro em segundos. UOL, 5 oct. 2023. Disponible en: <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>. Acceso en: 7 jul. 2025.
6. AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL (Brasil). Anatel apresenta esclarecimentos sobre o Flipper Zero. Brasília, 29 mar. 2023. Actualizado el 31 may. 2023. Disponible en: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-apresenta-esclarecimentos-sobre-o-flipper-zero>. Acceso en: 07 jul. 2025.
7. CINTRA, Caroline. "Perdi meu coração", diz mãe de garoto que morreu após choque em carregador. Correio Braziliense, Brasília, 12 ago. 2020. Actualizado el 12 ago. 2020. Disponible en: <https://www.correiobraziliense.com.br/cidades->

- df/2020/08/4868126--perdi-meu-coracao---diz-mae-de-garoto-que-morreu-apos-choque-em-carregador.html. Acceso en: 07 jul. 2025.
8. VÍDEO: Incêndio em auditório pode ter sido provocado por carregador de celular, dizem bombeiros. G1 Tocantins, 08 ene. 2024. (Actualizado hace un año). Disponible en: <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>. Acceso en: 07 jul. 2025.
 9. DIOGO, Darcianne. Jovem sofre queimadura de 1º grau após celular explodir na tomada no DF. Correio Braziliense, Brasília, 14 may. 2023. Disponible en: <https://www.correiobraziliense.com.br/cidades-df/2023/05/5094486-jovem-sofre-queimadura-de-1-grau-apos-celular-explodir-na-tomada-no-df.html>. Acceso en: 07 jul. 2025.
 10. SILVA, Cristiane. Celulares já mataram 23 no Brasil: especialistas apontam principais vilões. Correio Braziliense, Brasília, 01 oct. 2019. Disponible en: 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. Acceso en: 07 jul. 2025.
 11. Cf. AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL (Brasil). Superintendencia de Fiscalización. Informe n.º 4/2021/FIGF4/FIGF/SFI. Brasília, 2021. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5PKr37An4NSs6sd1c9IPofluH3e-yRwywlgZFvUh-qW-f-MR8ln0HwABi8MWbOkspZajukWXFCisvs8oBuJmvd. Acceso en: 23 jul. 2025.
 12. Cf. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendencia de Fiscalización. Informe n.º 8/2022/FIGF4/FIGF/SFI. Brasília. 2022. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46lzCFD26Q9Xx5QNDbqbGHzc2pUgPteuRLZ6SDuwZoTzukaE9xm340u-SmUAwHzdKU2tlv4WgKQmypi8cvl3ntyOGfLQji7o_Cb0uH4U-. Acceso en: 23 jul. 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. Disponible en: <https://ieeexplore.ieee.org/document/7784601>. Acceso en 25 jul. 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. Disponible en: <https://ieeexplore.ieee.org/document/9461272>. Acceso en: 31 ago. 2025.
 15. VAN DER SAR, Ernesto. The Pirate Bay Website Runs a Cryptocurrency Miner. 2017. Disponible en: <https://torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/>. Acceso en: 14 jun. 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. Disponible en: <https://csimq-journals.rtu.lv/csimq/article/view/csimq.2016-9.03>. Acceso en: 31 ago. 2025.
 17. SATORI THREAT INTELLIGENCE AND RESEARCH TEAM. Satori Threat Intelligence Disruption: BADBOX 2.0 Targets Consumer Devices with Multiple Fraud Schemes. 2025. Disponible en: <https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/>. Acceso en: 19 maio 2025.
 18. AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL (Brasil). Anatel emite alerta sobre malware "Bad Box 2.0" em TV Boxes piratas. Brasilia, DF: Anatel, 25 jul. 2025. Disponible en: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-emite-alerta-sobre-malware-bad-box-2-0-em-tv-boxes-piratas>. Acceso en: 14 ago. 2025.
 19. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendencia de Otorgamiento y Recursos a la Prestación, Superintendencia de Fiscalización. Despacho Decisório n.º 5657/2024/ORCN/SOR. Brasilia, 2024. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46lzCFD26Q9Xx5QNDbqYmK7UOAaw8fj5jIUHIDwe0NhuPf9JzG-Uyip5lqqRmZXWq3_FHP60CDJBwjfirYwgLZsBySFp8Kq5_qlyt8sBgO. Acceso en: 23 jul. 2025.

20. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Superintendencia de Otorgamiento y Recursos a la Prestación, Superintendencia de Fiscalización, Superintendencia de Control de Obligaciones. Despacho Decisório n.º 5686/2024/ORCN/SOR. Brasília, 2024a. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqZApP7PurlyWa1s0oaWqCwkV7A2ZHNvzF5QswTfpGIhwO97BwkTz78Z4IVzkLfICyMkA1dhf6kvAa4Vna4sXaT3. Acceso en: 23 jul. 2025.
21. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL (Brasil). Anatel, Polícia Federal e Receita Federal realizam ação conjunta em Pelotas (RS). Brasília, DF: Anatel, 09 jul. 2025. Disponible en: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-policia-federal-e-receita-federal-realizam-acao-conjunta-em-pelotas-rs>. Acceso en: 27 jul. 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, 29 jul. 2025. Disponible en: <https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-e-pf-desarticulam-esquema-milionario-de-tv-box-e-gatonet-em-operacao-praedo>. Acceso en: 29 jul. 2025.
23. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria General Federal, Procuradoria Federal Especializada ante la Agencia Nacional de Telecomunicaciones. Parecer n.º 01580/2015/PFE-ANATEL/PGF/AGU. Brasília, 2015. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?Yj72kUioo_z14_E1ere_NErKAAYpCDMsB4uhQFHnURzlCcsEezBx7gPUNtxU8bNUcaTcr0nBnveExhjlYaFQPg7w474YcqjoUmoQPS4yTNLNaLUCTtkxM0SgmZMjHGDh. Acceso en 21 jul. 2025.
24. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria General Federal, Procuradoria Federal Especializada ante la Agencia Nacional de Telecomunicaciones. Parecer n.º 00524/2018/PFE-ANATEL/PGF/AGU. Brasília, 2018. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5Aq93gDCiAKZgfvdufplsL2yUPD34g1U-JBQb1D9R_dacgaUTkfl4JNVnd23QsN5FoeTx1MPAZEgSqZRwJaIOS. Acceso en 21 jul. 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. Disponible en: <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103>. Acceso en: 10 ago. 2025.
26. En este sentido, 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. MINISTERIO DE JUSTICIA Y SEGURIDAD PÚBLICA. SECRETARÍA NACIONAL DEL CONSUMIDOR. COORDINACIÓN DE CONSUMO SEGURO Y SALUD. Nota Técnica n.º 610/2019/CCSS/CGCTSA/DPDC/SENACON/MJ. Disponible en: <https://www.gov.br/mj/pt-br/assuntos/noticias/senacon-questiona-sites-sobre-politica-para-evitar-anuncio-e-venda-de-produtos-falsificados/NTPirataria.pdf> . Acceso en: 10 ago. 2025.
28. MINISTERIO DE JUSTICIA Y SEGURIDAD PÚBLICA. SECRETARÍA NACIONAL DEL CONSUMIDOR. COORDINACIÓN DE CONSUMO SEGURO Y SALUD Nota Técnica n.º 91/2020/CCSS/CGCTSA/DPDC/SENACON/MJ, Disponible en: <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> . Acceso en: 10 ago. 2025.
29. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer . 00453/2021/PFE-ANATEL/PGF/AGU. Brasília, 2021. Diponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO4t0UuV0d7ERjywGrRjzWiwaEv5qDiucqzOSkmGuYZGIA6a-B118QiuybPF9Bdki34wmGMyB6GhHGdoEUeFV5_ . Acceso en 21 jul. 2025.
30. SUPREMO TRIBUNAL FEDERAL (STF) (Brasil). STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros. Brasília, 26 jun. 2025. Disponible en: <https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/>. Acceso en: 29 jul. 2025. Nota: acórdão ainda pedente de lavratura em 10 de outubro de 2025.
31. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. Parecer n.º 00695/2019/PFE-ANATEL/PGF/AGU. Brasília, 2019. Disponible en:

- https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5Sb4M9fy78errTgNmS1KvYO6MDBaTC20TJyVcVGyXzrRmS0t-IDw7p9ZA-wiumFQdmhpVP6MIDcdohmso_Flu_ . Acceso en 21 jul. 2025.
32. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria General Federal, Procuradoria Federal Especializada ante la Agencia Nacional de Telecomunicaciones. Parecer n. 00770/2019/PFE-ANATEL/PGF/AGU. Brasília, 2019a. Disponible en : https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO7vcSiACcxViZXBtJEqIYo_G5oZ0GTWldJ5bFQldK3XB0qatznYBYSXvUPbLchNV9NPFSFr5wuknNbIsCUZqEXN . Acceso en 21 jul. 2025.
33. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria General Federal, Procuradoria Federal Especializada ante la Agencia Nacional de Telecomunicaciones. Parecer . 00385/2023/PFE-ANATEL/PGF/AGU. Brasília, 2023. Disponible en: sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqa6i8M5H4M2ICd-In0Ov5885pJq4NQwRwrORFIXmO-AeuSMT701C3h8Xc2ljkSS0nxN_TT-x1yfiY6U6Z-DPLZK. Acceso en 21 jul. 2025.
34. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria General Federal, Procuradoria Federal Especializada ante la Agencia Nacional de Telecomunicaciones. Parecer n. 00329/2020/PFE-ANATEL/PGF/AGU. Brasília, 2020. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5BzURuP5bhnuacdW_NWcJqJATu7fxFbPmmPsQQNOp8Spe2mTwP5nRw2ylwB4yQmuqdKfNHT6EjUJB25_jBtPM7. Acceso en 21 jul. 2025.
35. AGENCIA NACIONAL DE TELECOMUNICACIONES – ANATEL (Brasil). Superintendencia de Otorgamiento y Recursos a la Prestación. Gerencia de Certificación y Numeración. Memorando nº 52/2022/ORCN/SOR. Brasília, 2022. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO6twY5HXXccmxWop68eTQTqTn9ixgaLS49XCr64tUHCc5brumli3HaJDIhwKGOzPY-2iCX7HynMovVtKoW_wErB. Acceso en: 23 jul. 2025.

36. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuradoria Geral Federal Procuradoria Federal Especializada junto à Agência Nacional de Telecomunicações. Parecer n. 00223/2022/PFE-ANATEL/PGF/AGU. Brasília, 2022a. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5ax4ZZUq2xuaXLoaMiATdWGeIxczd1TqyaqC0PDsQ2KQBdeJJETr0mD_5EQjZWmZoQcKGDxWFWugbgv77UV3fU. Acceso en 21 jul. 2025.
37. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. Parecer n. 00454/2021/PFE-ANATEL/PGF/AGU. Brasília, 2021a. Diponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO68ltWJtJ7YHhYP85DAYRwXLVYefsWGyUfp3DobEpcyWtximBn8o7NqLIGfbu_cwgEdo_tujUfwlH-bKJxFpKKZ. Acceso en 21 jul. 2025.
38. ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. Parecer n. 00103/2022/PFE-ANATEL/PGF. Brasília, 2022. Diponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO5sBHBMJmM0fxKRu2a4Qr-PGPvBLNbHPOOdoC0BU3-3lvzfzZw6OxT9C7mfgGXwntQyXc5eX5wVKWjddc0HI21S. Acceso en 21 jul. 2025.
39. AD ADVOCACIA GERAL DA UNIÃO (Brasil). Procuraduría General Federal, Procuraduría Federal Especializada ante la Agencia Nacional de Telecomunicaciones. Parecer n. 00063/2024/PFE-ANATEL/PGF/AGU. Brasília, 2024. Disponible en: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46lzcFD26Q9Xx5QNDbqZPZr_MlidKv2NAOXJQ69gtBrT0pFzcupimr_D0SIJIM4dMMlfb5Nlui0BcjfUnUpz93sTE18zCmc569falTP7. Acceso en 21 jul. 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. Disponible en: <https://www.journals.uchicago.edu/doi/full/10.1086/674020>. Acceso en: 19 maio 2025.

41. Proeletronic expõe o SmartPRO 4K, TV box com homologação da Anatel para provedores e IPTV. Revista RTI (Aranda Net), São Paulo, actualizado el 14 jun. 2024. Disponible en: <https://www.arandanet.com.br/revista/rti/noticia/8998-Proeletronic-expoe-o-SmartPRO-4K,-TV-box-com-homologacao-da-Anatel-para-provedores-e-IPT>. Acceso en: 07 jul. 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. Disponible en: https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf. Acceso en: 14 jun. 2025.
43. ESTADOS UNIDOS DA AMÉRICA (EUA). United States Code. Title 18. Part I. Chapter 1. Section 18 - Organization defined. Disponible en: <https://www.law.cornell.edu/uscode/text/18/18>. Acceso en: 19 jun. 2025.
44. COUNCIL OF THE EUROPEAN UNION (União Europeia). EMPACT Terms of Reference. Bruxelas: 2023. Disponible en: <https://data.consilium.europa.eu/doc/document/ST-8975-2023-INIT/en/pdf>. Acceso en: 19 jun. 2025.
45. EUROPOL (Unión Europea). Europol Programming Document 2025 – 2027. Haia: 2024. Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2025-2027.pdf. Acceso en: 14 jun. 2025.
46. UNIÃO EUROPEA (UE). Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022. Estrasburgo: 2022. Disponible en: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2022.169.01.0001.01.ENG. Acceso en: 14 jun. 2025.
47. UNIÃO EUROPEA (UE). Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012. Estrasburgo: 2012. Disponible en: https://www.epo.org/en/legal/up-upc/2022/upcaannexi_ciii.html. Acceso en: 14 jun. 2025.
48. ESTADOS UNIDOS DE LA AMERICA (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. Disponible en: <https://www.govinfo.gov/content/pkg/COMPS-937/uslm/COMPS-937.xml>. Acceso

en: 14 jun. 2025.

49. ESTADOS UNIDOS DE LA AMERICA (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. Disponible en: <https://www.govinfo.gov/content/pkg/COMPS-959/uslm/COMPS-959.xml>. Acceso en: 14 jun. 2025.
50. FEDERAL REGISTER (Estados Unidos de la America). Code of Federal Regulations. Title 47 - Telecommunication, as of June 14th, 2025. Washington (DC): 2025. Disponible en: <https://www.ecfr.gov/on/2025-06-14/title-47>. Acceso en: 14 jun. 2025.
51. JAPÓN. 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. Disponible en: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_5.pdf. Acceso en: 14 jun. 2025.
52. JAPÓN. Telecommunications Business Law (Law No. 86 of December 25, 1984) - as amended last by: Law No. 125 of July 24, 2003. Tóquio, 2003. Disponible en: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/TBL/TBL-index.html. Acceso en: 14 jun. 2025.
53. UNIÓN EUROPEA (UE). Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014. Estrasburgo, 2014. Disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053>. Acceso en: 14 jun. 2025.
54. UNIÓN EUROPEA (UE). Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011. Estrasburgo, 2011. Disponible en: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32011R0182>. Acceso en: 14 jun. 2025.
55. UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). Agreement - draft Supplement Q.Suppl.75. 2021. Disponible en: <https://www.itu.int/md/T17-SG11-211201-TD-GEN-1800/en>. Acceso en: 23 jul. 2025.
56. UIT, 2021.
57. ALIANZA CONTRA LA PIRATERÍA AUDIOVISUAL - ALIANZA. Piratería de Señales de

Televisión Paga y en Línea 2q-2024. 2024. Disponible en: <https://telesintese.com.br/wp-content/uploads/2024/12/Informe-de-Alianza.pdf>. Acceso en: 23 jul. 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, 17 ago. 2024. Disponible en: <https://www.broadbandtvnews.com/2024-ago-17/anti-piracy-alliance-ace-settles-copyright-infringement-cases-with-iptv-operators/>. Acceso en: 07 jul. 2025.
60. BRIEL, Robert. ACE takes legal action against IPTV pirates. Broadband TV News, 11 mar. 2025. Disponible en: <https://www.broadbandtvnews.com/2025/03/11/ace-takes-legal-action-against-iptv-pirates/>. Acceso en: 07 jul. 2025.
61. DICKERSON Jeremy. Premier League 'live' blocking order against livestream servers renewed for 2017/18 season. Lexology, 2 ago. 2017. Disponible en: <https://www.lexology.com/library/detail.aspx?g=a68db02f-12f5-4169-aa8f-56d35395d3b5>. Acceso en: 23 jul. 2025.
62. ENGLAND AND WALES HIGH COURT (Reino Unido). Chancery Division. Matchroom Boxing Ltd & Anor v British Telecommunications Plc & Ors (Decision). Londres, 20 set. 2018. Disponible en: <https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2018/2443.html&query=IL-2018-000155+>. Acceso en: 23 jul. 2025.
63. HEENAN, Emily. High Court blocks cyberlocker and stream-ripping websites. Lexology, 24 mar. 2021. Disponible en: <https://www.lexology.com/library/detail.aspx?g=87ca8734-1d84-4be3-85b9-325ec9d56d4d>. Acceso en: 23 jul. 2025.
64. DANAHER, Brett; SMITH, Michael D.; TELANG, Rahul, The Effect of Piracy Website Blocking on Consumer Behavior. 2019. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612063. Acceso en: 23 jul. 2025.
65. UNIÓN EUROPEA (UE). Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019. Estrasburgo, 2019. Disponible en: <https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng>. Acceso en: 16 jun. 2025.

66. HOMANN, Jochen. Online Copyright Clearance System arranges block of streaming site. Bonn: Bundesnetzagentur, 11 mar. 2021. Disponible en: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2021/20210311_Clearingstelle.html. Acceso en: 23 jul. 2025.
67. SATORI THREAT INTELLIGENCE AND RESEARCH TEAM, 2025.
68. FINLANDIA. Copyright Act (Act No. 404/1961 of July 8, 1961, as amended up to Act No. 608/2015 of May 22, 2015). 2015. Disponible en: <https://www.wipo.int/wipolex/en/legislation/details/15992>. Acceso en: 23 jul. 2025.
69. UE, 2019.
70. https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_17/wipo_ace_17_13.pdf
71. AUSTRALIA. Copyright Amendment (Online Infringement) Act 2015. Canberra, 2015. Disponible en: <https://www.legislation.gov.au/C2015A00080/latest/text>. Acceso en: 23 jul. 2025.
72. MOTION PICTURE ASSOCIATION (MPA). Measuring the Effect of Piracy Website Blocking in Australia on Consumer Behavior: December 2018. 2020. Disponible en: <https://www.mpa-apac.org/wp-content/uploads/2020/02/Australia-Site-Blocking-Summary-January-2020.pdf>. Acceso en: 23 jul. 2025.
73. MPA, 2020.
74. UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). LS on the agreement of Technical Report ITU-T QSTR-MCM-UC "Use Cases on the combat of Multimedia Content Misappropriation". 2024. Disponible en: <https://www.itu.int/md/T22-SG16-240415-TD-GEN-0295/en>. Acceso en: 23 jul. 2025.
75. UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). Output - Updated text of the draft Recommendation ITU-T Q.FC-MCM: Framework for combating Multimedia Content Misappropriation. Ginebra, 2024. Disponible en: <https://www.itu.int/md/T22-SG11-240501-TD-GEN-0993/en>. Acceso en: 23 jul. 2025.

White Paper Combate a la Piratería

HISTÓRICO, BENCHMARK INTERNACIONAL, RESULTADOS