Investigación sobre los mecanismos para el monitoreo del cumplimiento del principio de neutralidad de la red que resulten aplicables al marco regulatorio nacional

Mtra. Isabel Reza Meneses

Centro de Estudios[1]

Julio 2022

En el presente estudio se describe brevemente la experiencia internacional en materia de neutralidad de la red, seguido de la revisión de 6 casos de estudio en los que se advirtió la existencia de mecanismos orientados al monitoreo del cumplimiento de dicho principio, desde una perspectiva técnica, y se finaliza con una serie de recomendaciones sobre cómo los mecanismos existentes para monitorear la calidad del servicio de acceso a Internet en el contexto nacional pudieran ser empleados por el IFT para dar certeza jurídica a los usuarios finales respecto del cumplimiento de los Lineamientos de neutralidad de la red por parte de los PSI y, en consecuencia, se garantiza el derecho de los usuarios a acceder libremente a cualquier contenido, aplicación o servicio disponible en Internet.

[1] Centro de Estudios del IFT. El contenido, las opiniones y las conclusiones o recomendaciones vertidas en este documento son responsabilidad exclusiva de su autora, y no necesariamente reflejan el punto de vista oficial del Instituto Federal de Telecomunicaciones ni de su Centro de Estudios.

Investigación sobre los mecanismos para el monitoreo del cumplimiento del principio de neutralidad de la red que resulten aplicables al marco regulatorio nacional

Isabel Reza[2][3]

I. Resumen

La presente investigación proporciona una visión técnica de cómo, en el contexto internacional, los reguladores han implementado diversos mecanismos de monitoreo de la neutralidad de la red. Asimismo, se presentan argumentos técnicos que sugieren que, a través del monitoreo de parámetros de la calidad del servicio de acceso a Internet, tales como la velocidad (*downlink y uplink*), *jitter*, *delay* y *packet loss rate* y, eventualmente, con la identificación de variaciones en dichos parámetros se puede identificar la existencia de gestión de tráfico por parte de los PSI, toda vez que un tratamiento diferenciado del tráfico puede ocasionar un menor rendimiento de la QoS. Adicionalmente, se presenta una descripción sobre algoritmos y aplicaciones creadas específicamente para la detección de diferenciación de tráfico a través de modelos estadísticos. Al respecto, la investigación de mérito concluye que, bajo la normativa nacional, existen diversos mecanismos que actualmente se emplean para monitorear QoS del Servicio de Acceso a Internet (móvil y fijo), así como el sistema de quejas "Soy usuario", el medidor de velocidad "Conoce tu Velocidad", entre otros, que pueden ser válidamente empleados por el IFT para monitorear el cumplimiento del principio de neutralidad de la red. Lo anterior, sin menoscabo de la integración de un informe anual y del desarrollo de aplicaciones específicas para la detección de la diferenciación del tráfico en apego a las políticas de gestión de tráfico y administración de red permitidas por el marco normativo nacional.

[2] Es Ingeniera en Telecomunicaciones y Maestra en Ingeniería Eléctrica por la Universidad Nacional Autónoma de México. Actualmente cursa la Maestría en Regulación y Competencia Económica en Telecomunicaciones en INFOTEC, es Investigadora en Tecnologías y Regulación del Centro de Estudios del IFT. Es experta en regulación de la red y agentes económicos preponderantes, además de evaluación de la conformidad y disposiciones técnicas. Ha tenido a su cargo proyectos como el de los lineamientos de neutralidad de la red y la separación funcional de Telmex. Anteriormente, fue Directora de Desarrollo Digital y Subdirectora de Criterios Normativos en la Unidad de Política Regulatoria del IFT.

[3] La autora agradece la colaboración del enlace de investigación en análisis cuantitativo, Lic. Llusvy Amairani Peralta Rojo y de los practicantes de servicio social Rodolfo Saúl Cruz Ramirez y Mariana Vazquez Vieyra, en la recopilación de datos e información y realización de búsquedas bibliográficas sobre los distintos modelos y mecanismos regulatorios respecto del principio de neutralidad de la red.

II. Acrónimos y Glosario[4]

Término	Definición
ANATEL	*Agência Nacional de Telecomunicações*; en español, Agencia Nacional de Telecomunicaciones (Brasil)
ARCEP	*Autorité de Régulation des Communications Électroniques*; en español, Autoridad de Regulación de las Telecomunicaciones Electrónicas (Francia)
ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones (Ecuador)
Banda ancha	Acceso de alta capacidad que permite ofrecer diversos servicios convergentes a través de infraestructura de red fiable, con independencia de las tecnologías empleadas, cuyos parámetros serán actualizados por el Instituto[5] periódicamente. (LFTR, 2014)
BEREC	*Body of European Regulators for Electronic Communications*; en español, Organismo de Reguladores Europeos de las Comunicaciones Electrónicas

[4] Los términos antes señalados pueden ser usados indistintamente en singular o plural, en mayúsculas o minúsculas.

Término	Definición
Bundesnetzagentur	En español, Agencia Federal de Redes de Alemania
Calidad	Totalidad de las características de un servicio de telecomunicaciones y radiodifusión que determinan su capacidad para satisfacer las necesidades explícitas e implícitas del usuario del servicio, cuyos parámetros serán definidos y actualizados regularmente por el Instituto. (LFTR, 2014)
CCTS	*Commission for Complaints for Telecom-television;* en español Comisión de Quejas de Telecomunicaciones y Televisión (Canadá)
CGI	*Comitê Gestor da Internet no Brasil;* en español Comité Gestor de Internet (Brasil)
CRC	Comisión de Regulación de Comunicaciones (Colombia)
CRTC	*Canadian Radio-television and Telecommunications Commission*; en español, Comisión Canadiense de Radio, Televisión y Telecomunicaciones (Canadá)
Delay	El tiempo requerido para que un paquete atraviese la red o un segmento de la red (UITa, 2022)
DNS	*Domain Name System*; en español Sistema de Dominio de Nombres
DOF	Diario Oficial de la Federación

Término	Definición
DT	Diferenciación de Tráfico
E2E	*End to End*; en español, Extremo a Extremo
ETSI	European Telecommunications Standards Institute, en español, Instituto Europeo de Estandarización en Telecomunicaciones
Enacom	Ente Nacional de Comunicaciones (Argentina)
Fast lane	En español vía rápida, es una vía menos congestionada intencionalmente para darle mayor prioridad a la transmisión de datos por ese medio. (Thiago Garrett, 2022, p. 6)
FCC	*Federal Communications Commission*; en español, Comisión Federal de Comunicaciones (Estados Unidos de América)
FEC	*Forward Error Correction*; en español, Corrección de errores en recepción.
Frecuencia	Número de ciclos por segundo que efectúa una onda del espectro radioeléctrico, cuya unidad de medida es el Hertz (LFTR, 2014)
Gestión de tráfico	Conjunto de técnicas utilizadas por los proveedores del servicio de acceso a Internet para el manejo, tratamiento y procesamiento del flujo de tráfico cursado por una red pública de telecomunicaciones (IFTa, 2021)
Host	Es una computadora que se comunica utilizando los protocolos de Internet. Un host implementa funciones de enrutamiento (es decir, opera en la capa IP) y puede implementar funciones

Término	Definición
	adicionales, incluidos protocolos de capa superior. (UITa, 2022)
IFT o Instituto	Instituto Federal de Telecomunicaciones
Internet	Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única. (LFTR, 2014)
IoT	*Internet of Things;* en español, Internet de las Cosas
IP	*Internet Protocol*; en español, Protocolo de Internet
Jitter	Una medida de la variación de latencia por encima y por debajo del valor medio de latencia. El *jitter* máximo se define como la variación de latencia máxima por encima y por debajo del valor de latencia medio (UITa, 2022)
Latencia	Tiempo que tarda un paquete de datos en ir de un extremo a otro de la red. (Tapia & Acosta, 2015)
LFTR	Ley Federal de Telecomunicaciones y Radiodifusión

Término	Definición
NN	*Network Neutrality*; en español, Neutralidad de la Red
MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información (Ecuador)
Monitoreo	Término también conocido como seguimiento o vigilancia, un monitoreo es una secuencia planificada de observaciones, controles o mediciones para evaluar si ciertas medidas normativas están funcionando como lo previsto (QCA, 2018) El monitoreo de las medidas de control es el proceso continuo de obtención de información en la etapa que sea plica la medida de control. Las actividades de monitoreo se centran habitualmente en mediciones realizadas en "tiempo real" y el funcionamiento de una medida de control específica (QCA, 2018)
OTT	*Over The Top Services*; por sus siglas en inglés
OCDE	Organización para la Cooperación y Desarrollo Económico
OFCOM	*Office of Communications*; en español Oficina de Telecomunicaciones (Reino Unido)
OPSITEL	Organismo Supervisor de Inversión Privada en Telecomunicaciones (Perú)
P2P	*Peer to Peer, e*n español Persona a Persona
PSI	Proveedor del Servicio de Acceso a Internet

Término	Definición
PACS	Proveedor de aplicaciones, contenidos y/o servicios.
QoS	*Quality of Services*; en español, Calidad del servicio
QoSO	*QoS Offered/planned by service provider*; en español, Calidad del Servicio ofrecida por un proveedor de servicios (UITa, 2022)
Rendimiento (*throughput*)	Es la capacidad de una red o parte de la red para proporcionar las funciones relacionadas con las comunicaciones entre usuarios de la red, se aplica a la planificación, desarrollo, operaciones y mantenimiento del proveedor de la red, y es la parte técnica detallada de QoS (UITa, 2022)
RPC	Registro Público de Concesiones del Instituto
Servicio de acceso a Internet o SAI	Servicio público de telecomunicaciones que provee conectividad a Internet a los usuarios finales para que accedan a los contenidos, aplicaciones y/o servicios disponibles en Internet, mediante el intercambio, la carga y descarga de tráfico bajo el protocolo de comunicación de Internet IP (IFTa, 2021)
Servicio especializado	Servicios distintos de los servicios de acceso a internet optimizados para contenidos, aplicaciones o servicios específicos, o una combinación de los mismos, cuando la optimización sea necesaria para cumplir los requisitos de los contenidos, aplicaciones o

Término	Definición
	servicios para un nivel específico de calidad (BEREC, 2015)
SUBTEL	Subsecretaría de Telecomunicaciones (Chile)
DT detection	*Traffic Differentiation detection*; en español, Detección de la diferenciación de tráfico (Thiago Garrett, 2022)
Telecomunicaciones	Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión (LFTR, 2014)
Tráfico	Datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que circulan por una red de telecomunicaciones (LFTR, 2014)
UIT	Unión Internacional de Telecomunicaciones
VPN	*Virtual Private Network*; en español, Red Privada Virtual
Zero Rating	En español, rating cero o datos de tráfico gratuito. Se trata de una práctica comercial en la que el PSI no cobra a los usuarios por el volumen de datos consumido en el uso de aplicaciones específicas, generalmente redes sociales (IFTa, 2021).

III. Introducción

III1 Principio de neutralidad de la red

La neutralidad de red se ha conceptualizado internacionalmente como un principio rector de Internet, cuyo objetivo primordial es preservar un Internet abierto y, con ello, garantizar que los usuarios finales puedan acceder libremente a cualquier contenido, aplicación o servicio disponible en Internet. El concepto de neutralidad de la red surgió en 2003 cuando Tim Wu (Wu, 2003) analizó, desde una perspectiva de competencia económica, los conflictos entre los intereses privados de los proveedores de Internet y el interés del público por un mercado competitivo entorno a la innovación en Internet.

Por su parte, el termino de neutralidad de la red fue definido por BEREC como el principio consistente en que todas las comunicaciones electrónicas que transitan por una red deben ser tratadas de la misma manera con independencia de su contenido, servicio, aplicación, origen o destino (BEREC, 2011).

Bajo este contexto, surgió la necesidad de regular la neutralidad de la red y desde los primeros momentos, el sistema normativo ha sido objeto de debate entre académicos, reguladores, la industria y recientemente las organizaciones civiles, toda vez que las dimensiones que el referido principio engloba van desde técnicas de gestión de tráfico, modelos de negocio, algoritmos de detección de diferenciación de tráfico, temas regulatorios y de calidad del SAI, hasta el ejercicio de derechos humanos en el entorno digital, transparencia y privacidad de los usuarios finales.

Particularmente, en América, la neutralidad de la red está mandatada por ley en 8 países, a saber: Argentina, Brasil, Canadá, Chile, Colombia, Ecuador, México y Perú. (Limbatto, 2022). No obstante, en cada país se ha implementado bajo diferentes términos y condiciones, ciertamente cada enfoque obedece a un contexto regulatorio y realidad nacional particular.

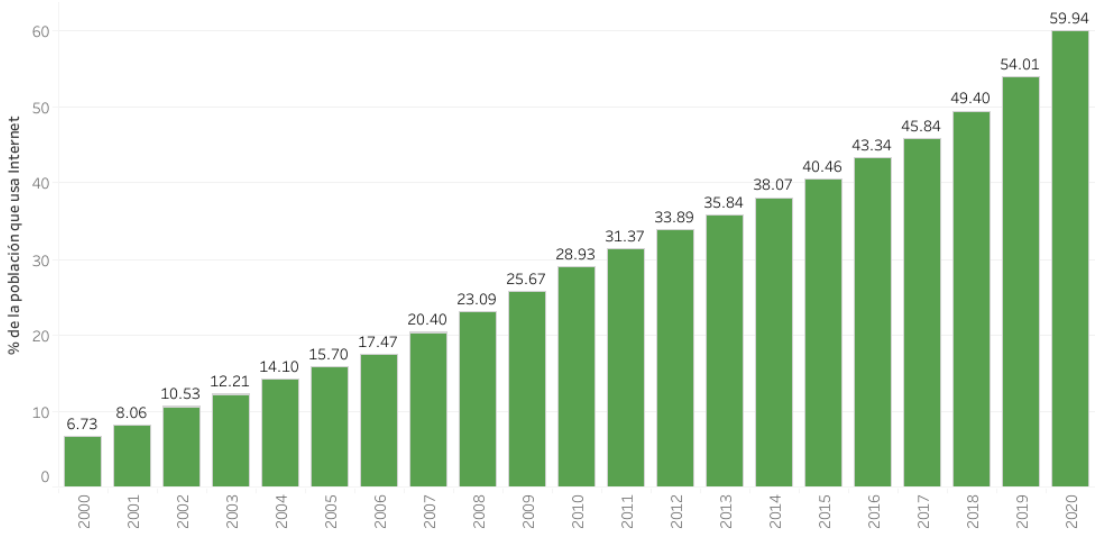
Sin embargo, desde una visión técnica, la neutralidad de red refiere a un trato no discriminatorio del tráfico cursado en Internet, de tal forma que los usuarios puedan acceder libremente a cualquier contenido, aplicación o servicio disponible en Internet. De ahí, que dicho principio haya adquirido una gran relevancia, pues hoy en día las tecnologías digitales sustentan el potencial para promover la conectividad, la democracia, el crecimiento sostenible y el disfrute de derechos humanos y libertades fundamentales en el entorno digital.

Conviene destacar que la neutralidad de la red incide de manera directa en el acceso efectivo en condiciones de calidad, accesibilidad e igualdad a Internet. Particularmente, la Declaración Conjunta sobre la Libertad de Expresión en Internet realizada por el Relator Especial de las Naciones Unidas

(ONU) para la Libertad de Opinión y de Expresión y otras organizaciones en defensa de los derechos humanos y libertades fundamentes (OEA, 2011) establece que el tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino, además de privilegiar la transparencia respecto de las prácticas que emplean los operadores de Internet para gestionar el tráfico.

Por otro lado, mientras que la pandemia de COVID-19 potencializó, como nunca antes, la dependencia global de la tecnología digital en todos los aspectos de la sociedad, desde la educación hasta la salud (OCDE, 2020), el crecimiento de los usuarios de Internet también potenció el incremento de los servicios y aplicaciones que se ofrecen. Sin embargo, los recursos de las redes e infraestructura en telecomunicaciones son finitos, y con ello surge la necesidad de gestionarlos en el contexto del principio de la neutralidad de red. Por su parte, el Banco Mundial señala que el porcentaje de las personas que usan Internet a nivel mundial ha crecido de 2000 a 2020 cerca de 800%. Al año 2020 la cobertura de Internet a nivel mundial era de 59.9% de la población (Banco Mundial, 2022).

Gráfica 1 Porcentaje de la población a nivel mundial que usa Internet[6]



Mientras tanto, la regulación sobre el principio de neutralidad adquiere relevancia, toda vez que impacta a todos los usuarios de Internet que lo utilizan, entre otras cosas, como la base de la comunicación, educación, interacción con el gobierno, economía e innovación. En este ecosistema, los PSI son los administradores de la red y tienen la capacidad técnica de ralentizar, priorizar o bloquear cualquier contenido o servicio en Internet como resultado del incremento del tráfico que cursa por las redes. El papel de los reguladores es central en el tema de la neutralidad de la red, ya que tienen la responsabilidad de vigilar el buen funcionamiento de las redes y favorecer el ejercicio

[6] Elaboración propia con datos del Banco Mundial

del derecho a los usuarios de acceder libremente a cualquier contenido, servicio o aplicación, al mismo tiempo que fomentan el desarrollo sostenible de la infraestructura de telecomunicaciones.

Así, la implementación y, eventualmente el monitoreo del cumplimiento del principio de neutralidad de la red es crítico, pues esta, según (Rammneek, et al., 2017), podría tener un impacto considerable en el diseño de los futuros principios y leyes asociadas al Internet, así como en el derecho de elección de los usuarios finales a cualquier contenido, aplicación o servicio disponible en Internet, y todo lo que ello implique.

De lo anterior, se advierte que el marco regulatorio respecto del principio de neutralidad de la red requiere de una visión multidimensional que no solo se enfoque en los aspectos meramente técnicos y/o económicos; sino también en aquellos que permitan el equilibrio entre distintos derechos.

Ilustración 1 Dimensiones del principio de neutralidad de la red[7]

[7] Elaboración propia con imágenes de Internet.

III2 Experiencia Internacional

A nivel mundial cada país ha trazado su propia historia entorno a la regulación de la neutralidad de la red. Según el estudio *"A survey of Network Neutrality regulations worldwide"* de 2022, actualmente 18 países[8] tienen regulación sobre neutralidad, además de los países que integran la Unión Europea[9], como se representa en la Ilustración 2.

Ilustración 2 Países que cuentan con regulación sobre Neutralidad de la Red[10]

En el presente apartado se describen las principales características de la regulación de los países del continente americano y europeo. La elección de los países estudiados obedece a algunas similitudes en relación, ya sea con la interpretación del principio de neutralidad de la red o con las atribuciones de los órganos reguladores que los hace comparables al caso mexicano.

[8] Japón, Canadá, Noruega, Paraguay, Chile, Colombia, Singapur, Corea del Sur, Ecuador, Perú, Argentina, Brasil, Israel, México, Rusia, Estados Unidos, Sudáfrica y India.

[9] Alemania, Bélgica, Croacia, Dinamarca, España, Francia, Irlanda, Letonia, Luxemburgo, Países Bajos, Suecia, Bulgaria, Eslovaquia, Estonia, Grecia, Malta, Polonia, República Checa, Austria, Chipre, Eslovenia, Finlandia, Hungría, Italia, Lituania, Portugal y Rumanía.

[10] Elaboración propia con base en el estudio "*A survey of Network Neutrality regulations worldwide* de 2022". Disponible en: https://www.sciencedirect.com/science/article/pii/S0267364922000024

Argentina

La Neutralidad de la Red en Argentina está mandatada a través de la Ley 27.078 llamada "**Ley Argentina Digital"**, cuyo objetivo se centra en promover el desarrollo de las tecnologías de la información y comunicaciones.

La Ley Argentina Digital, a través del artículo 57, prohíbe a los PSI (Ley 27.078, 2014):

- Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción o acceso a cualquier contenido, aplicación, servicio o protocolo de Internet, salvo orden judicial o solicitud del usuario;
- Fijar el precio de acceso a Internet en virtud de los contenidos, servicios, protocolos o aplicaciones; y
- Limitar arbitrariamente el derecho de los usuarios a utilizar cualquier hardware o software para acceder a Internet, siempre que no dañen o perjudiquen la red.

Particularmente, en materia de *zero rating,* la regulación argentina no regula esta práctica. Sin embargo, se tiene conocimiento de que operadores como Tuenti, Personal, Claro y Movistar ofrecen acceso gratuito a ciertas aplicaciones (Limbatto, 2022)

Brasil

El debate sobre la regulación de la neutralidad de la red comenzó en el 2009, a través de los "10 principios de gobernanza del uso de Internet" resolución emitida por el Comité Directivo de Internet (CGI) de Brasil. Aunado a lo anterior, el Ministerio de Justicia en colaboración con la Fundación Getúlio Vargas lanzaron un proyecto para construir el marco de derechos civil para Internet basado en los 10 principios del CGI (Thiago Garrett, 2022). Finalmente, el 23 de abril de 2014, se aprobó la Ley 12.965 que encuentra fundamento en el Marco Civil de Internet. Al respecto, el gobierno brasileño emitió el Decreto N°9771, con el objetivo de dar cumplimiento al "Marco Civil da Internet".

La regulación brasileña obliga a los PSI a tratar cualquier tráfico de datos de la misma manera, sin distinción de contenido, origen, destino, servicio, terminal o aplicaciones. Además, prohíbe toda discriminación o degradación del tráfico según la normativa, salvo que se deba a requisitos técnicos para la adecuada prestación del servicio (Ley N° 12.965, 2014).

El Marco Civil de Internet establece que el uso de Internet en Brasil se basa en el respeto a la libertad de expresión; a través del reconocimiento de su escala global, derechos humanos, pluralidad, libre competencia, protección al consumidor y el reconocimiento de Internet como un elemento clave en el desarrollo de la sociedad (Ley N° 12.965, 2014).

La ley establece en el Art.7 del Marco Civil de Internet (Ley N° 12.965, 2014) que el acceso a Internet es esencial para el ejercicio de los derechos humanos y garantiza al usuario el derecho a la intimidad,

inviolabilidad de las comunicaciones, mantener la calidad del servicio contratado, información clara sobre el SAI, a conocer el proceso del tratamiento y almacenamiento de datos personales por parte de los PSI, aplicación de las normas en defensa del consumidor y la libre expresión.

La priorización se permite en casos de emergencia, incluso en el caso de una discriminación permitida los PSI nunca deberán dañar a los usuarios finales (Thiago Garrett, 2022). En lo que refiere a *zero rating* no está regulado, pero se ha identificado que proveedores como TIM, Claro, Vivo y Oi ofrecen aplicaciones gratuitas. (Limbatto, 2022)

La regulación establecida en 2016 señala que, en situaciones de emergencia la degradación y discriminación del tráfico solo se puede realizar en comunicaciones destinadas a los prestadores de servicios de emergencia y en comunicaciones reservadas a informar a la población, en esos casos la trasmisión de datos será gratuita (Decreto N° 8771, 2016).

Chile

Las reglas sobre la NN en Chile se establecieron en la Ley 20.453 de 2010, además SUBTEL publicó el reglamento de la referida ley, el 18 de marzo de 2011 y, a partir de ello, comenzó a supervisar las obligaciones de calidad de servicio, gestión de tráfico y transparencia.

La referida ley establece, entre otras cosas, los siguientes principios: **i)** los PSI no pueden arbitrariamente bloquear, interferir, discriminar, prevenir o restringir el derecho de los usuarios de acceder, enviar, recibir y ofrecer cualquier contenido, aplicación o servicio legal a través de la red; **ii)** los PSI no pueden limitar el derecho de los usuarios de hacer uso o introducir cualquier dispositivo en la red, siempre que dichos dispositivos sean legales y no dañen la calidad de la red, **iii)** los PSI deben proveer (bajo solicitud) el servicio de control parental para contenidos que violen las leyes o la moral, y **iv)** los PSI deben publicar en sus sitios web toda la información sobre las características del servicio de Internet ofrecido (Decreto 368, 2011)

Particularmente, el Decreto 368 estable a los PSI la obligación de medir trimestralmente la QoS[11],además del tiempo de reposición de servicio de acceso a Internet[12] y publicar los resultados de forma fácil de entender para el usuario, en un sitio web dedicado como parte del seguimiento a la implementación de la regulación en materia de neutralidad de red (Decreto 368, 2011). Referente al *zero rating*, la SUBTEL decidió, en agosto de 2014, permitir dicha práctica para ciertas aplicaciones, siempre que los usuarios puedan acceder a cualquier página de Internet (Limbatto, 2022).

[11] Tiempo de acceso de usuario, velocidad de transmisión de datos conseguida, proporción de transmisiones de datos fallidas, proporción de accesos de usuario con éxito.

[12] Tiempo de reposición de fallas válidas y el porcentaje de las fallas reparadas en el tiempo establecido por el PSI.

Colombia

En el 2011, en el marco del Plan Nacional de Desarrollo, el Gobierno Colombiano aprobó la Ley 1450 que establece, entre otras cosas, que: i) los proveedores de Internet no pueden bloquear, interferir, discriminar o restringir el derecho de los usuarios finales a acceder, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio, de forma legal, en Internet; ii) los PSI no pueden limitar el derecho de los usuarios de implementar cualquier tipo de dispositivo en la red, siempre que este sea legal y no dañe o impida la calidad de la red; iii) los PSI deben proveer a los usuarios del servicio del control parental para bloquear contenido que violen la ley; iv) los PSI deben publicar en su sitio web toda la información referente a las características de su servicio; v) los PSI deben implementar mecanismos para asegurar la privacidad y protección contra virus y otras amenazas, y vi) los PSI pueden bloquear cierto contenido, aplicación o servicio, siempre que sea a solicitud expresa del usuario.

En este contexto, y en cumplimiento a lo establecido en la Ley 1450, la CRC expidió la Resolución CRC 3502 de 2011, través de la cual, se "establecieron las condiciones regulatorias relativas a la neutralidad en Internet en cumplimiento de lo establecido en el artículo 56 de la Ley 1450 de 2011", para garantizar que los contenidos, aplicaciones o servicios lícitos se mantuvieran abiertos disponibles y accesibles a todos los usuarios, de tal manera que se constituyó, como una norma relevante no solo para las telecomunicaciones, sino para todos los actores que están involucrados en ella, teniendo en cuenta que, para ese momento, en América Latina solo Chile se había pronunciado al respecto (Colombia, 2021).

Es de destacar que la CRC estableció en 2020 que derivado de la pandemia por Covid-19 los PSI podrían priorizar el tráfico para garantizar el acceso del usuario a contenidos o aplicaciones relacionados con los servicios de salud, las páginas gubernamentales y el sector público, actividades laborales, educación y el ejercicio de derechos fundamentales, además estableció que al menos 24 horas antes de iniciar la priorización el PSI debía informar a la CRC sobre la priorización del tráfico (Resolución 5969, 2020).

Estados Unidos

En 2015 a través de la "*Open Internet Order*" (Ley de Internet abierto) emitida por la FCC se establecieron reglas estrictas para los proveedores de banda ancha sobre la gestión de tráfico (FCC, 2015), a saber:

- No pueden bloquear el acceso a contenido legal, aplicaciones, servicios o dispositivos no dañinos;
- No pueden perjudicar o degradar el tráfico legal de Internet sobre la base de contenido, aplicaciones, servicios o dispositivos no dañinos, y
- No pueden favorecer cierto tráfico legal de Internet sobre otro tráfico legal a cambio de una contraprestación de cualquier tipo (sin «*fast lanes*»)

No obstante, debido a intensos debates y al cambio de gobierno, la "Open Internet Order" de febrero de 2015, fue derogada en diciembre de 2017, pues se sostuvo que la neutralidad tal y como había quedado prevista en dicha orden dificultaba el progreso y la inversión en el área de las telecomunicaciones (FCC, 2017).

Además, en el contexto del debate, algunos estados, tales como, California, Colorado, Maine, Nueva Jersey, Oregón, Vermont y Washington, así como Puerto Rico, han establecido sus propias regulaciones. El caso más destacado es el de California, con una Ley de Neutralidad de la Red que entró en vigor en marzo de 2021. La gran relevancia de California radica en el desarrollo de aplicaciones y servicios a través de Internet y, esto, lo vuelve atractivo para establecer un marco normativo apegado al principio de neutralidad de la red, pues ello supone las mejores condiciones para el desarrollo e implementación de nuevos servicios, contenidos y aplicaciones.

California

Como se señaló, la FCC adoptó la orden "*Restore Internet Freedom*" (Restaurar la libertad de Internet) en 2017 para derogar su régimen de neutralidad de la red, reclasificando los servicios de Internet de telecomunicaciones como servicios de información. Según la ley federal, la FCC solo puede regular los servicios de información "según sea necesario en la ejecución de sus funciones". En este contexto, el estado de California promulgó la SB 822 en 2018. Sin embargo, el gobierno federal demandó para detener la aplicación de dicha ley, poco después, retiró la demanda a las pocas semanas de la toma de posesión del presidente Joe Biden. (Cullen, 2022)

Así, California a través de la Ley del SB No. 822 (SB-822, 2018) estableció su regulación de neutralidad de la red, la cual se centra en proteger a los usuarios en el acceso, uso y desarrollo de aplicaciones y servicios, además centra las bases de prácticas como *zero rating*.

Particularmente, la referida ley introdujo una ***prohibición explícita*** de los proveedores de Internet de banda ancha para:

- Bloquear o degradar el tráfico de Internet basado en contenido, aplicaciones, servicios o dispositivos no dañinos, sujeto a una administración de red razonable;
- Interferir con la capacidad de los proveedores de servicios *over-the-top* OTT para ofrecer servicios a los usuarios finales;
- Participar en la priorización pagada de aplicaciones o servicios; y
- Ofrecer paquetes de *zero rating* con fines comerciales o que abarquen solo algunas aplicaciones o servicios, es decir, no eximir el tráfico de toda una categoría de aplicaciones o servicios del límite de datos incluido en la suscripción del usuario final (Cullen, 2022).

Canadá

Canadá regula la neutralidad de la red a través de un marco normativo que establece las medidas de gestión de tráfico permitidas y que se abordan desde cuatro aspectos: transparencia, innovación, claridad y neutralidad competitiva (CRTC, 2009), los cuales se describen a continuación:

- Transparencia: cuando se empleen prácticas de gestión de tráfico los PSI deben ser transparentes sobre su uso;
- Innovación: la inversión en la red es una herramienta fundamental para hacer frente a la congestión de la red, pero la inversión por sí sola no elimina la necesidad gestionar el tráfico de la red;
- Neutralidad competitiva: para los servicios minoristas, los PSI pueden realizar prácticas de gestión de tráfico sin la aprobación previa de la CRTC. Sin embargo, la CRTC revisará dichas prácticas. Para los servicios mayoristas habrá una observación adicional. Cuando un PSI realice prácticas de gestión de tráfico más restrictivas para sus servicios mayoristas que, para sus servicios minoristas, esto requerirá la aprobación de la CRTC, y
- Claridad: los PSI deben asegurar que cualquier práctica de gestión de tráfico que empleen no sea injustamente discriminatorio ni indebidamente preferencial.

La CRTC establece un enfoque basado en el equilibrio entre la libertad de los usuarios finales de usar Internet para diversos fines y el interés legítimo de los PSI para administrar el tráfico generado en sus redes. No obstante, se establece que los PSI deben ser transparentes en el uso de prácticas de gestión de tráfico, además de comunicar el costo de sus servicios con el objetivo de empoderar al usuario y favorecer la libre competencia (CRTC, 2009).

Ecuador

A través de la "Ley de Orgánica de Telecomunicaciones de 2015", el gobierno ecuatoriano publicó la regulación de gestión del tráfico y el acceso a Internet con un enfoque en los derechos de los usuarios. En el Art. 22 de la ley se reconoce el derecho a los usuarios de acceder a cualquier aplicación o servicio permitido disponible en Internet (Ley Orgánica de Telecomunicaciones, 2015).

La ley también señala que los PSI no podrán limitar, bloquear, interferir, discriminar, entorpecer o restringir el derecho de sus usuarios de utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación de Internet, y señala que los PSI tampoco podrán limitar el derecho de los usuarios de utilizar cualquier dispositivo para acceder a Internet (Ley Orgánica de Telecomunicaciones, 2015).

La regulación autoriza a los usuarios a poner controles parentales si así lo desean y permite a los PSI la implementación de acciones técnicas que consideren necesarias para la adecuada administración de la red y garantizar el servicio de Internet. Por otro lado, la ley señala que los PSI pueden establecer planes tarifarios constituidos por uno o varios servicios o por uno o varios productos de un servicio, de conformidad con su título de concesión, autorización o registro del servicio; los PSI deben publicar en su página web y proporcionar la información acerca de sus planes, promociones, tarifas y precios

en los formatos y condiciones que se determina la regulación (Ley Orgánica de Telecomunicaciones, 2015).

Perú

En las normas de aplicación de la Neutralidad de la Red de Osiptel, que se encuentran vigentes desde enero de 2017, se estableció que los PSI no pueden bloquear, interferir, discriminar o restringir arbitrariamente el derecho de los usuarios a utilizar una aplicación o protocolo, independientemente de su origen, destino, naturaleza o propiedad (Reglamento de la Neutralidad de la Red, 2016). Adicionalmente, dicho reglamento establece cuatro principios sobre la neutralidad de la red, a saber: libertad de uso, cautela, equidad y transparencia.

Las medidas de gestión de tráfico están permitidas. No obstante, los PSI no deben filtrar o bloquear arbitrariamente servicios y aplicaciones legales; además, no tienen permitido realizar diferenciación arbitraria en la oferta comercial de productos de acceso a Internet y en materia de *zero rating* los PSI tienen la posibilidad de ofertar planes que realicen tratamiento diferenciado, empresas como Entel Perú, Movistar, Claro y Bitel ofrecen este tipo de servicios. (Limbatto, 2022)

Por otra parte, los PSI están obligados a poner a disposición del público en general, a través de su sitio web, la información relativa a la Neutralidad de Red y las medidas que implemente en sus redes (Reglamento de la Neutralidad de la Red, 2016). La regulación peruana permite a los usuarios establecer quejas o reclamos si considera que se ha violado la Neutralidad de la Red.

En la siguiente tabla se muestra un escenario resumido sobre la regulación existente en los países antes descritos, respecto a la neutralidad de la red.

Tabla 1 Resumen de la experiencia internacional en materia de neutralidad de red en el Continente Americano[13].

País	Año	Nombre de la regulación	¿Los PSI Pueden realizar prácticas de gestión de tráfico?	¿Existen parámetros de calidad mínima en el contexto de la regulación de neutralidad de red?	¿Hay regulación específica sobre *zero rating?*	¿Hay regulación sobre *servicios especializados?*	¿Existen medidas transparencia respecto de la gestión de tráfico?
Argentina	2014	Ley Argentina Digital	Sí	No	No	No	No
Brasil	2014	Marco Civil de Internet de 2014 y el Reglamento 8771 de 2016	Sí	No	No	Sí	Sí
Canadá	2009	CRTC 2009-657	Sí	No	Sí	Sí (prohibición general, sujeta a revisión)	Sí
Chile	2010	Ley 20.453 de 2010 y el Reglamento de Aplicación de la Ley de Neutralidad de la Red de 2011	Sí	No. Sin embargo, se establece lo obligación de que los PSI publiquen sus velocidades mínimas y condiciones de calidad.	Sí	No	Sí
Colombia	2011	Normas de Aplicación de la Neutralidad de la Red	Sí	No	Sí	No	Sí
Ecuador	2015	Ley de Telecomunicaciones	Sí	No	No	No	No

[13] Fuente: elaboración propia con información de Cullen International.

País	Año	Nombre de la regulación	¿Los PSI Pueden realizar prácticas de gestión de tráfico?	¿Existen parámetros de calidad mínima en el contexto de la regulación de neutralidad de red?	¿Hay regulación específica sobre *zero rating?*	¿Hay regulación sobre *servicios especializados?*	¿Existen medidas transparencia respecto de la gestión de tráfico?
Estados Unidos de América			Sí	No	Derogada	Derogada	No
California	2018	Ley del Senado No. 822	Sí	No	Sí	Sí	Sí
Perú	2012	En 2012 la Ley de promoción de la banda ancha y construcción de la red dorsal nacional de fibra óptica y las Normas de aplicación de la neutralidad de la red en 2017	Sí	No	Sí	No	Sí

Unión Europea

Reglamento (UE) 2015/2120

En los países que integran a la Unión Europea[14], la neutralidad de la red está regulada por el "Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas relativas al acceso abierto a Internet y se modifica la Directiva 2002/22/CE sobre el servicio universal y los derechos de los usuarios en relación con las redes y servicios de comunicaciones electrónicas y el Reglamento (UE) n.º 531/2012 sobre la itinerancia en las redes públicas de comunicaciones móviles dentro de la Unión" , en lo sucesivo el Reglamento. (Europeo, 2015)

De acuerdo con Hruba[15] el Reglamento introduce normas directamente vinculantes para toda la UE sobre la protección del acceso abierto a Internet (neutralidad de la red) que se aplican a partir de abril de 2016. Estas normas exigen a los PSI, entre otras cosas, que traten todo el tráfico por igual; y establecen el derecho de todos los usuarios finales a acceder y distribuir contenidos, aplicaciones y servicios legales de su elección.

Particularmente, el Reglamento señala que los PSI pueden utilizar medidas razonables de gestión del tráfico. Tales medidas deben basarse en requisitos técnicos objetivos, no en consideraciones comerciales. El bloqueo o la limitación solo se permite en un número limitado de circunstancias enumeradas en el reglamento, por ejemplo, para bloquear contenido ilegal, contrarrestar un ataque cibernético o tratar congestiones de tráfico excepcionales o temporales.

El Reglamento también permite acuerdos sobre servicios especializados para contenido específico cuando sea necesaria la optimización, bajo la condición de que los PSI garanticen la calidad general de los servicios de acceso a Internet. Ejemplos de estos servicios especializados son la IPTV gestionada y las videoconferencias de alta definición.

Lineamientos para la implementación de la Regulación del Internet Abierto

BEREC emitió en el 2016 los Lineamientos para la implementación del Reglamento por parte de los reguladores nacionales, el objetivo de dichos lineamientos es proporcionar orientación sobre la correcta implementación de las obligaciones de las autoridades regulatorias nacionales en materia de neutralidad de red, esto es, sobre las obligaciones de asegurar el cumplimiento de las reglas para salvaguardar el trato no discriminatorio del tráfico en la provisión del SAI y los derechos los usuarios

[14] Alemania, Bélgica, Croacia, Dinamarca, España, Francia, Irlanda, Letonia, Luxemburgo, Países Bajos, Suecia, Bulgaria, Eslovaquia, Estonia, Grecia, Malta, Polonia, República Checa, Austria, Chipre, Eslovenia, Finlandia, Hungría, Italia, Lituania, Portugal y Rumanía.

[15] Cullen International. Disponible en: https://www.cullen-international.com/client/site/documents/TRMEEU20190245?version=this

finales. De acuerdo con BEREC los Lineamientos deben contribuir a la aplicación coherente del Reglamento.

Posteriormente, en octubre de 2019 BEREC inició un proceso de consulta pública en el que propuso un borrador de los Lineamientos actualizado. BEREC recibió 52 respuestas de diversos tipos de partes interesadas.

Los cambios propuestos se resumen a continuación:

- Nombre de los Lineamientos. Se requiere la adopción de un nombre que esté alineado con la "Regulación de Internet Abierta"
- Servicios especializados. BEREC establece un precedente al señalar que las reglas de neutralidad no constituyen un impedimento para el despliegue de tecnologías 5G.
- Dispositivos M2M e IoT. BEREC encuadra los requerimientos de M2M y IoT en el tipo de servicios especializados, por lo que su implementación y provisión estaría a en línea con la regulación de neutralidad de la red.
- Evaluación de servicios especializados. Considerando la evolución tecnológica, BEREC sugiera una revisión periódica de los servicios especializados que son hoy provistos, toda vez que en el futuro podrían ya no clasificar en la misma categoría.
- Zero rating. BEREC amplía la definición de prácticas de *zero rating* y adiciona una serie de ejemplos y una guía para la evaluación ex post de dichas prácticas.

Después del correspondiente proceso de análisis de comentarios recibidos, BEREC publicó una nueva versión de los "Lineamientos para la Implementación de la Regulación de Internet Abierta", los cuales entraron en vigor en junio de 2020.

Adicionalmente, en una reciente interpretación del TJUE respecto a los casos relacionados con tarifas de *zero rating*, dicho tribunal señala que las ofertas de *zero rating* serían incompatibles con el Reglamento de Internet Abierta de la UE[16]. BEREC se encuentra evaluando actualmente los detalles de las sentencias emitidas por TJUE el 2 de septiembre de 2021 en relación con la violación del Reglamento de Internet Abierta (C 34/20 – Telekom Deutschland, C-854/19 – Vodafone y C-5/20 – Vodafone). Esta evaluación, de acuerdo con BEREC, ayudará a preparar la revisión de las Lineamientos para la Implementación del Reglamento sobre Internet abierta en consonancia con las sentencias del TJUE.

En consecuencia, Durante su 48ª reunión plenaria (30 de septiembre de 2021, Dubrovnik), el Consejo de Reguladores decidió lanzar una convocatoria a todas las partes interesadas para ofrecerles la

[16] En el Anexo 1B, se detalla la interpretación del TJUE en relación con las tarifas de *zero rating.*

oportunidad de compartir sus puntos de vista sobre las resoluciones del TJUE sobre el *zero ratin*g con una justificación adecuada que respalde su comprensión.

Por su parte, BEREC en abril de 2022, sometió a consulta pública una nueva versión de los Lineamientos de referencia y se espera que esta sea aprobada a principios de junio de 2022 (International, 2022).

Finalmente, el 9 de junio de 2022 BEREC aprobó y publicó los "Lineamientos para la implementación de la regulación del internet abierto". Dichos lineamientos fueron revisados a la luz de las sentencias del TJCE relativas a la interpretación de los artículos específicos del Reglamento. Al respecto, se destaca que uno de los cambios importantes de estos lineamientos es que BEREC considera que cualquier práctica de diferenciación de precios que no sea independiente de la aplicación es inadmisible para las ofertas de los PSI, tal es el caso de aplicar zero rating a las aplicaciones propias de los PSI. (BEREC, 2022)

III3 México

Antecedentes

El 11 de junio de 2013 fue publicado en el DOF el "Decreto por el que se reforman y adicionan diversas disposiciones de los artículos 6o., 7o., 27, 28, 73, 78, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos, en materia de telecomunicaciones ", mediante el cual se creó el Instituto como un órgano autónomo con personalidad jurídica y patrimonio propio, cuyo objeto es regular, promover y supervisar el uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de radiodifusión y telecomunicaciones, además de ser la autoridad en materia de competencia económica en los sectores de los servicios antes referidos.

En este contexto, en la LFTR publicada en el DOF el 14 de julio de 2014, el capítulo referente a la neutralidad de la red establece lo siguiente:

> ***Capítulo VI De la Neutralidad de las Redes***
>
> ***Artículo 145.*** *Los concesionarios y autorizados que presten el servicio de acceso a Internet deberán sujetarse a los lineamientos de carácter general que al efecto expida el Instituto conforme a lo siguiente:*
>
> *I.* ***Libre elección****. Los usuarios de los servicios de acceso a Internet podrán acceder a cualquier contenido, aplicación o servicio ofrecido por los concesionarios o por los autorizados a comercializar, dentro del marco legal*

aplicable, sin limitar, degradar, restringir o discriminar el acceso a los mismos. No podrán limitar el derecho de los usuarios del servicio de acceso a Internet a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos que se conecten a su red, siempre y cuando éstos se encuentren homologados;

II. No discriminación. Los concesionarios y los autorizados a comercializar que presten el servicio de acceso a Internet se abstendrán de obstruir, interferir, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicio;

III. Privacidad. Deberán preservar la privacidad de los usuarios y la seguridad de la red;

IV. Transparencia e información. Deberán publicar en su página de Internet la información relativa a las características del servicio ofrecido, incluyendo las políticas de gestión de tráfico y administración de red autorizada por el Instituto, velocidad, calidad, la naturaleza y garantía del servicio;

V. Gestión de tráfico. Los concesionarios y autorizados podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red conforme a las políticas autorizadas por el Instituto, a fin de garantizar la calidad o la velocidad de servicio contratada por el usuario, siempre que ello no constituya una práctica contraria a la sana competencia y libre concurrencia;

VI. Calidad. Deberán preservar los niveles mínimos de calidad que al efecto se establezcan en los lineamientos respectivos, y

VII. Desarrollo sostenido de la infraestructura. En los lineamientos respectivos el Instituto deberá fomentar el crecimiento sostenido de la infraestructura de telecomunicaciones.

Artículo 146. Los concesionarios y los autorizados deberán prestar el servicio de acceso a Internet respetando la capacidad, velocidad y calidad contratada por el usuario, con independencia del contenido, origen, destino, terminal o aplicación, así como de los servicios que se provean a través de Internet, en cumplimiento de lo señalado en el artículo anterior.

En el ejercicio de las facultades conferidas por los artículos 145 y 146 de la LFTR, el 11 de diciembre de 2019 el Pleno del Instituto, en su XXXIV Sesión Ordinaria, mediante Acuerdo P/IFT/111219/876 aprobó el "Acuerdo mediante el cual el Pleno del Instituto determina someter a consulta pública el Anteproyecto de lineamientos para la gestión de tráfico y administración de red a que deberán

sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet", por un periodo de 45 días hábiles para el desarrollo de la consulta pública. Posteriormente, el 4 marzo de 2020 el Pleno del Instituto, en su VI Sesión Ordinaria, mediante Acuerdo P/IFT/040320/83, acordó ampliar el plazo de la consulta pública por 20 días hábiles, por lo que concluyó dicho proceso el 15 de julio de 2020.

Derivado del proceso de consulta pública, el Instituto recibió un total de 75,595 participaciones (IFTb, 2021), de las cuales publicó un total de 74,065[17] que presentaron manifestaciones, opiniones, comentarios y propuestas concretas; de estas, 73,645 fueron participaciones derivadas de la iniciativa Salvemos Internet[18] y 420 fueron participaciones de personas físicas (381) y morales (39), entre los que se destacan Facebook, Mozilla México, Nokia Operations de México, Hispasat México, GSMA, PEGASO, AT&T, CANIETII, ASIET, ANATEL,UNESCO, entre otros.

Considerando la nutrida participación en el proceso de consulta pública, del 9 de junio al 07 de julio de 2020 el Instituto llevó a cabo el Foro virtual "Neutralidad de la red en México. Análisis y debate", en el que se desarrollaron 5 mesas de discusión en las cuales se abordaron los temas de i) técnicas de gestión de tráfico y administración de red; ii) brecha digital; iii) servicios especializados; iv) derechos de los usuarios; v) servicios diferenciados. En dicho foro se contó con la participación de autoridades, académicos, asociaciones civiles, especialistas en materia de neutralidad de red, integrantes de la industria y personal del Instituto[19].

Así, el 28 de junio de 2021, en su XI Sesión Extraordinaria, mediante Acuerdo P/IFT/EXT/280621/13 el Pleno del Instituto aprobó el "Acuerdo mediante el cual el Instituto Federal de Telecomunicaciones expide los Lineamientos para la gestión del tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet", en lo sucesivo los Lineamientos NN. Los lineamientos fueron publicados en el DOF el 5 de julio de 2021 y entraron en vigor el 3 de septiembre de 2021.

Adicionalmente, respecto del Artículo 11 de los Lineamientos de NN que a la letra señala:

> " Los PSI que cuenten con ofertas con patrocinio de datos en términos de la fracción I del artículo 8, que provean acceso a contenidos, aplicaciones y/o

[17] Total de participaciones publicadas disponibles en: http://www.ift.org.mx/industria/consultaspublicas/comentarios/?nid=13791, con excepción de 1530 participaciones, dado que estas fueron presentadas en contravención a lo establecido en el artículo 8° de la Constitución Política de los Estados Unidos Mexicanos, que a la letra señala: Artículo 8°. Los funcionarios y empleados públicos respetarán el ejercicio del derecho de petición, siempre que esta se formule por escrito, de manera pacífica y respetuosa.

[18] https://salvemosinternet.mx/

[19] Serie de videos disponibles en: https://www.youtube.com/watch?v=8N9HtnswAPA

> servicios en términos del artículo 9 y/o que provean servicios en términos del artículo 10 deberán presentar ante el Instituto, en formato electrónico editable dentro de los 10 (diez) días hábiles siguientes al término de cada semestre, en los términos y formato que al efecto determine el Instituto, un informe semestral que incluya, al menos, lo siguiente:
>
> I. Respecto a las ofertas con patrocinio de datos, la referencia al contenido, aplicación o servicio patrocinado, la persona física o moral que patrocina los datos y el folio de inscripción del Registro Público de Concesiones que contenga la tarifa contratada.
>
> II. Respecto a las ofertas de servicios en términos del artículo 10, un listado y descripción de cada uno de los servicios provistos en el periodo reportado. (IFTa, 2021)"

Así como del transitorio:

> "Cuarto. El Instituto publicará en el Diario Oficial de la Federación el formato para la entrega del informe al que refiere el artículo 11 de los Lineamientos a más tardar al cierre del primer trimestre de 2022."

El Instituto, en 2021, llevó a cabo la consulta pública sobre el "Anteproyecto mediante el cual se definen los términos y el formato relativos al informe que deberán presentar los concesionarios y autorizados que presten el servicio de acceso a Internet"[20], esta consulta pública estuvo abierta durante veinte días, del 20 de diciembre de 2021 al 28 de enero de 2022.

Posterior al análisis de la información, comentarios, opiniones, aportaciones que se recibieron de la consulta pública, el Instituto publicó en el DOF el "Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones establece los términos y formato relativos al informe que deberán presentar los concesionarios y autorizados que presten el servicio de acceso a Internet" el 30 de marzo de 2022, el cual señala (IFT, 2022):

- Los términos y formato bajo los cuales los PSI deberán entregar al IFT el informe semestral señalado en el Art.11;
- Los PSI deberán cumplir con el Anexo A referido a la Información de Identificación y el Anexo B el Formato para la Presentación del Informe de Ofertas y Servicios, y

[20] Obtenido de http://www.ift.org.mx/industria/consultas-publicas/consulta-publica-sobre-el-anteproyecto-mediante-el-cual-se-definen-los-terminos-y-el-formato

- El informe semestral se entregará 10 días después del término de cada semestre en la Ventanilla Electrónica[21] del IFT[22].

En la siguiente figura se resumen los hitos del proceso normativo de la neutralidad de la red en México

Ilustración 3 Hitos del marco normativo nacional respecto de la neutralidad de la red[23]

[21] De acuerdo con el transitorio cuarto del "Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones establece los términos y formato relativos al informe que deberán presentar los concesionarios y autorizados que presten el servicio de acceso a Internet conforme a lo establecido en el Acuerdo P/IFT/EXT/280621/13", hasta en tanto el trámite se migre a un formato electrónico que se encuentre contenido en la Ventanilla Electrónica, los PSI deberán entregar los informes de ofertas de patrocinio de datos y otros servicios de telecomunicaciones de manera física ante la oficialía de partes común del Instituto, salvo que el PSI opte por el correo electrónico o por algún esquema que sustituya a este último y que se encuentre considerado en los "Lineamientos para sustanciación de los trámites y servicios que se realicen ante el Instituto Federal de Telecomunicaciones, a través de la Ventanilla Electrónica" y sus modificaciones.

[22] Si la información requerida no cumple con los términos y formatos establecidos, se les extenderá un plazo de 40 días más, en caso de prevención el PSI tendrá un plazo de 10 días para subsanar la omisión que corresponda, y en caso de no ser subsanada se turnará a la Unidad de Cumplimiento.

[23] Elaboración propia con información de https://www.dof.gob.mx/nota_detalle.php?codigo=5622965&fecha=05/07/2021#gsc.tab=0

Aspectos generales de los Lineamientos NN

El Instituto advirtió que, con la aprobación de los Lineamientos, se pretendía contribuir en: **i)** garantizar que el usuario final tuviera libertad de decisión sobre los contenidos, aplicaciones y servicios a los que accedería a través del SAI, así como conocimiento de la forma en que se gestiona su tráfico y se administra la red; **ii)** otorgaría certidumbre jurídica a la industria en materia de neutralidad de red, dando claridad sobre las políticas de gestión de tráfico y administración de red permitidas, así como respecto de los servicios y ofertas que podrían poner a disposición de los usuarios finales y PACS; **iii)** fomentaría la innovación del sector mediante el uso de tecnologías más eficientes en el uso de las redes; **iv)** favorecería la disminución de la brecha digital, a través de ofertas comerciales con objetivos específicos; **v)** promovería condiciones de competencia y libre concurrencia, y **vi)** incentivaría la inversión en redes para la provisión de acceso a Internet fijo y móvil con mayor calidad y más cobertura (IFTa, 2021).

Al respecto, resulta importante destacar los siguientes elementos previstos en los Lineamientos NN (IFTa, 2021):

Sujetos obligados

Los concesionarios y autorizados que presten, a través de redes públicas de telecomunicaciones (PSI), el SAI al usuario final, así como los permisionarios que también lo puedan hacer bajo su título habilitante, no así los concesionarios con concesiones únicas para uso público, social o privado, ni aquellos que, aun teniendo una concesión para uso comercial, no provean el servicio de acceso a Internet a los usuarios finales.

Contenido de los Lineamentos NN

1. *Gestión de tráfico*
    - Los PSI pueden implementar políticas de gestión de tráfico y administración de red que estén encaminadas a: **i)** asegurar la calidad; capacidad y velocidad del SAI, y **ii)** preservar la integridad y seguridad de la red.
    - Al implementar las políticas de gestión, los PSI deben observar: **i)** la libre elección de los usuarios finales para acceder a los contenidos, aplicaciones y servicios en Internet, sin que dificulten, limiten, degraden restrinjan o discriminen el acceso a los mismos, **ii)** el trato no discriminatorio a los usuarios finales, PACS , tipos de tráfico similares, así como el tráfico propio y el de terceros que curse por la red; **iii)** la

privacidad de los usuarios finales, y **iv)** la inviolabilidad de las comunicaciones privadas de los usuarios finales.

- Los PSI, al aplicar gestión de tráfico, no pueden en ninguna circunstancia, inspeccionar, monitorear o alterar el contenido específico del tráfico que curse por la red.

2. *Excepción a la regla de gestión de tráfico*
   - Los PSI no deben implementar políticas de gestión de tráfico que resulten en la limitación, degradación, restricción, discriminación, obstrucción, interferencia, filtrada o bloqueo, salvo en: **i)** riesgo, técnicamente comprobable, a la integridad y seguridad de la red, a la privacidad de los usuarios finales o la inviolabilidad de sus comunicaciones privadas; **ii)** congestión excepcional y temporal de la red , y **iii)** situaciones de emergencia y desastres que pongan en riesgo la operación de la red.
3. *Dispositivos homologados*
   - Los PSI deben respetar el derecho de los usuarios finales a incorporar o utilizar cualquier clase de instrumentos/dispositivos terminales que se conecten más allá del punto de conexión terminal de una red pública de telecomunicaciones, siempre que estos se encuentren homologados.
4. *Servicios/ofertas comerciales asociadas a las políticas de gestión de tráfico*
   - Los PSI no pueden ofrecer a los usuarios finales ofertas que proporcionen acceso a un subconjunto de contenidos, aplicaciones o servicios disponibles en Internet, salvo que consista en un servicio de telecomunicaciones que no requiere establecer una conexión a Internet.
   - Las ofertas del SAI que los PSI pongan a disposición de los usuarios finales podrán considerar: **i)** patrocinio de datos por un tercero, **ii)** patrocinio de datos (*zero rating*) por el mismo PSI, **iii)** *zero rating* sujeto a la vigencia del plan o paquete del SAI contratado por el usuario final, y **iv)** modificación de la velocidad de transmisión de datos una vez alcanzado el tope de datos, siempre y cuando dicha modificación se aplique por igual a todos los contenidos aplicaciones o servicios.
   - Los PSI podrán ofrecer paquetes de *zero rating* sin restricciones a disponibilidad de datos o de vigencia de un plan o paquete del SAI de: i) las autoridades, dependencias, entidades, órganos y organismos de los Poderes Ejecutivo, Legislativo y Judicial, en el ámbito federal, estatal o municipal, así como de órganos y organismos autónomos, que contribuyan con la reducción de la brecha digital en el ámbito de sus atribuciones sustantivas, ii) de las instituciones del sistema financiero con el objetivo de promover la inclusión financiera digital, o iii) de los PSI para permitir a los usuarios finales realizar consultas, recargas, pagos y contrataciones de los servicios de telecomunicaciones.
   - Los PSI pueden proveer servicios de telecomunicaciones mediante la asignación de características y recursos de red específicos, en tanto, cumplan con alguno de los siguientes criterios: i) provean un contenido, aplicación y/o servicio que requiere de

parámetros técnicos inherentes y exclusivos al contenido, aplicación o servicio de que se trate, que no puede replicarse en condiciones óptimas a través del SAI; provean funcionalidades adicionales, mediante la transmisión de datos entre aplicaciones, dispositivos, plataformas u otros equivalentes, que no puedan ser replicadas a través del SAI, o iii) consistan en un servicio de telecomunicaciones que no requiere establecer una conexión con Internet. Lo anterior, sin detrimento de la calidad del SAI, por lo que se debe asegurar la capacidad suficiente en la red.

5. *Transparencia e información*
    - Los PSI que cuenten con ofertas de patrocinio de datos[24] deberán presentar ante el Instituto un informe semestral que incluya, al menos, lo siguiente:
        - La referencia al contenido, aplicación o servicio patrocinado, la persona física o moral que patrocina los datos y el folio de inscripción en el RPC que contenga la tarifa contratada.
        - Un listado y descripción de cada uno de los servicios provistos en el periodo reportado[25].
    - Los PSI deben publicar su código de políticas de gestión de tráfico y administración de red, dicho código debe contener, al menos, las políticas aplicadas, en qué consisten, los casos y para qué se emplean, los impactos de su implementación, las posibles afectaciones, las recomendaciones para los usuarios, las referencias actualizadas y la fecha de última actualización.
    - Los PSI deberán entregar al Instituto aquella información que les requiera sobre el seguimiento de la implementación y resultados de los Lineamientos.
6. *Obligaciones para el Instituto*
    - Publicar anualmente (30 de abril de cada año[26]) un informe relacionado con la implementación de los lineamientos.
    - En cualquier momento, el Instituto podrá determinar la suspensión de las políticas de gestión de tráfico y administración de red específicas, o bien, de servicios puestos a disposición de los usuarios finales o PACS, de advertir que contravienen lo dispuesto en los Lineamientos o que afectan negativamente el desarrollo de la competencia y libre concurrencia en la provisión del SAI.
    - El Instituto podrá requerir a los PSI realizar adecuaciones a sus códigos de políticas de gestión de tráfico y administración de red de considerar que no se apegan a lo estipulado respecto al código de políticas.

[24] En términos de la fracción I del artículo 8, que provean acceso a contenidos, aplicaciones y/o servicios en términos del artículo 9 y/o que provean servicios en términos del artículo 10 de los Lineamientos NN.

[25] Respecto a las ofertas de servicios en términos del artículo 10 de los Lineamientos NN.

[26] El primer informe está previsto para abril de 2023.

De lo anterior, se desprende que el Instituto mandató un esquema regulatorio basado en "principios" a través del establecimiento de las políticas de gestión de tráfico y administración de red que pueden implementar los PSI, así como las prácticas comerciales asociadas a ello. Adicionalmente, el Instituto fue claro al señalar las obligaciones en materia de transparencia y los mecanismos a través de los cuales dará cuenta del estado de la implementación de los Lineamientos.

Ahora bien, de acuerdo con Julia Black y otros autores (2007, p. 191), la regulación basada en principios fue introducida en la jurisdicción del Reino Unido en 1990, mediante la regulación de los servicios financieros. Para dichos autores, la regulación basada en principios requiere apartarse de la regulación basada en reglas altamente prescriptivas para apoyarse en determinados principios que establezcan estándares para que los regulados conduzcan sus actividades conforme a estos. (Black, et al., 2007, pp. 192,193)

Al respecto, esta aproximación regulatoria basada en principios tiene por lo menos tres elementos principales (Black, et al., 2007, pp. 192,193):

1. *Principios*. Diseñados con alto nivel de generalidad, que permitan su aplicación flexible en industrias de rápidos cambios, que sean razonables y enfocados en el propósito de lo que deben cumplir;
2. *Resultados*. El enfoque debe ser en los resultados, no en los procesos que los regulados deben seguir para llegar a dichos resultados, por lo que la regulación no prescribe esos procesos, sino que define el objetivo a lograr, y
3. *Responsabilidad de los regulados*. Se traslada en gran medida la responsabilidad a los sujetos regulados, para que estos definan la mejor manera de organizarse a fin de dar cumplimiento a los resultados establecidos por el regulador.

En este contexto, el establecer el resultado al que se quiere llegar, se permite que la regulación sea flexible y sea más fácil de cumplir y, si bien es cierto que la regulación basada en reglas da mayor certeza por el grado de detalle de sus reglas, esta podría llevar a resultados no deseados y rigidez que podría no ser apta para los cambios tecnológicos que existen. (Black, et al., 2007, pp. 192,193) En línea con lo anterior, el Instituto señaló que los resultados a los que buscaría llegar con la aprobación de los Lineamientos eran: : i) garantizar que el usuario final tuviera libertad de decisión sobre los contenidos, aplicaciones y servicios a los que accedería a través del SAI, así como conocimiento de la forma en que se gestiona su tráfico y se administra la red; ii) otorgar certidumbre jurídica a la industria en materia de neutralidad de red, dando claridad sobre las políticas de gestión de tráfico y administración de red permitidas, así como respecto de los servicios y ofertas que podrían poner a disposición de los usuarios finales y PACS; iii) fomentar la innovación del sector mediante el uso de tecnologías más eficientes en el uso de las redes; iv) favorecer la disminución de la brecha digital, a través de ofertas comerciales con objetivos específicos; v) promover condiciones de competencia y libre concurrencia, e vi) incentivar la inversión en redes para la provisión de acceso a Internet fijo y móvil con mayor calidad y más cobertura (IFTa, 2021).

Sin embargo, bajo este modelo regulatorio basado en principios, si bien se traslada en gran medida la responsabilidad a los sujetos regulados, para que estos definan la mejor manera de organizarse a fin de dar cumplimiento, no puede dejarse de lado que, como se describirá en la siguiente sección, un sistema normativo debe considerar elementos de monitoreo que aseguren no solo la implementación de las reglas, sino su cumplimiento y, con ello, se alcancen, eventualmente, los objetivos que dieron origen a dicho sistema normativo.

III4 Sistema Normativo

De acuerdo con (OCDE(a), 2019),la regulación es el conjunto de normas jurídicas de distintos niveles jerárquicos que definen la participación de las personas o las empresas en un mercado, en un sector o en alguna actividad económica o social. El proceso mediante el cual se establecen e implementan estas reglas puede definir su pertinencia, importancia y efecto sobre el sujeto y el objeto de la normativa. Lo anterior, implica que el proceso de emisión de la normativa determina la calidad de la misma y tiene un efecto directo sobre los resultados o consecuencias de la política pública.

Al respecto, la OCDE señala que la calidad en el proceso de emisión de la normativa tiene un efecto directo sobre los resultados previstos una vez que se pone en marcha (incluso, es frecuente que se generen efectos que no fueron identificados). Esto significa que el proceso de emisión de normativa tiene una influencia importante sobre el cumplimiento de los objetivos planteados y el posible beneficio neto potencial.

Lo anterior se considera así, toda vez que una regulación puede abrir o cerrar mercados; puede promover la eliminación de monopolios o su formación; puede generar barreras de entrada; puede reducir o impulsar los incentivos para innovar o emprender; etc. También puede asegurar la calidad de servicios públicos como la educación, salud, entre otros.

En consecuencia, la OCDE también advierte la importancia de revisar y mejorar el proceso por el cual se emite la normativa, para asegurar que esta se ha planteado en la dirección correcta y tiene como objetivo resolver un problema específico.

En este contexto, el diseño de las normas son un factor clave tanto para las empresas como para los ciudadanos, pero también lo es la forma en la que las regulaciones se implementan y cumplen, y la forma en la que se promueve el cumplimiento del marco regulatorio resulta un determinante crítico para que el sistema normativo cumpla con los objetivos para los que fue diseñado. (OCDE, 2019)

Entonces, la OCDE desarrolló una Guía para el Cumplimiento Regulatorio y las Inspecciones basada en 12 criterios, que se constituyen como una herramienta para los gobiernos y los órganos reguladores para la evaluación del grado de desarrollo del sistema de inspecciones y de cumplimiento

de las normas en una jurisdicción, institución o estructura específica, para identificar fortalezas, debilidades y oportunidades de mejora.

Los doce criterios son (OCDE, 2019):

1. *Cumplimiento basado en evidencia*: Las inspecciones y la promoción del cumplimiento de las normas deben basarse en evidencia y en indicadores: la toma de decisiones sobre qué y cómo inspeccionar debe fundamentarse en datos y evidencia y los resultados deben ser evaluados con regularidad.
2. *Selectividad:* En la medida de lo posible, la promoción del cumplimiento y la aplicación de las normas deben ser dejadas a las fuerzas del mercado, al sector privado y la sociedad civil: las inspecciones y la promoción del cumplimiento no pueden llevarse a cabo en todos los entes regulados ni pueden atender todas las situaciones. Existen muchas formas de lograr los objetivos de las normas y su cumplimiento.
3. *Enfoque de riesgo y proporcionalidad:* La promoción del cumplimiento de las normas debe hacerse según los riesgos involucrados y proporcionalmente: la frecuencia de las inspecciones y los recursos a emplear deben ser proporcionales al nivel de riesgo y las acciones de cumplimiento de las normas deben dirigirse a la reducción de los riesgos reales derivados de las infracciones.
4. *Regulación responsiva:* El hacer cumplir las normas debe basarse en principios de "regulación responsiva"; es decir, las acciones de promoción del cumplimiento e inspecciones deben ser adecuadas al perfil y al comportamiento de los sujetos regulados.
5. *Visión a largo plazo:* Los gobiernos deben adoptar políticas en materia de inspecciones y promociones del cumplimiento de las normas y establecer mecanismos institucionales con objetivos definidos y una estrategia de largo plazo.
6. *Coordinación y consolidación:* Las actividades de inspección deben ser coordinadas y, cuando sea necesario, consolidadas: con menos duplicaciones y superposiciones se asegura un mejor uso de los recursos públicos, minimizando la carga en los administrados y maximizando la efectividad.
7. *Gobernanza transparente:* Las estructuras de gobernanza y las políticas de recursos humanos deben basarse en la transparencia, el profesionalismo y la gestión de resultados. Las acciones para la promoción del cumplimiento de las normas deben estar libres de toda influencia política y los esfuerzos deben ser recompensados.
8. *Integración de la información:* Se debe emplear tecnologías de la información para maximizar un enfoque de riesgos, promover la coordinación y el intercambio de información y asegurar el uso óptimo de los recursos.
9. *Procesos claros y justos:* Los gobiernos deben asegurarse que las reglas y los procesos para las in secciones y la promoción del cumplimiento sean claros. Se debe adoptar y difundir legislación coherente y adecuada; los derechos y obligaciones de los funcionarios y de las empresas deben estar claramente establecidos.

10. ***Promoción del cumplimiento:*** Se debe promover la transparencia y el cumplimiento de las normas mediante el empleo de instrumentos adecuados como guías, herramientas y listas de verificación.
11. ***Profesionalismo***: Los inspectores deben ser capacitados y dirigidos de manera que se asegure su profesionalismo, integridad, consistencia y transparencia. Todo ello exige un entrenamiento sustancial, con un enfoque no solo en lo técnico, sino también en destrezas generales relacionadas con los lineamientos vinculados a la promoción del cumplimiento y las inspecciones, a fin de asegurar consistencia e imparcialidad.
12. ***"Poniendo los pies sobre la tierra":*** Las instituciones a cargo de las inspecciones y de hacer cumplir la normatividad- así como la totalidad del sistema de promoción del cumplimiento- deben alcanzar los niveles de desempeño que se espera de ellos en términos de satisfacción de los interesados, eficiencia (beneficios/costos) y efectividad general (seguridad, salud, protección ambiental, entre otros).

En suma, los mecanismos de monitoreo que se implementen para vigilar el cumplimiento del principio de neutralidad de red, teóricamente, tendrían que considerar los doce criterios previstos por la OCDE.

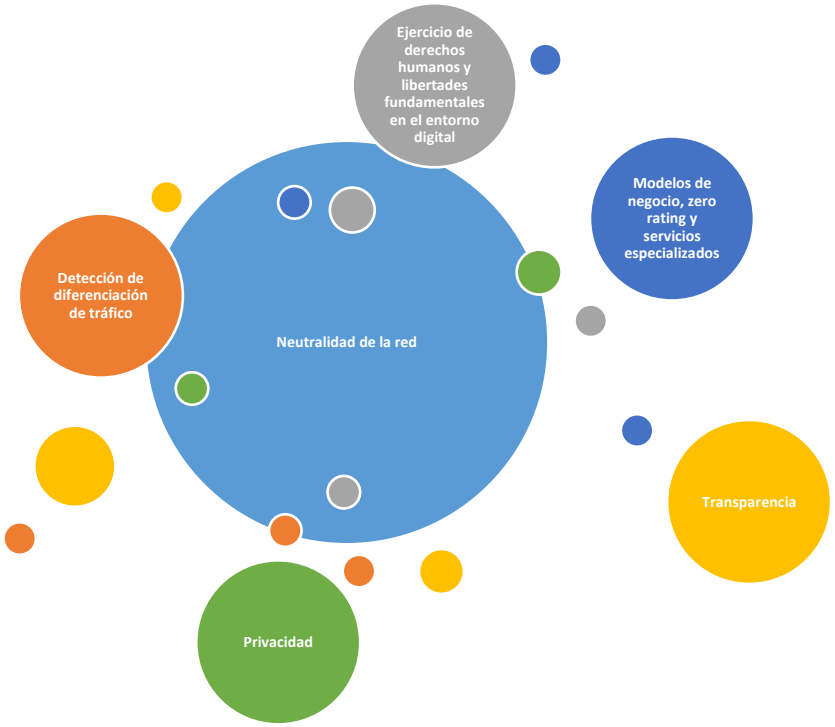
III5 Los lineamientos de neutralidad de la red y los mecanismos que monitoreen el cumplimiento resultan un determinante crítico para que el sistema normativo cumpla con los objetivos para los que fue diseñado

Como se señaló en las secciones anteriores, el Instituto estableció, a través de los Lineamientos NN, los términos y condiciones bajo los cuales los concesionarios y autorizados que presten el SAI pueden implementar políticas de gestión de tráfico y administración de red, así como las prácticas comerciales asociadas a ello que pueden o no ofrecer a los usuarios finales. También el Instituto destinó varias obligaciones en los referidos Lineamientos NN encaminadas a trasparentar la aplicación de gestión de tráfico y las ofertas comerciales como *zero rating* o servicios especializados.

Sin embargo, se advierte la necesidad de la definición de los mecanismos a través de los cuales se monitoreará el cumplimiento de los Lineamientos NN por parte de los PSI, respecto de la gestión y administración del tráfico. Lo anterior, naturalmente no se considera como una tarea sencilla, pues si bien el Instituto tiene las facultades expresas para tales efectos, es necesario dar certeza jurídica a los sujetos regulados sobre dichos mecanismos.

Para ello, es preciso señalar que existen diversos mecanismos para monitorear el cumplimiento del principio de neutralidad de la red, cada uno de estos se asocia con un aspecto en el que tiene incidencia directa la no discriminación del tráfico cursado por Internet. Así, tenemos que el cumplimiento de la neutralidad de la red se puede monitorear desde, al menos, los siguientes aspectos:

Ilustración 4 Aspectos relacionados con el monitoreo de la NN[27]



No obstante, la presente investigación se centrará en los mecanismos de monitoreo asociados exclusivamente con: **i) detección de diferenciación de tráfico** y **ii) calidad del servicio de acceso a Internet.** Lo anterior, en virtud de que, a consideración de esta investigadora, los mencionados son elementos críticos para asegurar los objetivos regulatorios que dieron origen a la regulación en materia de neutralidad de red. Además de que, se considera que algunos de los otros aspectos se cubren de forma parcial o total a través de obligaciones específicas establecidas ya en los Lineamientos NN.

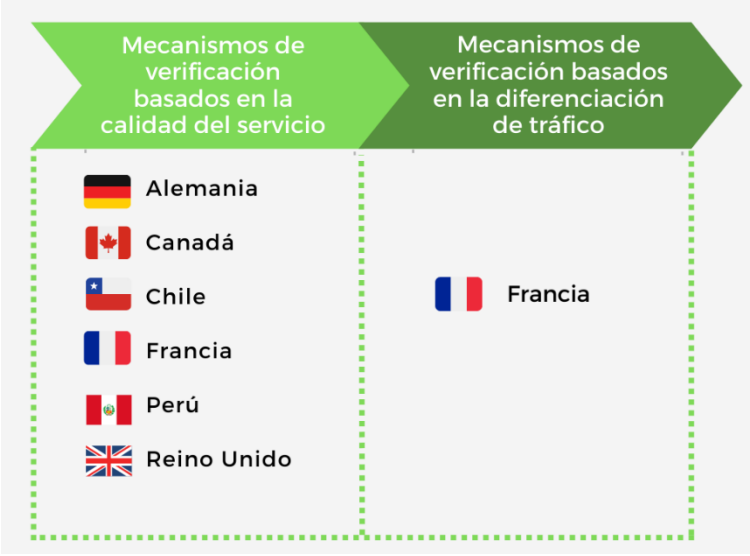
[27] Elaboración Propia

IV. Mecanismos para el cumplimiento del principio de neutralidad de la red

IV6 Propuesta de clasificación de los mecanismos existentes para verificar el cumplimiento del principio de neutralidad de la red

Como se mencionó en la introducción, cuando se habla de neutralidad de la red intervienen varios actores. Al respecto, existen diversas perspectivas desde las que se puede monitorear el cumplimiento de la neutralidad de la red. En este sentido, considerando el aspecto puramente técnico de dicho principio, esto es, la gestión de tráfico y, en su caso, bloqueo de puertos de comunicación, se identifican dos tipos de mecanismos, los cuales se describen en la Ilustración 5. La primera clasificación se basa en el monitoreo de la calidad del servicio de acceso a Internet (QoS) y, la segunda, en la detección de la aplicación de diferenciación de tráfico (DDT), estas categorías se caracterizan por tener acercamiento *ex post*. Adicionalmente, en la tabla de referencia se encuentran listados los países que se identifican en cada categoría.

Ilustración 5 Clasificación por tipo de mecanismo de verificación de la neutralidad de la red[28]



[28] Elaboración Propia

De ahí que, en las siguientes secciones, se presenta el análisis de los mecanismos para monitoreo del cumplimiento del principio de neutralidad de la red, de acuerdo con la clasificación planteada.

IV7 Calidad del Servicio de Acceso a Internet QoS

QoS

De acuerdo con la UIT la calidad del servicio (QoS, *quality of service*) es el efecto global de la calidad del funcionamiento de un servicio, que determina el grado de satisfacción de los usuarios. (UIT, 2008). Asimismo, (Xiao, et al., 2003) señalan que la calidad de servicio (QoS) se refiere a la capacidad de una red para proporcionar un mejor servicio al tráfico de red seleccionado a través de un tipo de redes o una red heterogénea.

Naturalmente, con la transición de las redes y servicios de telecomunicaciones de Red Telefónica Pública Conmutada a redes IP y servicios basados en IP, las métricas de QoS más importantes para la prestación de servicios de telecomunicaciones tradicionales (voz, TV y líneas arrendadas) junto con los servicios tradicionales de Internet (web, correo electrónico, FTP y todos los demás servicios OTT) son los parámetros de QoS de extremo a extremo en redes basadas en IP. La Recomendación Y.1540 del UIT-T define los indicadores clave de desempeño de red que pueden emplearse para especificar y evaluar el rendimiento de la red IP, a saber (UITa, 2017):

- Ancho de banda (bandwidth): el número máximo de bits que puede transportar una ruta de transmisión;
- Retardo de propagación (propagation delay): el tiempo que requiere un paquete, en función de la longitud combinada de todas las rutas de transmisión y la velocidad de la luz a través de la ruta de transmisión;
- Retraso en cola (queuing delay): el tiempo que un paquete espera antes de ser transmitido. Tanto el *delay* promedio como la variación del *delay* (*jitter*) son importantes, ya que los dos juntos establecen un intervalo de confianza para el tiempo dentro del cual se puede esperar que un paquete llegue a su destino, y
- Pérdida de paquetes: es la probabilidad de que un paquete nunca llegue a su destino. Esto podría deberse a errores de transmisión, pero los errores son bastante raros en las redes fijas modernas basadas en fibra. Más a menudo, los paquetes se pierden porque el número de paquetes que esperan la transmisión es mayor que la capacidad de almacenamiento disponible (búferes).

Dichos indicadores corresponden estrechamente a los parámetros definidos por la ETSI y son los recomendamos por (BEREC, 2014) para las mediciones de la QoS en el marco de la neutralidad de la red.

Particularmente, existen tres nociones diferentes de estimaciones de ancho de banda (identificado como uno de los parámetros para medir QoS del SAI) de una conexión en una red de datos[6]: la capacidad, el ancho de banda disponible y el *throughput*.

- Capacidad: es el ancho de banda máximo posible que una conexión puede entregar, medido entre la capa física y de enlace de datos. También se conoce como la tasa de bits neta. Por ejemplo, la capacidad de Fast Ethernet es de 100 Mbps, de 802,11 g 54 Mbps (máximo) y ADSL2+ 24576/1024 (downlink/uplink) Kbps (Koukoutsidis, 2015).
- Ancho de banda disponible: es la capacidad no utilizada de la conexión durante un cierto período de tiempo. Cambia con el tiempo y depende de la carga del conjunto de enlaces que abarca la conexión (Koukoutsidis, 2015).
- Rendimiento (throughput): generalmente se define como el rendimiento máximo alcanzable, es decir, el rendimiento que se espera que se logre utilizando protocolos de transporte estándar al intentar saturar la ruta de acceso. (Koukoutsidis, 2015)

Ahora bien, en el contexto de la neutralidad de la red, el objetivo principal de la evaluación de la QoS es identificar la degradación del servicio como resultado de la congestión o de las prácticas de los operadores (por ejemplo, la prioridad otorgada a los flujos de tráfico seleccionados sobre otros).

Así, las mediciones de QoS son una parte central del debate de la neutralidad de la red, toda vez que la detección de una violación a la neutralidad se basa en la medición de los parámetros asociados con la calidad del servicio de acceso a Internet (Koukoutsidis, 2015). De hecho, se han desarrollado varias herramientas especializadas para realizar automáticamente esta detección y también se han puesto a disposición del público (por ejemplo, Glasnost, Shaperprobe, NANO). En general, la medición de diversos parámetros de rendimiento/ *throughput* de una red puede indicar la presencia de técnicas de gestión de tráfico y estas pueden ser positivas si mejoran la calidad del SAI, o negativas si, por el contrario, degradan la calidad de dicho servicio.

Esto quiere decir que, mediante pruebas de velocidades de subida y bajada se pueden detectar variaciones y, ello llevaría a la identificación de la existencia de gestión de tráfico, en virtud de que el tratamiento diferenciado de datos puede ocasionar un menor *throughput* en la QoS.

Adicionalmente, el monitoreo de los parámetros de QoS muestra si el PSI estaría incumpliendo con la calidad contratada por el usuario final, ya que, al momento de contratar el servicio de acceso a Internet, el PSI adquiere la obligación de entregar la QoS establecida en el contrato, y al momento de incumplir, se estaría atentando a los principios de la NN[29].

[29] Lo anterior, en el supuesto de que la aplicación de la gestión de tráfico estuviera supeditada a condiciones de calidad del SAI.

Por esta razón, las leyes y reglamentos de varios países establecen que se produce una violación de la NN cuando la calidad del servicio prestada por un PSI es inferior a la contratada por el usuario. De este modo, los PSI deben entregar exactamente la QoS especificada en el contrato. (Thiago Garrett, 2018)

Existen varias soluciones para monitorear la QoS entregada dados los correspondientes Acuerdos de Nivel de Servicio (SLA). Algunas de estas soluciones, son HAKOMetar y Adkintun, las cuales se describen a continuación, y fueron desarrolladas debido al interés de los gobiernos por garantizar el cumplimiento de las redes con la normativa relacionada con la NN.

HAKOMetar

En una herramienta que permite a un usuario final comprobar la QoS suministrada por su PSI. La herramienta fue desarrollada por HAKOM, la agencia reguladora de las telecomunicaciones en Croacia. El objetivo de la agencia era emplear HAKOMetar para aumentar la transparencia y la competencia en el mercado de la banda ancha. La herramienta se creó a partir de resultados anteriores sobre las prácticas de gestión del tráfico, obtenidos en experimentos realizados en Croacia. (Thiago Garrett, 2018)

La herramienta se basa en mediciones activas del ancho de banda, entre un host final y los hosts de medición, para inferir si el usuario final está recibiendo el mismo ancho de banda anunciado por el PSI. Los resultados del estudio "*HAKOMetar be used to increase transparency in the context of nertwork neutrality*[30]" confirman que HAKOMetar aumentó de forma efectiva la transparencia en el mercado croata de la banda ancha, ya que los consumidores pudieron comprobar si sus PSI estaban entregando realmente el ancho de banda contratado. (M. Weber, 2013)

Adkintun

Es una solución para supervisar la calidad de servicio ofrecida por los PSI en Chile. La solución fue desarrollada por NIC Chile *Research Labs* a petición de SUBTEL, el organismo regulador de las telecomunicaciones en ese país, con el fin de supervisar el cumplimiento de la Ley chilena de NN por parte de los PSI. Adkintun puede instalarse en los dispositivos de los usuarios finales o incrustarse en los routers residenciales proporcionados a los consumidores seleccionados. (Thiago Garrett, 2018)

La herramienta realiza periódicamente mediciones activas entre los hosts finales y varios hosts de medición distribuidos por todo el país. Se emplean varias métricas, como el rendimiento/*throughput,* el *delay* y el *loss rate*. Todos los resultados obtenidos por Adkintun están disponibles públicamente a través de un sitio web. En el estudio "*Monitoring Network Neutrality: A survay on Traffic*

[30] Traducción al español: HAKOMetar se utilizará para aumentar la transparencia en el contexto de la neutralidad de la red.

Differentiation Detection"[31] se afirma que Adkintun está ayudando a los consumidores a proteger sus derechos; la herramienta ha servido de base para reclamaciones e incluso para procesos judiciales que implican a los PSI y a la SUBTEL. También se ha desarrollado una herramienta similar, Adkintun Mobile, para monitorear la QoS de las redes móviles en Chile. Esta herramienta emplea una combinación de mediciones pasivas y activas obtenidas de dispositivos móviles." (Thiago Garrett, 2018)

En la siguiente tabla, se muestra un resumen de los países en los que los reguladores en la materia han implementado herramientas de monitoreo de la QoS o han establecido criterios técnicos para dichas herramientas.

Tabla Herramientas de QoS del SAI[32]

País	Link (URL)	Características
Alemania	https://www.breitbandmessung.de/test	Latencia, velocidad de subida y bajada. Contiene mapas con el promedio de velocidad de bajada
Austria	Test | RTR-NetTest (netztest.at)	Ping, velocidad de subida, velocidad de bajada, 3 conexiones paralelas, 7 segundos de duración del test
Croacia	HAKOMeter	Conexiones HTTP y/o FTP, gran número de conexiones paralelas para obtener la velocidad, duración de la prueba 5 segundos
Francia	Code de conduite 2020 de la qualité de service Arcep (5gmark.com)	No tiene un sitio oficial, pero señala cuáles son las aplicaciones para medir QoS que son acordes al Código de Conducta.[33]

[31] Traducción al español: Supervisión de la neutralidad de la red: una investigación sobre la detección de la diferenciación de tráfico.

[32] Elaboración propia.

[33] Code de conduite 2020 de la qualité de service d'internet 14/09/2020 (arcep.fr)

País	Link (URL)	Características
	https://support.ookla.com/hc/en-us/articles/4413722458509-Measurement-Methodologies– Ookla	
Grecia	https://hyperiontest.gr/?action=yperion	Usa NDT M-Lab
México	http://www.ift.org.mx/conocetuvelocidad	Latencia, *Jitter*, velocidad de carga y de descarga, proveedor y dirección IP. Basado en Ookla
Chile	https://www.speedtest.net/	Capa 4 (Modelo OSI) Protocolo TCP con HTTP, 4 o 2 sesiones paralelas dependiendo de la velocidad y del explorador, 22 bytes, 15 segundos descarga, 15 subida.
Paraguay	Sin software, medición por medio de Sondas de medición	QoS, *throughput* promedio, *throughput* real, tiempo de ida y vuelta promedio, fluctuaciones mínimas, promedio y máxima y perdida de paquetes.
Perú	https://checatuinternetmovil.osiptel.gob.pe/	Subida, bajada, cobertura, Latencia, perdida de paquetes (WeplanAnalytics)
Brasil	https://beta.simet.nic.br/	Protocolo UDP con HTTP, Mediciones contra servidores de infraestructura propia, latencia, *jitter*, perdida de paquetes.
Ecuador	https://cntep.speedtestcustom.com/	Speedtest by Ookla

País	Link (URL)	Características
Reino Unido	https://www.broadbandchoices.co.uk/tools/speed-test/test	Ping, velocidad de subida, velocidad de descarga y *packet loss*
EUA	https://play.google.com/store/apps/details?id=com.samknows.fcc&hl=es_MX&gl=US	Velocidad de bajada, velocidad de carga, latencia, *packet* loss y *jitter*
Canadá	Sin software, mediante sonda de medición llamada "Whitebox"	TCP con HTTP5, tres conexiones paralelas, Velocidad de carga y descarga, latencia, packet loss y tiempo de acceso

A fin de ejemplificar la implementación de los mecanismos de monitoreo del cumplimiento de la neutralidad de la red basados en QoS, se presenta a continuación una descripción de la experiencia internacional enfocada en tal sentido.

Alemania

Alemania al igual que el resto de la UE, se encuentra sujeta a la Directiva EU2015/2120 del Parlamento Europeo[34], así como a los Lineamientos para la Implementación de las Reglas Europeas[35], ambos instrumentos en materia de neutralidad de la red. Al respecto, en dicha normativa se plantean las obligaciones de los reguladores de verificar, a través del monitoreo de la red y la publicación de reportes, el cumplimiento del principio de neutralidad de la red.

[34] Regulation (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015. Layiung down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users´ rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=en

[35] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. Disponible en:
https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules

En consecuencia, la Agencia Federal de Redes de Alemania (Bunedesnetzagentur) ha publicado diversos informes anuales[36] respecto de la aplicación de las disposiciones sobre neutralidad de la red en Alemania. Particularmente, el informe Anual 2020/2021[37] se centra en las siguientes cuestiones:

- Debate sobre la introducción de tarifas de *zero rating*;
- Bloqueo de DNS;
- La investigación de las medidas de transparencia, incluidas aquellas relacionadas con la tramitación de quejas de los usuarios relativas a las bajas tasas de transmisión de datos; y
- El funcionamiento de un mecanismo de control de la calidad.

Ahora bien, del análisis de los informes mencionados, se advierte que los mecanismos de verificación de la Neutralidad de la Red por parte de la Bunedesnetzagentur consisten en un portal web, aplicación de escritorio y aplicación móvil en ambos casos para medir, principalmente, la velocidad del servicio de acceso a Internet y por último la publicación de informes anuales (Agencia Federal de Redes, 2021).

El portal web denominado *Breitbandmessung* brinda a los usuarios la posibilidad de realizar mediciones de velocidad para probar el *throughput* de navegación de Internet. Adicionalmente, la aplicación de escritorio Breitbandmessung Desktop-App y la aplicación móvil Breitbandmessung son capaces de medir la velocidad de banda ancha, con el objetivo de comprobar las velocidades acordadas en el contrato con el PSI y dar a los usuarios la posibilidad de reducir o terminar el contrato previamente establecido (Agencia Federal de Redes, 2021).

El medidor de velocidad de banda ancha es también usado por la autoridad regulatoria para colectar muestras a través de una infraestructura "*crowdsourcing*". Dicha información se pública de forma anual. Además, los usuarios pueden visualizar en un mapa las tasas de transmisión medidas en regiones específicas. Los mapas se actualizan diariamente. (Bundesnetzagentur, 2021)

[36] Desde 2016 a la fecha, ha publicado 5 informes. Todos disponibles en: https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/NetNeutrality/start.html

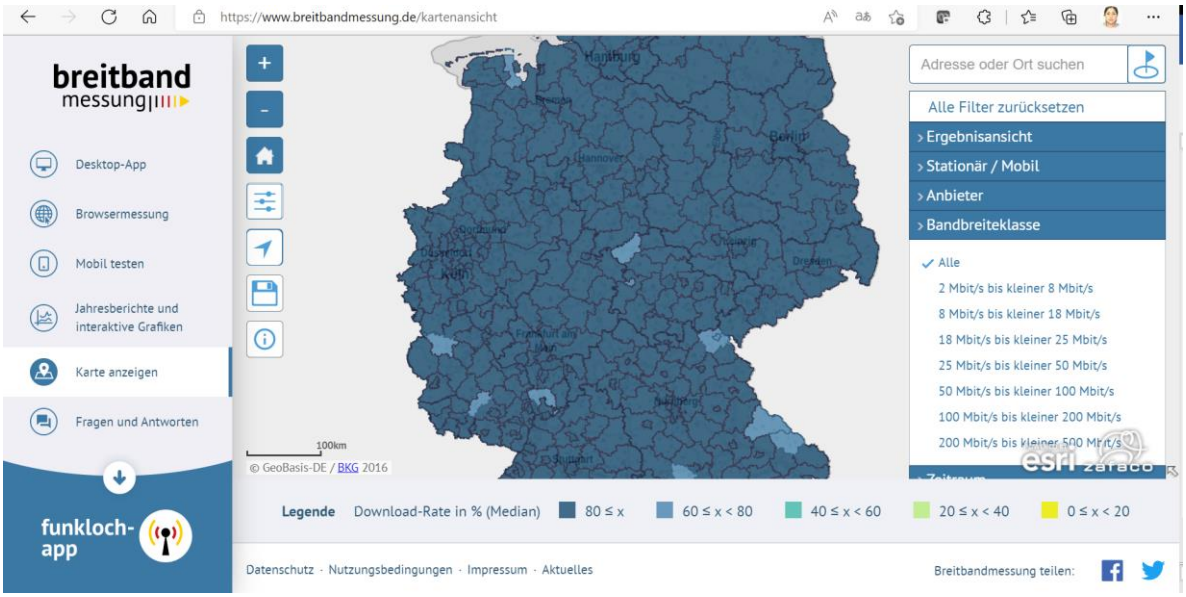
[37] Net Neutrality in Germany. Annual Report 2020-2021. Disponible en: https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/MarketRegulation/NetNeutrality/NetNeutralityInGermanyAnnualReport2020_2021.pdf?__blob=publicationFile&v=3

Ilustración 6 Medidor de velocidad de la Agencia Federal de Redes[38,39]

[38] Prueba realizada el 9 de junio de 2022, operador Totalplay. Disponible en: https://www.breitbandmessung.de/test

[39] Las imágenes y el contenido de las imágenes se tradujeron al español. La versión original se encuentra en el Anexo 1d

Ilustración 7 Ejemplo de un mapa que despliegue los resultados de las mediciones del medidor de velocidad[40]



En este contexto, en el caso de que un usuario considere que su servicio es deficiente, esto es, que la velocidad medida sea significativamente discrepante[41] de la velocidad contratada, existe un procedimiento, a través del cual este debe realizar las pruebas del *throughput* del SAI, con la intención de que dichas pruebas adquieran el rigor necesario para sustentar la queja del usuario. Las mediciones se deben realizar en tres días distintos y deben sumar treinta mediciones en total, con el objetivo de dar mayor certeza al proceso. La aplicación tiene instrucciones precisas y además guarda el resultado haciendo más fácil el proceso para los usuarios. Los resultados obtenidos de la aplicación móvil, no son parte de los informes anuales (Agencia Federal de Redes, 2021).

El objetivo primordial es poder extraer la información para generar estadísticas vinculadas a la velocidad de Internet, por periodo de tiempo y ubicación geográfica. Adicionalmente, esta información es agregada al informe anual de la Agencia Nacional de Redes de Alemania como resultado de la regulación impuesta por BEREC en 2015.

[40] Consultado el 6 de junio de 2022. Disponible en: https://www.breitbandmessung.de/kartenansicht

[41] Desde el punto de vista del regulador alemán, una discrepancia significativa ocurre para la velocidad de bajada del servicio fijo de banda ancha cuando: **a)** el 90% de la velocidad máxima acordada contractualmente no se alcanza al menos una vez, en al menos dos días de medición; **b)** la velocidad normalmente disponible no se alcanza en el 90% de las mediciones, o **c)** la velocidad cae por debajo del mínimo acordado contractualmente en al menos en dos días de medición.

Canadá

La CRTC reconoce que algunos de los PSI en Canadá han implementado prácticas técnicas y/o económicas relacionadas con la gestión del tráfico en Internet. Al respecto, la CRTC ha establecido un marco para evaluar si las prácticas de gestión de tráfico existentes y futuras aplicadas a los servicios minoristas y mayoristas de Internet cumplen con la Ley de Telecomunicaciones Canadiense (Anon., 2021).

Particularmente, la CRTC ha establecido un sitio web titulado "*Complaints about Internet Traffic Management Practices*" en el que se señala que, en caso, de que un usuario quiera ingresar una queja a la CRTC sobre una práctica de gestión de tráfico, este debe contactar a su PSI para "ver" si este puede resolver el problema.

En el caso de que el PSI no haya solucionado la queja del usuario y el usuario considere que su PSI no cumple con las políticas de la CRTC, este puede presentar una queja ante la autoridad reguladora, para ello, la CRTC requiere a dicho usuario que conozca sus derechos y la información que debe incluir en la queja de "prácticas de gestión de tráfico".

La autoridad canadiense publica todos los hallazgos de incumplimiento en su sitio web, con el nombre del PSI y la naturaleza de la queja. Adicionalmente, de forma trimestral, la CRTC publica en su sitio web un resumen del número y tipo de denuncias que haya recibido, incluyendo el número de denuncias activas y resueltas.

Ilustración 8 Estatus del reporte sobre las quejas relacionadas con las prácticas de gestión de tráfico en Canadá[42,43]

No obstante que la CRTC vigila la aplicación de prácticas de gestión de tráfico del servicio de acceso a Internet mayorista y minorista. La CRTC no está directamente involucrada en las prácticas de facturación, problemas de calidad y relaciones con los usuarios finales del SAI. En estos casos, el usuario final debe ponerse en comunicación con la Comisión de Quejas de Servicios de Telecom-Televisión (CCTS, por sus siglas en inglés), dicho organismo es una agencia independiente encargada de ayudar a resolver quejas de consumidores (usuarios finales) y pequeñas empresas. En este contexto, se menciona que un usuario final puede generar una queja directamente a la CCTS a través de un link u otros métodos, que incluyen correo electrónico, teléfono fijo, fax, entre otros.

La CCTS ha establecido un sistema de quejas a través de su portal web (ilustración 9), un número de teléfono y un correo electrónico donde el usuario puede levantar una queja o reclamo. El sistema de quejas se basa de seis pasos que se describen a continuación (CCTS, 2022):

1. Reclamación Aceptada: si la queja cae dentro de lo mandatado en los de servicios de telecomunicaciones y televisión, se envía una copia al proveedor de servicios. El PSI deberá resolver el problema con el cliente e informar a la CSTC dentro de los 30 días. Si la queja es sobre un servicio de telecomunicaciones (y no de televisión) y el proveedor del servicio no participa en el CCTS, se toman las medidas necesarias para que el proveedor se una al CCTS.

[42] La página fue traducida al español, la versión original se encuentra en el Anexo 1d

[43] (CRTC, Enero-Marzo 2022)

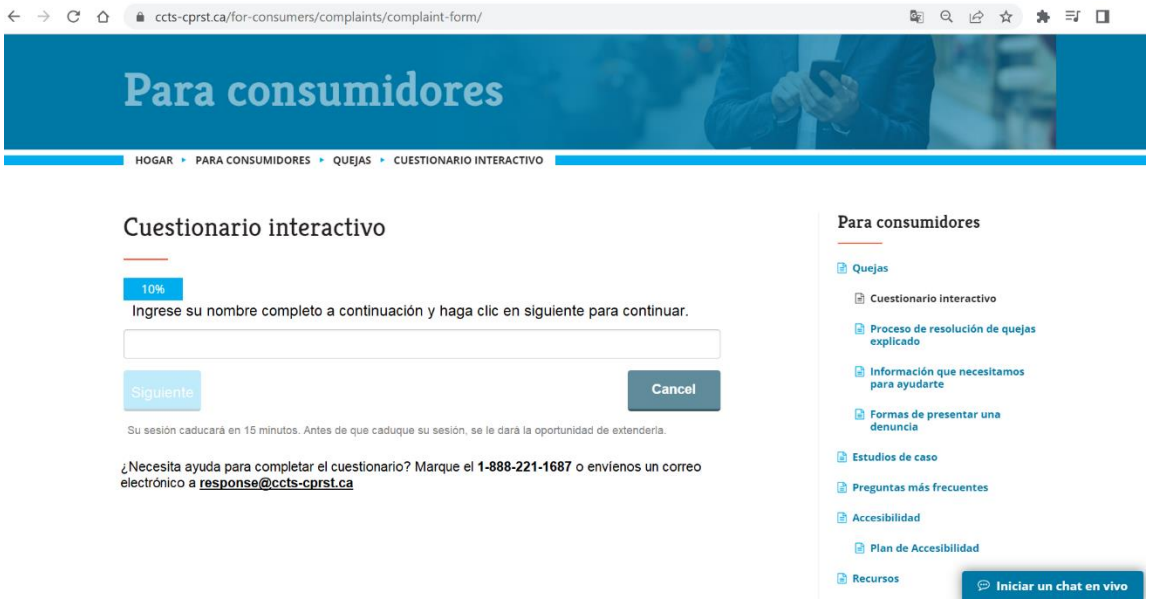
2. Resolución informal: cuando una queja sigue sin resolverse, se evalúa la complejidad, la cantidad de información adicional que se puede requerir y la probabilidad de resolver el asunto. Muchas de estas quejas se resuelven a satisfacción de ambas partes en esta etapa.

3. Investigación: las quejas no resueltas son investigadas, durante este proceso, se solicita más información o documentación adicional de una o ambas partes. Una queja puede rechazarse o desestimarse en cualquier etapa del proceso de investigación si se determina que el proveedor actuó razonablemente en el cumplimiento de sus obligaciones en virtud del contrato o ha tomado medidas razonables para resolver la queja, incluso si el cliente no está de acuerdo.

4. Recomendación: cuando se completa la investigación, se procede a hacer una recomendación por escrito para la resolución de la queja basada en el análisis de la CCTS. La recomendación puede consistir en indicar que el proveedor de servicios tome alguna medida o se abstenga de tomar alguna medida. Los ejemplos incluyen la corrección de un error de facturación, la conexión o desconexión del servicio, la exención de cargos y la suspensión de la actividad de cobro. En algunos casos, incluso una disculpa o una explicación. También se puede recomendar que el proveedor de servicios realice un pago al cliente como compensación por cualquier pérdida, el proveedor tiene 20 días para determinar si la acepta o la rechaza.

5. Decisión: si el cliente o el proveedor de servicios (o ambos) rechazan la recomendación, se les solicita explicar el por qué, por escrito, para reconsiderar la recomendación. En la decisión, el CCTS puede mantener la recomendación o modificarla si las razones proporcionadas muestran que existen dudas sustanciales sobre la corrección de la Recomendación original.

Ilustración 9 Cuestionario Interactivo de la CCTS[44,45]



Ahora bien, de acuerdo con la información del portal de la CRTC existen dos excepciones notables en las que dicha autoridad reguladora daría seguimiento puntual a las quejas de los usuarios finales, a saber:

- Tarifas minoristas de Internet de Northwestel, brinda servicios de Internet a una pequeña población que se encuentra dispersa en un gran territorio y en el 2013, la CRTC encontró que había competencia limitada para ciertos servicios de Internet residenciales y comerciales ofrecidos por dicha empresa. En consecuencia, la CRTC decidió que regularía de manera excepcional las tarifas de Northwestel en dichos servicios.
- Prácticas de gestión del tráfico de Internet. La CRTC supervisa cómo los proveedores de servicios de Internet utilizan las políticas de gestión de tráfico. Las prácticas técnicas incluyen medidas para ralentizar el tráfico de un usuario, priorizar el tráfico o detectar usuarios pesados para limitar su ancho de banda, por su parte, las prácticas económicas implican cobrar más por los usuarios cuyo uso de Internet excede un límite predefinido. De acuerdo con la CRTC, las prácticas antes mencionas son legítimas, siempre que el PSI sea transparente sobre su uso de la gestión de tráfico y sus clientes sean conscientes de cómo se administrará su tráfico.

  Al respecto, la CRTC señala que las prácticas prohibidas de gestión de tráfico se asocian con: bloquear la entrega de contenido y/o degradar notablemente el tráfico de Internet sensible al tiempo, en la medida en que equivale a bloquear el contenido.

[44] (CCTS, 2022)

[45] La página fue traducida al español, la imagen original se encuentra en el Anexo 1d

Chile

La regulación de Neutralidad de la Red en Chile está mandatada bajo un enfoque de calidad del servicio donde establece tres mecanismos de verificación: mecanismo de verificación individual, un Organismo Técnico Independiente (OTI) y la posibilidad de levantar quejas o reclamos.

La SUBTEL obliga a los PSI a poner a disposición de los usuarios una aplicación capaz de realizar mediciones individuales de velocidad; la cual mide la velocidad, *delay*, *jitter*, pérdida de paquetes, disponibilidad de acceso a sitios web y velocidades instantáneas.

Como parte de las medidas establecidas para la verificación del cumplimiento de la Ley 20.453 de 2010 y el Reglamento de Aplicación de la Ley de Neutralidad de la Red de 2011, se establece la creación de un Organismo Técnico Independiente que está encargado de ejecutar las mediciones de calidad, además de operar y gestionar la aplicación de los PSI para mediciones individuales. El resultado de las mediciones efectuadas por el OTI es utilizado por el regulador para la elaboración y publicación de informes y estudios (Ley. 21.046, 2017).

Por último y con el objetivo de empoderar al usuario, los PSI están obligados a recibir reclamos por teléfono a través de la numeración especial y a través de su sitio web, bajo las siguientes condiciones:

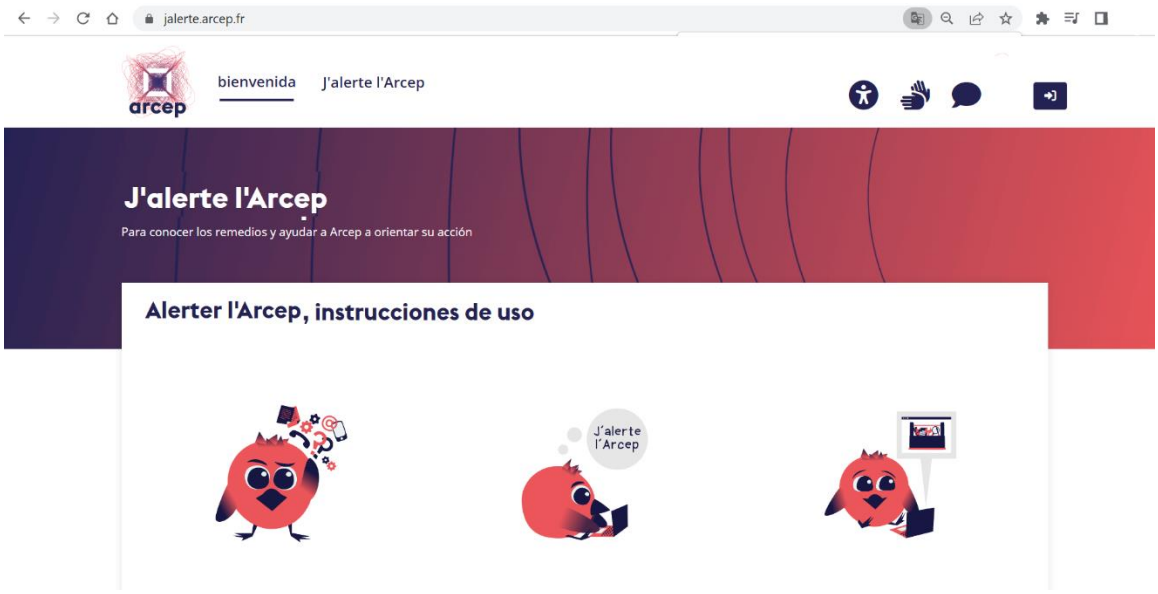
- Los medios de reclamos deberán funcionar las 24 horas y los 7 días de la semana.
- Los PSI deberán reportar mensualmente a la SUBTEL indicadores de atención telefónica.
- Las compensaciones se deberán descontar de la tarifa mensual del plan para servicios de prepago por aquellos días en que no se contó con el servicio y extender la vigencia del servicio de acceso a Internet por los días en los que no se cumplió con el servicio.

Francia

Resultado del Reglamento Europeo n° 2015/2120 que garantiza un Internet abierto para todos los usuarios, la ARCEP puso a disposición de los usuarios la página *J'alerte l'Arcep* como mecanismo de protección.

Lanzada en octubre de 2017, la plataforma *J'alerte l'Arcep* está a disposición de todo ciudadano francés, empresa o de toda comunidad francesa que desee resolver cualquier problema relacionado con internet fijo y móvil, en la Ilustración 10 se puede visualizar la página de inicio de *J'alerte l'Arcep* (ARCEP, 2018). Esta aplicación da a los usuarios la oportunidad de establecer una alerta por violaciones a la reglamentación de Neutralidad de la Red.

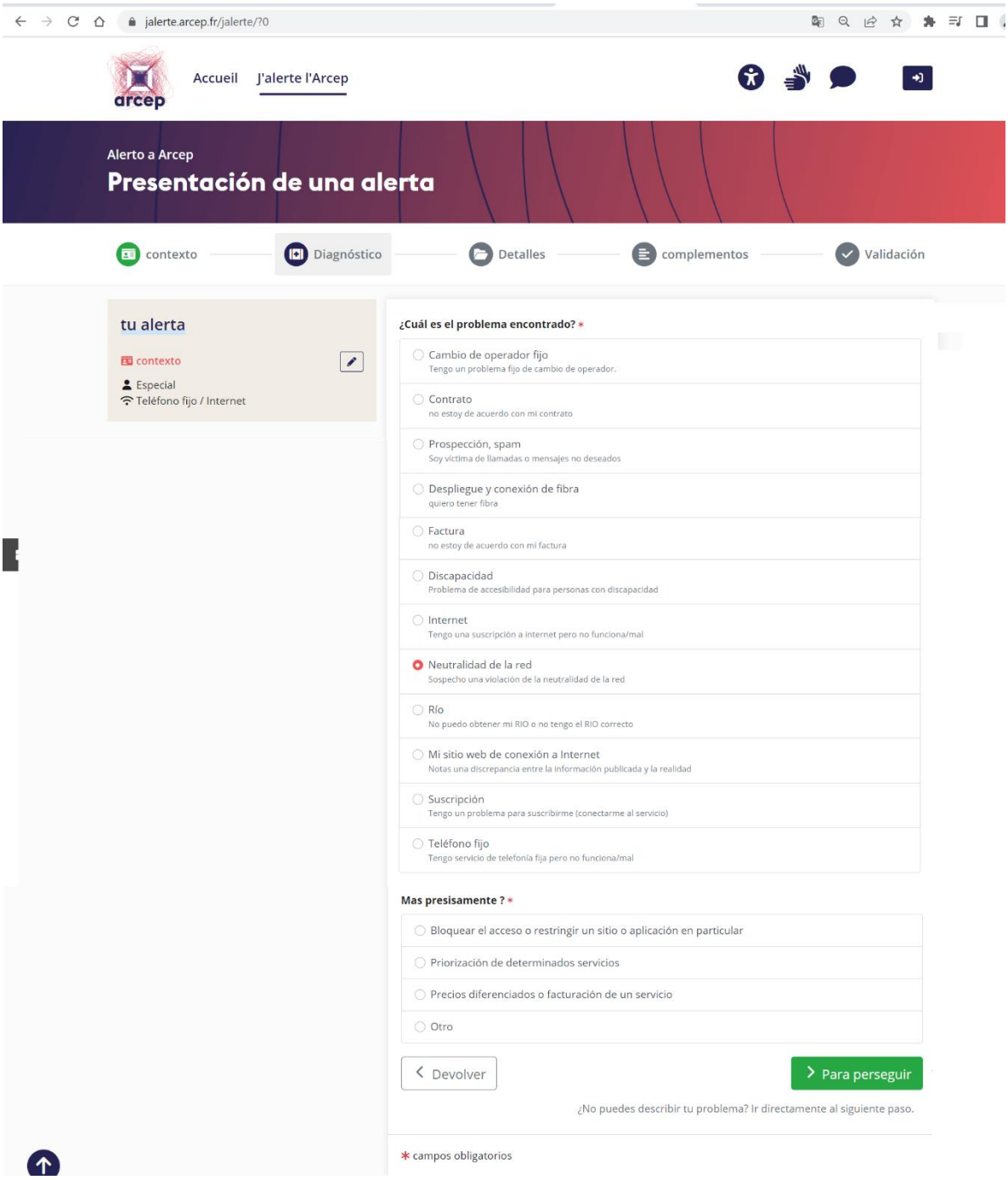
Ilustración 10 Página de quejas y reclamos ante violaciones a los derechos de los usuarios y regulación J'alert a l'Arcep [46]



J'alerte a l'Arcep tiene como objetivo empoderar, apoyar la elección de los usuarios y ser una herramienta que genere mayor competencia en el mercado. Esta plataforma permite a los usuarios influir en la regulación del mercado a través de su experiencia y participar en él, para alentar a los operadores a mejorar sus servicios y desarrollar sus redes, por otro lado, para facilitar el uso de la aplicación los usuarios son orientados de manera particular según su situación (ARCEP, 2021).

[46] (ARCEP, 2017)

Ilustración 11 Razones por las que un usuario puede emitir una alerta J'alerte l'Arcep[47,48]



[47] (ARCEP, 2018)

[48] La página original fue traducida al español, la versión en el idioma original se encuentra en el Anexo 1d

La aplicación permite a la ARCEP monitorear en tiempo real los principales problemas que enfrentan los usuarios para identificar fallas recurrentes o picos en las alertas. El objetivo, señala ARCFEP, es mejorar la aplicación de la normativa y regulación, puesto que las redes se desarrollan y evolucionan antes que la regulación (ARCEP, 2021).

El proceso de levantamiento de la alerta consta de cinco pasos descritos a continuación (ARCEP, 2017):

> Contexto: en este apartado el usuario señala si es un particular, empresa, operador, asociación o desarrollador, además se elige si la alerta es en un servicio móvil, Internet fijo, servicio postal o de prensa.
>
> Diagnóstico: el usuario elige la razón por la que levanta la alerta incluida una sospecha a la violación de la regulación de neutralidad de la red; posteriormente el usuario deberá elegir si considera que se trata de un bloqueo al acceso, restricción de un sitio, aplicación en particular, priorización de determinados servicios, precios diferenciados, facturación de un servicio o algún otro no considerado en las opciones.
>
> Detalles: el usuario selecciona el operador y tecnología con la que tiene problemas.
>
> Complemento: se amplía la información proporcionando mayores detalles y si el usuario tiene pruebas puede anexar algún documento.
>
> Validación: en este apartado se solicitan datos personales y se procede a validar la queja, además se envía un resumen al correo electrónico registrado.

La ARCEP publica un informe sobre las estadísticas generadas con la información recabada a través de la página de J'alerte *a l'Arcep* y, finalmente, el informe contiene lecciones y acciones tomadas por el regulador.

Según el informe del Estado de Internet en Francia en 2020 se presentaron más de 33 000 quejas a la ARCEP, el 40% se referían a un problema relacionado con la calidad y disponibilidad de los servicios fijo y móvil (ARCEP, 2021).

Adicionalmente, la ARCEP pone a disposición de los usuarios del SAI la aplicación WeHe a través de la cual se pueden realizar pruebas para detectar la existencia de técnicas de gestión de tráfico a los datos generados por ciertos contenidos, aplicaciones y/o servicios disponibles en Internet.

Reino Unido

El Reino Unido abandonó la Unión Europea el 31 de enero de 2020, con un período de transición hasta el 31 de diciembre de 2020. Tras el final de este período, las normas de la Unión Europea sobre neutralidad de la red se convirtieron en parte de la legislación nacional del Reino Unido (OFCOM, 2021).

Para dar cumplimiento a la regulación de neutralidad de la red, OFCOM a través del informe *Ofcom's approach to assessing compliance with net neutrality rules* expresa el enfoque para evaluar el cumplimiento de la regulación, la supervisión se concentra en analizar la correcta aplicación de la regulación en las ofertas comerciales de ***zero rating*** y gestión de tráfico.

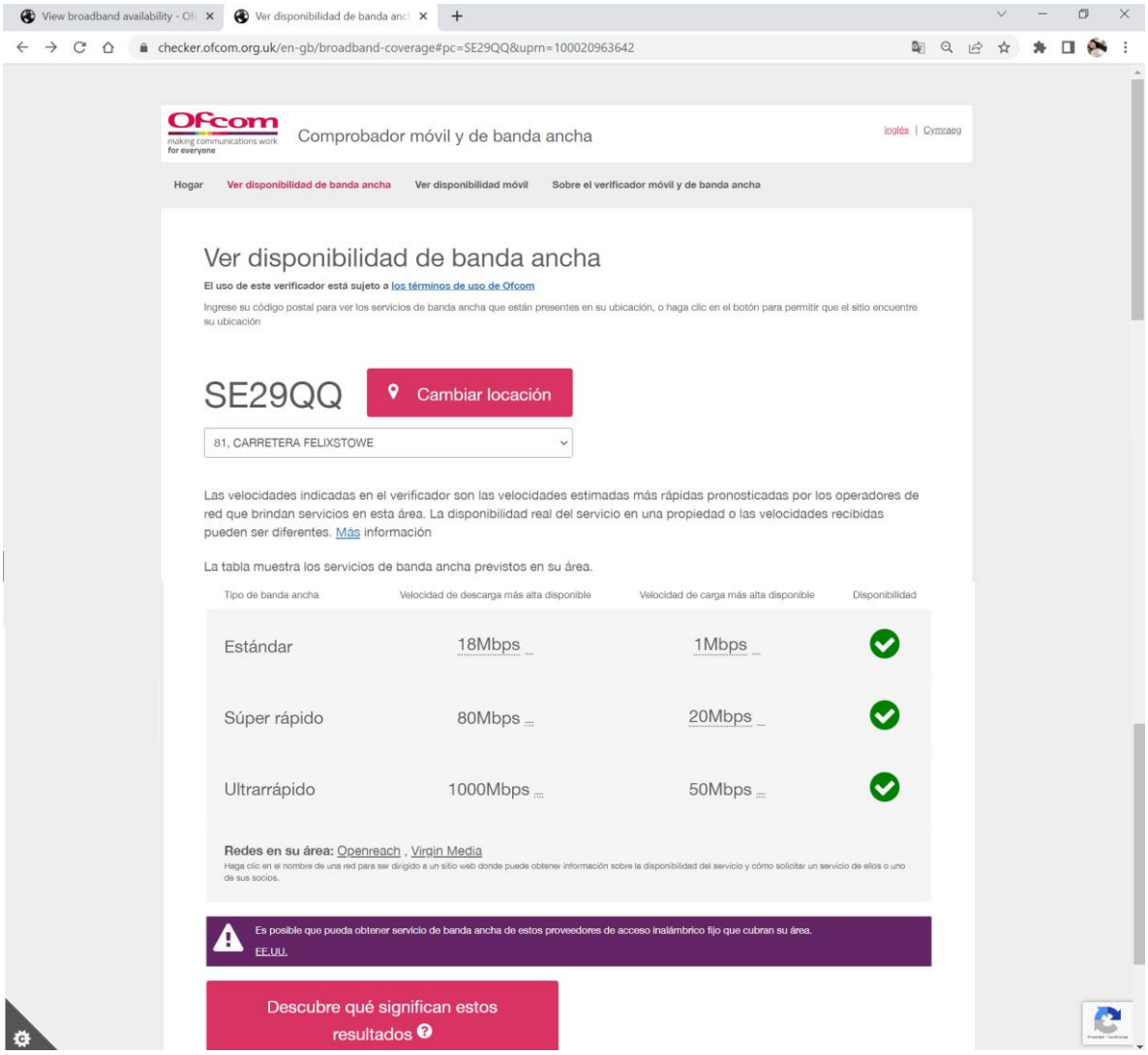
Para analizar las prácticas de gestión de tráfico OFCOM analiza que, en el marco de la regulación, la gestión sea razonable. Sin embargo, en el caso de aplicación de "gestión de tráfico no razonable", OFCOM verifica que esta haya sido aplicada con la intención de: a) de cumplir con la legislación de la Unión Europea o Reino Unido, b) preservar la integridad de la red, servicios o equipos terminales de los usuarios finales y/o c) prevenir la congestión de la red (OFCOM, 2019).

OFCOM monitorea la cobertura móvil en el Reino Unido y, como parte de esto, produce mapas mensuales de cobertura basados en predicciones de cobertura de PSI móvil. Los mapas de cobertura móvil de Reino Unido se encuentran disponibles a través de la página Mobile and Broadband Checker[49] y están diseñados para ayudar a las personas a conocer la disponibilidad de servicios móviles y de banda ancha en un área en particular, además de ayudar a las personas a obtener la información de forma rápida y sencilla, para que puedan tomar decisiones informadas (OFCOM, 2017).

La página Mobile and Broadband Checker muestra información sobre la velocidad más alta prevista en tres rangos de velocidad: estándar (hasta 30 Mbps), súper rápido (entre 30 Mbps y 300 Mbps) y ultra rápida (superior a 300Mbps), como se puede observar en la Ilustración 12. Para realizar la búsqueda, la página requiere que el usuario introduzca su código postal y posteriormente seleccione la colonia a la que pertenece su domicilio, por otro lado, la aplicación muestra a los PSI disponibles en esa ubicación (OFCOM, 2017).

[49] https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/advice/ofcom-checker

Ilustración 12 Página sobre la cobertura móvil en Reino Unido, Velocidad Prevista más Alta[50,51]



OFCOM también recopila información de una muestra tipo panel de dispositivos móviles, con el objetivo de comprender mejor cómo las personas usan sus servicios móviles y la experiencia que reciben, esta información se pública en el informe Mobile Matters. La última edición fue el informe Mobile Matters 2021 que utilizó datos recopilados entre enero y marzo de 2021 de alrededor de 280,000 dispositivos en todo el Reino Unido (OFCOM, 2021).

[50] (OFCOM, 2017)

[51] La página fue traducida al español, la versión original se encuentra disponible en el Anexo 1d

OFCOM recaba información a través de *SDK-enabled apps* en dispositivos Android de Reino Unido y la información es administrada por umlaut communications GmbH (Umlaut), quienes además de recolectar la información apoyan en el análisis y generación de indicadores. Umlaut anonimiza la información y la recolecta siempre que el teléfono inteligente esté en uso activo.

La información que se recolecta corresponde a la distribución de la conexión a Internet por tipo de tecnología (2G, 3G, 4G, 5G, Wi-Fi), la tasa de éxito para conexiones móviles, latencia y el promedio de usuarios que usan servicios de voz y datos. La información se pública en los informes de Mobile Matters y también en mapas interactivos publicados en la página de OFCOM, los cuales contienen información sobre el acceso a Internet por tipo de tecnología y la latencia promedio, como se observa en la Ilustración 13.

Por otro lado, OFCOM en 2021 publicó el informe UK home broadband performance, measurement period March 2021 con el objetivo de conocer el estado de Internet fijo en Reino Unido y contiene información sobre los siguientes temas (OFCOM, 2021) :

- Pruebas de velocidad de Internet
- Velocidad de carga y descarga
- Pruebas de trasmisión de video (Netfllix)
- Latencia

La metodología empleada en el informe sobre banda ancha doméstica se realizó en colaboración de SamKnows Limited, socio técnico de OFCOM, quién recluta a una muestra tipo panel de usuarios de banda ancha residencial del Reino Unido, proporciona unidades de monitoreo conocidas como *whiteboxes*, además recopila y apoya en el análisis de datos (OFCOM, 2021).

Ilustración 13 Mapas Interactivos de Internet Móvil en Reino Unido[52,53]

Perú

Perú ha avanzado en la creación de herramientas que favorecen el cumplimiento del Reglamento de Neutralidad de la Red de 2016, garantizando la calidad de experiencia del usuario, a través de tres herramientas: quejas directamente con su PSI, apelación al Tribunal Administrativo de Solución de Reclamos de Usuarios (TRASU) y a través de la página "Checa tu Internet móvil".

Queja directamente con su PSI

Cuando el usuario de Internet detecta una incidencia que infrinja la regulación sobre neutralidad de red, puede presentar una queja directamente al PSI, con las siguientes consideraciones (Reglamento de la Neutralidad de la Red, 2016):

- El PSI cuenta con 3 días hábiles para absolver tu reclamo.
- Posteriormente el PSI emite la resolución de primera instancia.

Si el usuario no se encuentra conforme con la resolución, puede presentar un recurso de apelación al PSI. La empresa operadora eleva el expediente al TRASU quién es la última instancia administrativa para la solución de reclamos de usuarios de servicios públicos de telecomunicación, el TRASU emite la resolución final y este es considerado el término de la queja.

Recurso de apelación al TRASU

El TRASU se considera como última instancia administrativa para la solución de reclamos de usuarios de servicios públicos de telecomunicaciones, creado mediante Resolución N° 013-95-CD/OSIPTEL, publicada el 24 de septiembre de 1995 en el Diario Oficial "El Peruano" (OPSITEL, 2021).

Los lineamientos de quejas establecidos por TRASU permiten al usuario establecer una queja por calidad o idoneidad en la prestación del servicio, a través de problemas derivados de un inadecuado funcionamiento de la red (OPSITEL, 2020).

De acuerdo con los lineamientos de quejas establecidos por el OSIPTEL, el usuario puede establecer una queja o reclamo al TRASU bajo las siguientes condiciones (OSIPTEL, 2021):

- Por infracción de plazos respecto a la atención oportuna de reclamos y recursos
- Aplicación del silencio administrativo positivo
- Suspensión del servicio con reclamo en trámite
- Requerimiento de pago con reclamo en trámite

[52] (OFCOM, 2021)

[53] La página fue traducida al español, la versión original se encuentra disponible en el Anexo 1d

- No permitir la presentación de reclamos y recursos
- No elevar recurso de apelación
- No elevar queja
- Otros defectos de tramitación

Checa tu Internet móvil

En 2021 OPSITEL puso a disposición de los usuarios la página Checa tu Internet móvil, donde los usuarios pueden conocer y comparar directamente el desempeño de la calidad de experiencia del servicio de Internet móvil ofrecido por las principales empresas operadoras en Perú, la cual permite conocer los siguientes indicadores (OPSITEL, 2021):

- Velocidad de subida (Mbps)
- Velocidad de bajada (Mbps)
- Tiempo de cobertura (%)
- Latencia (ms)
- Pérdida de paquetes (%)

La información está disponible a nivel región, provincia y distrito, además el usuario puede elegir consultar tecnología 4G y 3G, para obtener la información OPSITEL recopila de más de 150 millones de mediciones mensuales, en más de 600 distritos a nivel nacional y 25 regiones, además la información se actualiza mensualmente y se publica en la página de Internet OPSITEL a través de un informe trimestral con los principales resultados de dichas métricas (OPSITEL, 2021).

Ilustración 14Página checa tu Internet Móvil[54]

Filtros de búsqueda:

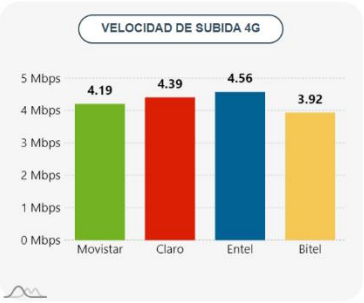
Región | Provincia | Distrito | 2022 | Mayo

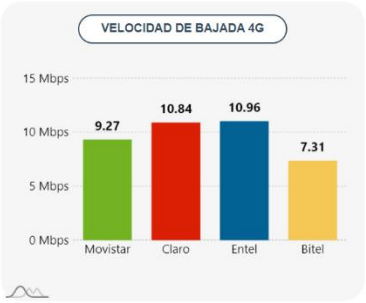
Tipo de red: 4G

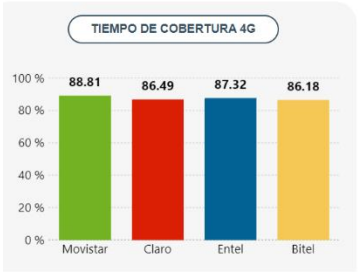
INDICADORES DE INTERNET MÓVIL

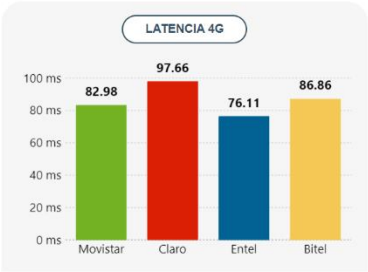
Indicador	Movistar	Claro	Entel	Bitel	Promedio ponderado
Velocidad de subida 4G (Mbps)	4.19	4.39	4.56	3.92	4.29
Velocidad de bajada 4G (Mbps)	9.27	10.84	10.96	7.31	9.94
Tiempo de cobertura 4G (%)	88.81	86.49	87.32	86.18	87.25
Latencia 4G (ms)	82.98	97.66	76.11	86.86	87.54
Pérdida de paquetes 4G (%)	1.59	1.11	0.97	2.32	1.39

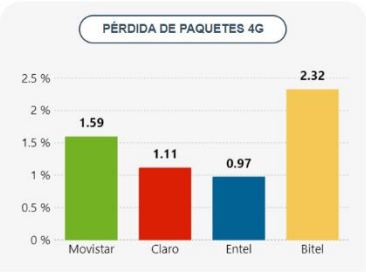
N.D.= No disponible (mediciones insuficientes). Fuente: Weplan Analytics











IV8 Diferenciación y detección de la diferenciación de tráfico

Si bien el monitoreo de la QoS es considerado como un mecanismo indirecto para verificar el cumplimiento de la neutralidad de la red, a partir de que una modificación a los parámetros asociados con dicha calidad puede indicar la aplicación de gestión de tráfico por parte de los PSI, existen otros mecanismos que de forma "directa" estarían encaminados a la detección de la diferenciación del tráfico.

Es este contexto es preciso señalar que la neutralidad de la red en cada país obedece, ciertamente a una realidad y contexto particulares, por lo que *per sé* la detección de diferenciación de tráfico puede no ser considerada como una violación a la NN, sino que depende de un análisis en el marco de las políticas de gestión de tráfico que pueden o no implementar los PSI.

Diferenciación del Tráfico DT

Se entiende por diferenciación de tráfico (DT), a la gestión de tráfico que se usa para degradar o priorizar tipos específicos de tráfico sobre otros, ya sea por su contenido, protocolo, origen o destino.

Es utilizado en prácticas como *zero rating*, ya que permite al usuario decidir que tráfico se tratará con prioridad, puede suponer un mayor beneficio tanto para el usuario final como para el PSI, los cuales darían la misma oportunidad a servicios pequeños y nuevos en el mercado, no afectando a la competencia justa. (Yiannis Yiakoumis, 2016)

Ahora bien, para entender cómo funcionan los algoritmos de diferenciación de tráfico es preciso señalar que desde sus inicios Internet fue pensado para seguir dos principios esenciales para la NN: E2E y el principio llamado *best effort*. El principio E2E establece que los mensajes intercambiados entre dos hosts finales se envían en paquetes que son reenviados por enrutadores autónomos, donde un enrutador simplemente reenvía un paquete al siguiente salto para que el paquete llegue al destino a través de la ruta más corta. En particular, un enrutador no puede definir ni controlar la ruta completa que atraviesa un paquete desde el origen hasta el destino.

Por otra parte, el principio de *best effort* establece que cada paquete debe atravesar la red lo más rápido posible. Un enrutador emplea una cola[55] para administrar los paquetes entrantes. Si la cola crece y utiliza todo el espacio disponible, el enrutador debe descartar los siguientes paquetes entrantes, independientemente de su contenido, origen, destino o cualquier otra característica. (Thiago Garrett, 2018, p. 5)

[54] (OPSITEL, 2022)

[55] También llamada fila, es una estructura de datos caracterizada por ser una secuencia de elementos en la que la operación de inserción se realiza por un extremo y la operación de extracción por el otro.

Existen diversos algoritmos de programación para determinar el envío y reenvío de paquetes, algunos de ellos son considerados como alineados con el principio de neutralidad de la red, esto es, que no discriminan tipos de paquetes, sino que los despachan bajo el principio First in First Out (FIFO). Sin embargo, existen otros algoritmos que sí asignan prioridades a los paquetes recibidos. En la tabla 3 se muestran algunos de los algoritmos antes señalados:

Tabla 2 Despachadores de tráfico[56]

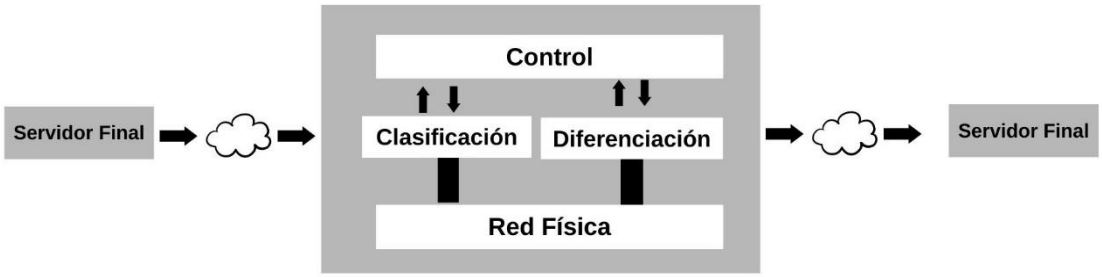
Nombre	Descripción	Neutral
First Come First Served (FCFS)	Los paquetes que llegan primero se reenvían primero	Sí
Strict Priority (SP)	El planificador siempre da prioridad a un tipo específico de tráfico	No
Leaky Bucket	Se definen tarifas máximas para cada tipo de tráfico	No
Token Buket	Se define un límite para la tasa promedio de cada tipo de tráfico	No
Weighted Fair Queuing (WFQ)	Las tasas máximas para los diferentes tipos de tráfico se basan en el peso	No
Drop Tail (DT)	Elimina los paquetes entrantes cuando el búfer está lleno	Sí
Weighted Random Early Detection (WRED)	Los paquetes de baja prioridad tienen una mayor probabilidad de ser descartados	No

[56] Fuente: Elaboración propia con base al estudio Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection de 2022.

Los mecanismos de DT más comunes son **traffic shaping** y el **traffic policing**. *Traffic shaping* emplea despachadores de tráfico (*schedulers*) no neutrales para limitar la tasa de tráfico de clase baja[57] mediante la eliminación de paquetes con más frecuencia, esto puede dar lugar a mayores tasas de perdida. En cambio, *traffic policing* limita la tasa de tráfico al retrasar los paquetes de clase baja, empleando programadores que priorizan el tráfico de clase alta[58] al reenviar o descartar paquetes, esto puede ocasionar mayores retrasos (*delays*) en el reenvío de la información. Otros ejemplos de mecanismos de DT incluyen: inyección de paquetes de restablecimiento de TCP falsificados (RST), lo que obliga a que las conexiones TCP finalicen abruptamente; y el tráfico sea reenviado a través de caminos separados dependiendo de sus clases, siendo uno de estos, el menos congestionado a propósito, el llamado carril rápido. (Thiago Garrett, 2018, p. 6)

En la figura 15 se muestra una descripción de alto nivel de cómo la DT puede incidir en el tráfico entre dos hosts finales. La figura es independiente de las características reales de la red y los mecanismos para DT específicos empleados. La red del PSI que emplea DT se divide en diferentes componentes lógicos. Cualquier tráfico que atraviese el AS (Sistema Autónomos, por sus siglas en inglés) se clasifica y trata de acuerdo con la clase asignada. Un componente de control define cómo se clasifica y diferencia el tráfico. Estos componentes lógicos se ejecutan sobre la red física real. (Thiago Garrett, 2018, p. 6)

Ilustración 15 Descripción de alto nivel de TD en una red de un PSI[59]



Ahora bien, Internet es una red global que funciona a partir de varios Sistemas Autónomos (AS), cada uno de estos comprende prefijos de enrutamiento de Internet, los cuales son controlados por el PSI. Por su parte, los PSI se organizan en 3 niveles. Los PSI de nivel 1 corresponden a la red troncal central de Internet, que consta de redes de alto rendimiento que interconectan a los PSI de nivel 2 a escala

[57] La clase baja es una característica que se asocia con paquetes que tienen poca susceptibilidad a los *delay*s, por ejemplo, el correo electrónico.

[58] Los paquetes de clase alta suelen ser aquellos susceptibles a *delays*, por ejemplo, datos que deriven de aplicaciones de streaming.

[59] (Thiago Garrett, 2018, p. 6)

mundial. Los PSI de nivel 2 brindan conectividad global a los PSI residenciales de nivel 3, que brindan acceso a Internet a los hosts finales. Un host final es cualquier computadora o dispositivo conectado directamente a un PSI de nivel 3 o una puerta de enlace que proporciona conectividad de Internet a una red local. Los hosts finales forman el llamado borde de Internet. (Thiago Garrett, 2018, p. 4)

Es importante destacar, que existen diferentes modalidades para implementar la clasificación del tráfico en una red real. Por ejemplo, la clasificación se puede ejecutar en el punto de entrada de un AS y la información de clase se puede insertar en el encabezado del paquete (de algún protocolo interno de AS) informando a los siguientes enrutadores cómo se debe tratar ese paquete/tráfico. Otra estrategia es configurar todos los enrutadores para clasificar y discriminar el tráfico. DT puede emplearse usando mecanismos diferentes y configuraciones diferentes, pudiendo realizarse solo en la entrada o salida del AS, en varios o en todos los routers de la de red, o mediante dispositivos especializados para DT llamados *middleboxes*. (Thiago Garrett, 2018, p. 5)

IV9 Detección de la Diferenciación de Tráfico

Para la detección de DT se usan diversas plataformas y servicios que adquieren diferentes mediciones en distintos puntos de la red. Estas soluciones monitorean propiedades de red de varios PSI, lo que permite una comparación de diferentes PSI.

Como ya se mencionó, la DT comprende al tratamiento diferenciado de datos, ya sea según su contenido, su protocolo, el origen o el destino. Por ejemplo, DT se puede utilizar para controlar la congestión de datos, limitando las aplicaciones que consumen mucho ancho de banda, como el intercambio de archivos P2P y la transmisión de video, pero también se puede adoptar debido a acuerdos comerciales, mediante los cuales los proveedores de contenido/servicio pagan tarifas adicionales para priorizar su tráfico. La parte relevante de la DT es que, si bien se puede identificar a través de diversos mecanismos, la sola existencia de DT no necesariamente implica una violación al principio de neutralidad de la red.

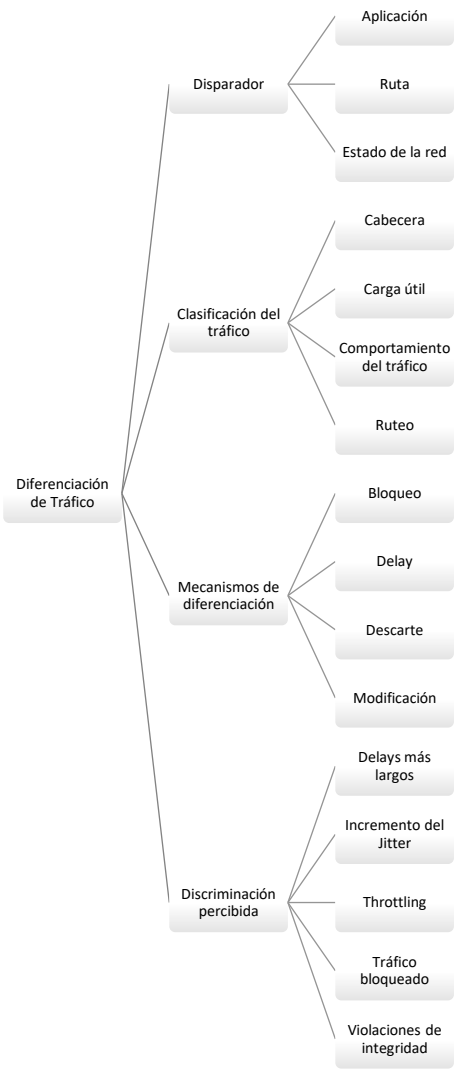
Lo anterior, debe ser analizado a la luz de la regulación que en cada caso se haya establecido, por ejemplo, en la Unión Europea la gestión del tráfico razonable está permitida y cualquier gestión que vaya más allá de lo razonable debe estar justificado por tres casos, a saber: i) como resultado de leyes que así lo señalen (propiedad intelectual), ii) sea necesaria proteger la integridad y seguridad de la red y/o iii) para evitar la congestión de la red.

En consecuencia, se presenta a continuación, una serie de mecanismos que detectan la DT, sin calificarla *per se* como contraria al principio de neutralidad de la red.

Taxonomía de la DT

El diagrama de la ilustración 16, se representa la taxonomía que, de acuerdo con (Thiago Garrett, 2022), caracteriza a la DT. En este contexto, se advierte que la DT consta de 4 elementos principales, a saber: a) un disparador o elemento que hace que se activen los mecanismos de DT; b) la clasificación del tráfico a partir de ciertos elementos del tráfico; c) los mecanismos de diferenciación, y d) cómo se puede "percibir" la diferenciación de tráfico. (Thiago Garrett, 2018)

Ilustración 16 Taxonomía de TD[60]



[60] Elaboración propia con información de (Thiago Garrett, 2018)

Así, para el caso de los disparadores de la DT, se tiene que puede ser por: aplicación, camino de ruteo, o el estado de la red. A partir de que la DT se ha "disparado", se procede a la clasificación de tráfico que puede ser considerando la cabecera del paquete de datos, la carga útil del paquete, el comportamiento del tráfico o el camino de ruteo. Adicionalmente y una vez que se ha clasificado el tráfico, se determina el mecanismo de DT a emplear y este puede ser, bloqueo, *delay*, descarte o modificación de los paquetes de datos.

Finalmente, la forma en la que se puede "percibir" la DT en la red puede ser a través de: *delays* más prolongados, incremento del *jitter*, *throttling*, trafico bloqueado o violación de la integridad del paquete de datos. En la siguiente tabla se muestran algunos ejemplos prácticos de la taxonomía de la DT.

Tabla 3 Taxonomía de DT[61]

Diferenciación de Tráfico (DT)			
Disparadores	Son las condiciones o características del tráfico que puede detectar el PSI para ejecutar DT, el PSI puede discriminar el tráfico porque hay propiedades específicas del tráfico, o por ciertas condiciones.	**Aplicación**	DT puede ser iniciado por una aplicación, la cual es discriminada por el PSI, este puede evitar la congestión ralentizando las aplicaciones que consumen mucho ancho de banda como las de servicios de streaming.
		Ruta	DT activada por ruta, en este puede ser discriminado todo el tráfico que se dirige a algún host especifico o AS específicos, por ejemplo, el PSI puede priorizar el tráfico que proviene de un determinado proveedor de contenido o un AS vecino, siendo esto lo que compone a las *fast-lanes*
		Estado de la Red	Este disparador de DT va en función del estado de la red, por ejemplo, el PSI puede emplear DT en enlaces con alta carga o en horas pico.
			Clasificación basada en la información contenida en el encabezado del paquete de datos, por ejemplo, direcciones o

[61] Elaboración propia con información de (Thiago Garrett, 2018)

Clasificación de tráfico	Se identifican cuatro categorías de clasificación de tráfico.	Encabezado	puertos de origen, destinos, protocolos de transporte utilizados, protocolos de aplicación, entre otros.
		Carga útil	Clasificación basada en los datos de la aplicación, usando información del encabezado de la PDU (Unidad de datos de protocolo, por sus siglas en inglés "*Protocol Data Unit*") de la aplicación, por ejemplo, encabezados de HTTP o BitTorrent, o también en función de la carga útil de la aplicación que se puede identificar mediante DPI y coincidencia de patrones.
		Comportamiento del tráfico	Es una clasificación por tasa de flujo, duración de flujo, tamaño promedio del paquete, intervalos entre paquetes, número de conexiones y ancho de banda total.
		Enrutamiento	Es la clasificación basada en redes o hosts finales de origen y/o destino, AS anteriores y siguientes.
Mecanismos de Diferenciación	Hay varios mecanismos que puede usar un PSI para implementar DT, diferentes mecanismos pueden afectar el tráfico de diferentes maneras, de estos se identificaron cuatro categorías.	Bloqueo	Los mecanismos de bloqueo interrumpen todo el tráfico, simplemente no reenviando paquetes o inyectando mensajes para terminar la conexión (Por ejemplo, con banderas con banderas FIN (*Finalize*, en español finalizar) o RST (*Reset*, en español, reiniciar) configuradas en el protocolo TCP))
		Delay	Los mecanismos de *delay* aumentan o disminuyen el *delay* de los paquetes. Estos mecanismos priorizan paquetes según su

			tipo y/o reenvían paquetes a través de rutas internas que son más rápidas o lentas.
		Descarte	Los mecanismos de descarte degradan el tráfico al descartar paquetes de acuerdo con algunos criterios.
		Modificación	Los mecanismos de modificación alteran los paquetes, el encabezado y/o la carga útil. Por ejemplo, los PSI pueden reducir el tamaño de la ventana TCP para obligar al remitente a reducir la velocidad, o incluso modificar campos de protocolo de aplicación específicos para manipular el comportamiento de la aplicación.
Discriminación percibida	DT es percibida por los usuarios y también por sistemas de monitoreo de diferentes	Mayor *delay*	Los usuarios perciben mayores *delay* al recibir datos de la red.
		Aumento de Jitter	La variación del *delay* es lo suficientemente alta como para interrumpir aplicaciones específicas.
		Estrangulamiento (throttling)	Los sistemas de monitoreo perciben DT como una reducción del ancho de banda disponible, aunque los usuarios lo perciben como demoras más largas o servicios que no responden, son comunes en el caso de las aplicaciones de transmisión de video.

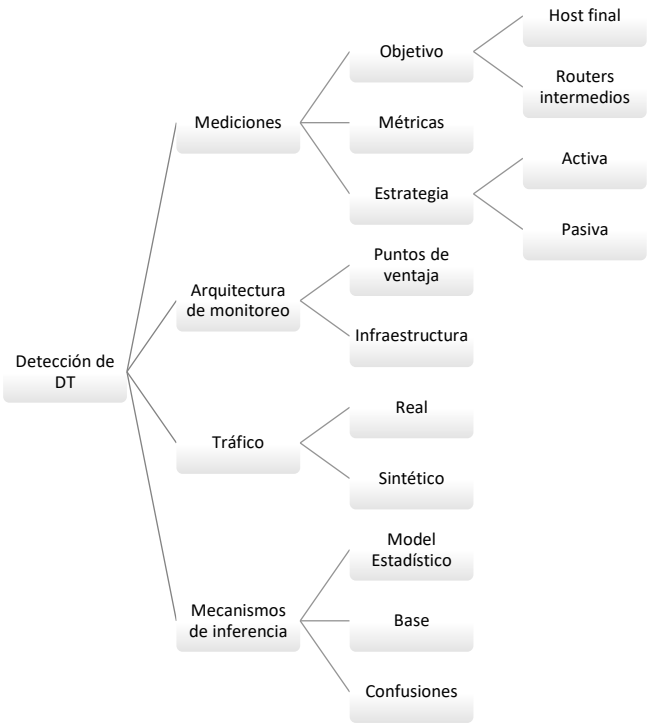
	maneras. Estas características reflejan cómo los usuarios perciben e informan DT.	Bloqueo de Tráfico	Los usuarios no reciben parcial o completamente alguna aplicación en particular.
		Violación de la integridad	La información recibida ha sido modificada en la red de forma no autorizada.

Ahora bien, una vez que se ha descrito la taxonomía de la DT, es posible describir cómo se implementan los mecanismos para detectar la diferenciación de tráfico.

Taxonomía de la detección de DT

En la ilustración 17 se presenta una clasificación para la detección de DT. Se identifican cuatro características principales: Mediciones, Arquitectura de monitoreo, Tráfico y Mecanismo de inferencia. Estas características representan aspectos de las estrategias de detección de DT, para las cuales se realizan mediciones desde los hosts en diferentes topologías; de los datos obtenidos se pueden procesar de diferentes formas para inferir la presencia de DT. (Thiago Garrett, 2018)

Ilustración 17 Taxonomía de la detección de DT[62]



[62] Elaboración propia con información de (Thiago Garrett, 2018)

Tabla 4 Taxonomía de la detección de DT[63]

Detección de la diferenciación de tráfico DTD			
Mediciones	Dado que las prioridades internas de los AS no se conocen a profundidad, las soluciones de detección de DT se basan en mediciones por fuera de la red infiriendo lo que sucede en el interior. Estas medidas se realizan en los hosts finales, los cuales tienen 3 características principales.	Objetivo	Las mediciones pueden tomarse en los hosts finales, sin considerar los *routers* de en medio, por ejemplo, las soluciones pueden medir el ancho de banda de subida en un host final, y medir el ancho de banda en el otro host final, ignorando cómo los *routers* intermedios interfieren en las mediciones.
		Métricas	Hay varias métricas que se pueden usar para evaluar diferentes tipos de tráfico. Los mecanismos de DT afectan el tráfico de diferentes maneras, por lo cual se usan diferentes métricas, como la vigilancia de tráfico que tiene un mayor impacto en la tasa de pédida en el *delay*. El rendimiento también puede verse afectado por la configuración y la vigilancia, ya que ambos harán que se transfieran menos paquetes durante un intervalo de tiempo determinado. Las métricas más comunes son el *delay*, la tasa de perdida y el *throughput*, aunque hay algunas otras.

[63] Elaboración propia con base al estudio *Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection* de 2018.

Detección de la diferenciación de tráfico DTD			
		Estrategia	Activo: Las mediciones activas **generan tráfico**, es decir sondas o flujos entre uno o más pares de hosts finales. Por ejemplo, las mediciones se pueden hacer para evaluar el *throughput* de las sondas, otro ejemplo es cuando el host inicial envía un archivo a un host final usando el protocolo FTP, ahí se evalúa el *throughput* a través de métricas como *throughput*, tasa de pérdidas de paquetes, *delay*, entre otros.
			Pasivo: Las mediciones pasivas consisten en observar el tráfico real de la red, sin generar sondas o flujos, las mediciones suelen ser en ambos finales, evaluando el desempeño de las características al enviar y recibir paquetes.
			Hibrido: estás mediciones pueden ser tanto activas como pasivas dependiendo de las pruebas que se realicen.
	Las mediciones pueden ser hechas usando diferentes tipologías y pueden requerir control de algunos o de todos los hosts que participan	**Infraestructura controlada**	Una solución de monitoreo puede requerir el control de uno o más hosts para hacer mediciones, tiene que tomar control de infraestructura preexistente para realizar mediciones. Por ejemplo, una solución puede correr una aplicación de medición en ambos hosts, que

Detección de la diferenciación de tráfico DTD			
Arquitectura de monitoreo	en las mediciones, dos aspectos diferentes de esto son:		puede o no requerir una instalación en ambos hosts, o mediciones basadas en alguna actividad existente como una red P2P.
		Puntos de ventaja	Las mediciones pueden ser tomadas desde diferentes puntos de vista. Por ejemplo, una solución puede requerir solo mediciones entre un par de hosts finales o entre múltiples pares de hosts finales recopilando los datos obtenidos.
Tráfico	Para inferir si hay DT se pueden usar diferentes tipos de tráfico. Se identifican dos tipos.	Real	Una solución para la detección de DT puede tomar ventaja del tráfico ya existente. Por ejemplo, las mediciones pasivas solo observan el tráfico, haciendo mediciones sin introducir nuevo tráfico a la red.
		Sintético	Se puede generar tráfico para realizar las mediciones, por ejemplo, algunas soluciones generan diferentes tipos de tráfico modificando tráfico real anteriormente grabado, mientras que otros crean tráfico solo siguiendo especificaciones de los protocolos de aplicación.

Detección de la diferenciación de tráfico DTD			
Mecanismos de Inferencia	Hay diferentes enfoques posibles para detectar DT a partir de las mediciones realizadas, se han identificado tres principales características	Modelo estadístico	Se pueden utilizar diferentes modelos estadísticos para analizar los datos recolectados y hacer conclusiones.
		Base	La mayoría de las soluciones comparan las mediciones de los tipos de tráfico con respecto a un tráfico de referencia, asumiendo que el tráfico no está siendo discriminado. Esta comparación contra el tráfico de referencia se puede obtener de diferentes maneras.
		Confusiones	Las confusiones son factores importantes ya que pueden tener un impacto en el tráfico. Diferentes soluciones consideran diversos factores de confusión y los enfocan de maneras diferentes, por ejemplo, algunas soluciones miden varias veces para reducir el tráfico cruzado.

Con base en la clasificación anterior, (Thiago Garrett, 2018) se presenta una clasificación de los mecanismos/algoritmos más conocidos que se han publicado para la detección de la diferenciación de tráfico.

Tabla 5 Herramientas para detectar la diferenciación de tráfico[64]

	Algoritmo/Mecanismo	Gnutella RSP	NetPolice	NANO	POPI	DiffProbe	Glasnost	Packsen
Mediciones	Métrica	Conectividad	Tasa de pérdida	Depende de la aplicación	Tasa de pérdida	Dealy y tasa de pérdida	throughput	Tiempos de llegadas y ancho de banda
	Hosts finales de destino	Host de medición	-	Múltiples hosts finales	Par de host finales	Par de host finales	Par de host finales	Par de host finales
	Objetivo: Routers intermedios	-	Puntos de ingreso y egreso	-	-	-	-	-
	Estrategia	Hibrido	Activo	Pasivo	Activo	Activo	Activo	Activo
Arquitectura de monitoreo	Puntos de ventaja	Un host de medición y múltiples hosts finales	Múltiples hosts finales	Múltiples hosts finales	Un par de hosts finales	Un par de hosts finales	Múltiples hosts finales y hosts de medición	Múltiples hosts finales y hosts de medición
	Infraestructura existente	Red Gnutella P2P	-	-	-	-	-	-
	infraestructura controlada	Un host de medición y un superpeer	Múltiples hosts finales en diferentes redes	Múltiples hosts finales en diferentes redes	Un par de hosts finales	Un par de hosts finales	Host final, hosts de medición y servidor web	Host final, hosts de medición, y un servidor experimental
Tráfico	Real	Protocolo Gnutella	-	Tráfico real existente en hosts finales	-	-	-	-
	Sintético	Referencial	HTTP, BitTorrent, STMP, PPlive y VoIP	-	Varias ráfagas que contienen varios tipos de trafico	Establecido en aplicaciones	Basado en tráfico real	No especificado

[64] Elaboración propia con información de *Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection* de 2018.

	Algoritmo/Mecanismo	Gnutella RSP	NetPolice	NANO	POPI	DiffProbe	Glasnost	Packsen
						de tráfico real		
Mecanismo de inferencia	Modelo estadístico	Modelo probabilístico para inferir si los puertos fueron bloqueados	Compara el throughput de diferentes aplicaciones con el throughput de la línea base	Agrupación de mediciones con factores de confusión similares, y realiza comparaciones con la línea base[65]	Clasifica las mediciones para cada ráfaga de datos y verifica si algún tipo de tráfico se clasificó consistentemente más alto que otros.	Compara el throughput de una aplicación con el throughput de la línea base	Compara el throughput de una aplicación con el throughput de la línea base	Compara el throughput de una aplicación con el throughput de la línea base
	Base	-	Asume que el tráfico HTTP no sufre TD	La línea base es el throughput promedio de varios PSI	-	La línea base se genera en función de la aplicación de destino y se asume que no está discriminada	La línea base se genera en función de la aplicación de destino y se asume que no está discriminada	Se asume que la línea base no está discriminada.
	Confusiones	Los clientes de Gnutella podrían ignorar las referencias.	Compara solo medidas relativas a un mismo núcleo (AS)	Requiere la identificación de todos los factores de confusión relevantes (relacionados con los hosts, la red y el tiempo)	Envía múltiples ráfagas de paquetes en orden aleatorio	Ambos tráficos tienen las mismas propiedades, como el tamaño de los paquetes y los intervalos de envío.	Emplear diferentes hosts de medición para evitar medidas evasivas de los proveedores de servicios de Internet	Repite las medidas varias veces; mantiene un ancho de banda constante para ambos tráficos

Tabla 6 Continuación Herramientas para detectar la diferenciación de tráfico (Fangfan Li, 2019) (Thiago Garrett, 2018) (Glorioso, 2008) (Vitali Bashko, 2013)

[65] Tráfico de referencia.

	Mecanismo/Algoritmo	Tomography	ChkDiff	VPN	Bonafide	Windrider	Neubot	Netalyzr	Wehe
Mediciones	**Métrica**	Cualquier métrica aditiva	Delay y tasa de pérdida	throughput demoras y tasa de pérdida	throughput de subida y de bajada	Tiempo de ida y vuelta y throughput	throughput Tiempo de ida y vuelta	Accesibilidad del servicio, filtrado de contenido	throughput
	Hosts finales de destino	Multiples host finales	-	Par de host finales	Par de host finales	Host final con opción de más host a petición del usuario	-	Múltiples host finales	Par de host finales
	Objetivo: Routers atravesados	-	¿	-	-	-	-	-	-
	Estrategia	Activo	Activo	Activo	Activo	Hibrido	Activo	Pasivo	Activo
Arquitectura de monitoreo	**Puntos de ventaja**	Múltiples hosts finales	Un solo host final	Un par de hosts finales	Múltiples hosts finales y hosts de medición	Uno o más hosts finales	Múltiples hosts finales	Múltiples host finales	Par de host finales
	Infraestructura existente	-	-	-	-	-	MLab	-	Aplicación
	infraestructura controlada	Múltiples hosts finales	Un solo host final	Un host final, un servidor VPN, y un host de medición	Host final, hosts de medición y servidor web	Uno o más hosts finales	Múltiples hosts finales	Múltiples host finales	Par de host finales
Tráfico	**Real**	-	Registra el tráfico real en el host final	Graba una aplicación de tráfico real	-	Tráfico basado en aplicaciones	Tráfico real existente en hosts finales	Tráfico real en hosts finales basado en protocolos HTTP y STMP	Tráfico real en hosts finales
	Sintético	No especificado	Reproduce tráfico con modificaciones	Reproduce tráfico a través de diferentes canales	Basado en tráfico real	No especificado	P2P, BitTorrent, VoIP, HTTP, SMTP	-	-
Mecanismo de inferencia	**Modelo estadístico**	Emplea tomografía de red para combinar mediciones desde diferentes puntos de vista y encontrar enlaces no neutrales	Compara cada tipo de tráfico reproducido con todos los demás tipos	Compara el throughput del tráfico registrado cuando está encriptado (VPN) y no encriptado (comunicación abierta convencional)	Compara el throughput de una aplicación con el rendimiento de la línea base	Compara el throughput en diferentes puertos según la aplicación	Compara el throughput la demora, el jitter y protocolos entre servidores y P2P	investiga propiedades de red, como traducción de direcciones IP, compatibilidad con IPv6, restricciones de descarga basadas en contenido, manipulación de contenido	"Grabar y reproducir" Compara el throughput de las aplicaciones con la línea base

	Base	-	La línea base es todo el tráfico, excepto para el tipo que se está evaluando	La línea base es el tráfico encriptado, reproducido en una VPN, que se supone no discriminado	La línea base se genera en función de la aplicación de destino y se asume que no está discriminada	No especificado	No especificado	-	La línea base es el tráfico de red generado por una aplicación asumiendo que no está discriminado
	Confusiones	-	El tamaño de todos los paquetes está estandarizado	-	Emplear diferentes hosts de medición para evitar medidas evasivas de los proveedores de servicios de Internet	-	-	-	-

Como se puede observar en las tablas anteriores, existe una diversidad de algoritmos/mecanismos para detectar la diferenciación del tráfico. Sin embargo, la mayoría de estos no cuentan con una arquitectura de monitoreo que vaya más allá de un entorno de pruebas controlado. Lo anterior, obedece a la complejidad y costo del desarrollo de una arquitectura de monitoreo abierta al público en general.

A pesar de lo anterior, se identifican al menos dos mecanismos, a saber: Neubot y WeHe que cuentan en el primer caso con una plataforma de mediciones M-LAB y, en el segundo, con una aplicación disponible para sistemas operativos Android y iOS.

M-LAB

En 2008, Vint Cerf, uno de los "padres de Internet", comenzó una serie de conversaciones con investigadores de Internet para aprender más sobre los desafíos que enfrentaron al tratar de estudiar el rendimiento de Internet. Los investigadores identificaron varios problemas, incluida la falta de servidores ampliamente implementados con amplia conectividad para realizar experimentos de medición de Internet. También informaron de la incapacidad de compartir grandes conjuntos de datos entre sí fácilmente (MLab, 2022).

De igual forma, tampoco existía un recurso público que pudiera proporcionar datos combinados de rendimiento a los responsables de la formulación de políticas o a los consumidores interesados en comprender el rendimiento de su servicio de Internet a lo largo del tiempo. Como resultado de estas conversaciones, M-Lab se fundó para ayudar a abordar los problemas centrales experimentados por los investigadores y para promover la medición de código abierto a gran escala de Internet (MLab, 2022).

En este contexto, M-Lab es un proyecto de código abierto con colaboradores de organizaciones de la sociedad civil, instituciones educativas y empresas del sector privado dedicadas a:

- Proporcionar una plataforma de medición abierta y verificable para el rendimiento de la red global;
- Alojar el mayor conjunto de datos abiertos de rendimiento de Internet del planeta, y
- Crear visualizaciones y herramientas para ayudar a las personas a dar sentido al rendimiento de Internet.

Así, de acuerdo con información de M-Lab, dicha plataforma tiene como objetivo avanzar en la investigación de Internet al capacitar a los consumidores con información útil sobre su rendimiento en Internet. Al proporcionar datos de medición de Internet abiertos y gratuitos, los investigadores, los reguladores, los grupos de defensa y el público en general pueden tener una mejor idea de cómo Internet está funcionando para ellos, y cómo mantenerlo y mejorarlo para el futuro (MLab, 2022).

Al respecto, se señala que todos los datos recopilados por la plataforma de medición global M-Lab están disponibles abiertamente, y todas las herramientas de medición alojadas por M-Lab son de código abierto. En la siguiente tabla se muestran las pruebas que actualmente se realizan bajo M-Lab.

Actualmente M-Lab ofrece los siguientes servicios (MLab, 2022):

- Packet Headers. Recopilación de encabezados de paquetes de datos para todos los flujos TCP entrantes y guarda cada flujo de capturas de paquetes en archivos tipo ".pcap".
- TCP Info. Recolecta estadísticas sobre las conexiones TCP que se ejecutan en la plataforma M-Lab utilicando tcp-inf.
- Traceroute. Recopila información de ruta de red para cada conexión a la plataforma M-Lab.

Tabla 7 Pruebas que actualmente se realizan en M-Lab[66,67]

	Pruebas	Descripción
Plataforma M-Lab	NDT (Network diagnostic Tool)	NDT mide el " throughput de flujo único" o la "capacidad de transporte a granel". NDT informa de las velocidades de carga y descarga y las métricas de latencia.
	Neubot DASH	DASH está diseñado para medir la fragilidad de las redes bajo prueba, emulando un reproductor de transmisión de video.

[66] Otras pruebas tales como: BISmark, Glasnot, NPAD, OONI Probe, MobiPerf, Pathloadd2, SamKnows, Shaperprobe y Windrider ya no estás realizando en la plataforma M-Lab. No obstante, los datos recolectados de dichas pruebas están disponibles en la plataforma.

[67] Consultado el 6 de junio de 2022. https://www.measurementlab.net/about/

	Reverse Traceroute	Mide la ruta de red de regreso al usuario desde los puntos del extremo de red seleccionados.
	WeHe	Emplea el dispositivo del usuario final para intercambiar el tráfico de Internet registrado desde aplicaciones reales y populares como YouTube y Spotify, e intenta advertir si un PSI está dando un trato diferenciado al tráfico de red de una aplicación en particular.

Aplicación WeHe

La aplicación Wehe se lanzó al público el 28 de septiembre de 2017, esta herramienta fue desarrollada por la ARCEP en colaboración con la Northeastern University. WeHe está basada en código fuente abierto. Está disponible para los dispositivos Android, iOS y recientemente en F-Droid. A finales del año 2020 se lanzó una nueva versión de WeHe, en la cual se implementó una lista de servicios más amplios para realizar mediciones, que incluye aplicaciones de video, música y videoconferencias. (ARCEP, 2021)

WeHe tiene dos funciones principales; **i)** realizar pruebas de detección de diferenciación de tráfico, y **ii)** pruebas de bloque de puertos. Lo anterior, con la finalidad de analizar el tráfico generado a través de la aplicación para determinar si es probable que el operador de redes restrinja o priorice ciertos flujos o puertos de acceso a Internet.

Prueba de detección de diferenciación de tráfico

La prueba de diferenciación es la base de la aplicación WeHe, esta permite analizar el tráfico para determinar si el operador puede estar restringiendo o priorizando determinados servicios o aplicaciones; esta prueba se realiza en tres etapas (ARCEP, 2021).

1) En la primera etapa, la herramienta simula que se está usando un servicio o aplicación [68] para medir cómo el PSI procesa el tráfico real de dicha aplicación o servicio, este tráfico real se graba para tenerlo después como un tráfico de referencia.

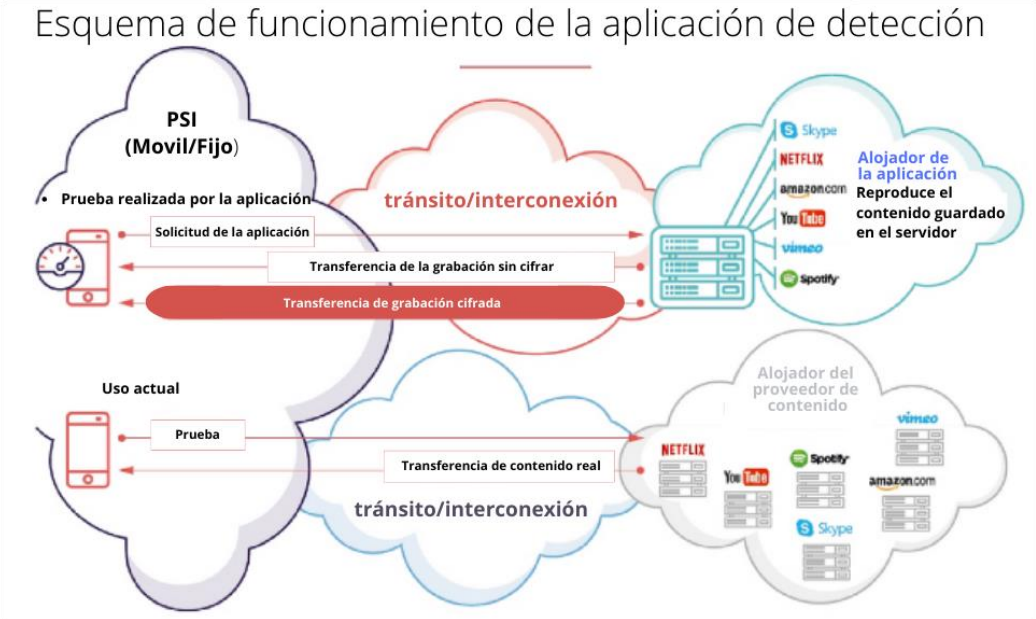
2) Posteriormente, la herramienta simula la misma cantidad de tráfico, solo que reemplazando el contenido de los paquetes por un texto sin formato y cuyo contenido este encriptado (a través de una VPN) y es invisible para el PSI, después de esto, compara los caudales de tráfico medidos en ambas etapas de la medición.

3) Por último, la herramienta repite la prueba para disminuir el margen de error que podría haber por el estado de la red en determinado momento. En caso de que haya una diferencia significativa entre ambas simulaciones de tráfico, la aplicación infiere si existe una medida de gestión de tráfico implementada por el PSI.

En caso de que haya una diferencia significativa entre ambas simulaciones de tráfico, la aplicación muestra como resultado "diferenciado". (ARCEP, 2021) En la ilustración 18, se muestra el proceso de la prueba. En el anexo 1A "Pruebas de detección de diferenciación de tráfico con sistema iOS y Android" se presentan algunos resultados en los que se detectó la aplicación de gestión de tráfico.

[68] En la versión para IOS algunas de las aplicaciones y servicios son Spotify, YouTube, Disney, Netflix, WhatsApp, primevideo, twitter video, Apple Music, Google Meet, Microsoft Teams, Skype, Webex y Zoom.

Ilustración 18 Esquema de funcionamiento de la aplicación de detección de diferenciación[69]



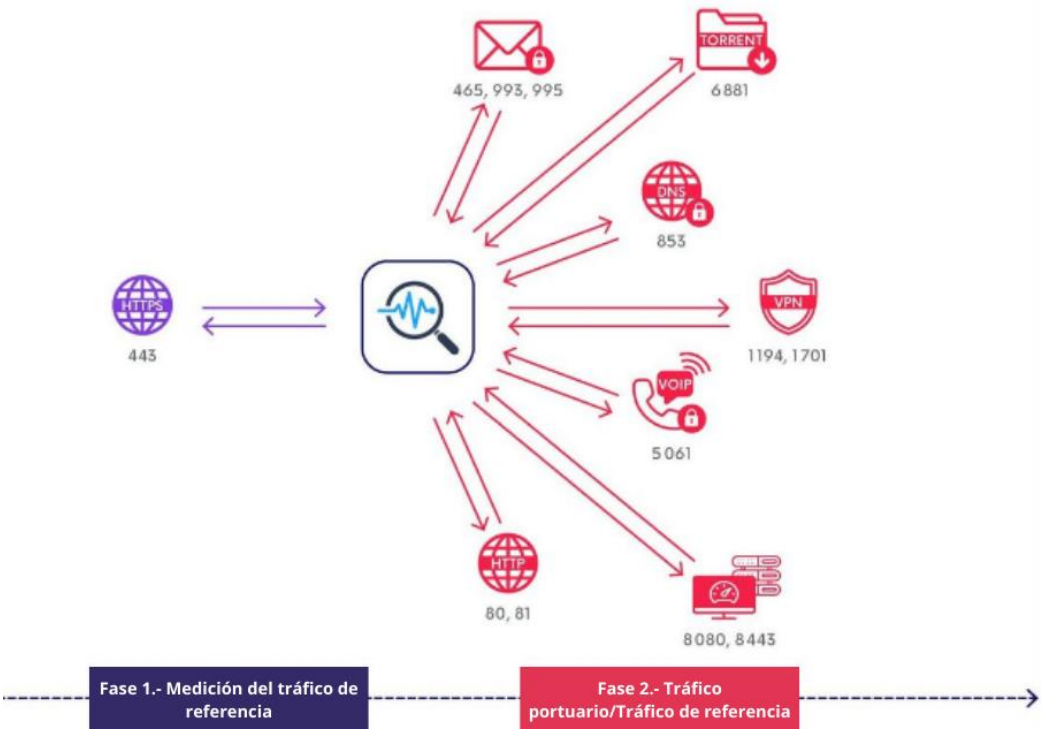
Prueba de Puerto

La segunda herramienta que ofrece WeH*e* y que recientemente fue añadida a la aplicación es la prueba de puertos, esta prueba detecta el bloqueo, restricción, priorización de puertos de software afectando el uso de ciertas aplicaciones o servicios para los usuarios. Actualmente, la aplicación brinda la capacidad de monitorear 12 de los puertos de software más utilizados, en la tabla 8 se describen dichos puertos (ARCEP, 2021).

En la ilustración 19 se muestra el funcionamiento de la detección de bloqueo de puertos. La prueba de puertos se caracteriza por dos fases, la primera, mide el tráfico del puerto 443, el cual es considerado como puerto de referencia, en la segunda etapa, se compara el tráfico https de cada uno de los puertos que selecciona el usuario final, relacionándolo con el tráfico del puerto 443. En caso de alguna desemejanza comprobada, la aplicación lo notifica, lo que, en términos prácticos, significaría el bloqueo del puerto bajo prueba. (ARCEP, 2021)

[69] (ARCEP, 2021)

Ilustración 19 Diagrama de funcionamiento de Pruebas de puerto[70]



Actualmente la aplicación brinda la capacidad de monitorear 12 de los puertos de software más utilizados que son:

Tabla 8. Puertos donde la aplicación WeHe puede detectar bloqueo[71]

Puerto	Descripción
80 HTTP	Se utiliza para la navegación web de forma no segura mediante el protocolo HTTP (Hypertext Transfer Protocol, en español, Protocolo de transferencia de hipertexto), es el puerto establecido por defecto en el servidor Web en la mayoría de las computadoras (Espinosa, 2022) (Palmer, 2021).

[70] (ARCEP, 2021)

[71] Elaboración propia con información de WeHe

Puerto	Descripción
81 HTTP	Es un puerto alternativo al 80, funciona como puerto de servidor web si el puerto anterior no se encuentra disponible por cualquier razón. (Espinosa, 2022)
465 SMTPS	Es un puerto que identifica al servicio específico SMTP (Simple Mail Transfer Protocol) protocolo especializado para la transmisión de correo electrónico en la web (Duó, 2021)
853 DoT	Es un puerto utilizado para DNS (*Domain Name System*, en español Sistema de nombres de dominio) sobre TLS (*Transport Layer Security,* en español, Seguridad de la capa de transporte) a lo que llamamos protocolo DoT, que es un protocolo de seguridad para cifrar y empaquetar las consultas y respuestas DNS a través del protocolo TLS, con la finalidad de aumentar la privacidad y seguridad de los usuarios. (Sáez, 2019)
993 IMAPS	Es un puerto dedicado al protocolo IMAP (*Internet Message Access Protocol,* en español, protocolo de acceso a mensajes de internet) el cual es un protocolo de correo usado para acceder al correo de un servidor web remoto desde un cliente local. (SiteGround, 2021)
995 POP3S	Es el puerto utilizado para conectarse usando POP3 (*Post Office Protocol version 3*) el cual es un protocolo de correo que se usa para la recepción de correo desde un servidor remoto a un cliente de correo local de forma segura (cifrada). (SiteGround, 2021)
1194 OpenVPN	Es el puerto utilizado por el protocolo OpenVPN para las redes privadas virtuales. (Espinosa, 2022)
1701 L2TP	Es el utilizado por el protocolo L2TP (*Layer 2 Tunneling Protocol*), este es un protocolo de túneles que amplía el protocolo punto a punto para que dé soporte a un túnel en la capa de enlace entre un cliente L2TP solicitante y un servidor L2TP destino. (IBM, 2021)
5061 SIPS	Es el puerto utilizado para el protocolo SIP (*Session Initiation Protocol*) el cual es un protocolo de señalización utilizado para establecer una “sesión” entre 2

Puerto	Descripción
	o más participantes, modificar esa sesión y eventualmente terminar esa sesión. (3CX, 2022) (olprod, 2022)

IV10 Otros mecanismos para vigilar el cumplimiento de la neutralidad de la red

Censorship

Otro concepto relevante respecto de la NN es la censura en Internet, de acuerdo con Mueller, a diferencia de los mecanismos que atienden a la QoS de Internet, existen incidentes reales de bloqueo y censura de Internet por parte de los operadores de red y los gobiernos. El ejemplo más famoso, de acuerdo con Mueller, es probablemente el caso de Madison River, en el que una compañía telefónica regional en los Estados Unidos utilizó el bloqueo de puertos para evitar que sus suscriptores usaran el servicio de voz sobre protocolo de Internet (VoIP) de Vonage[72] (Vonage también se quejó durante este período de que algunas compañías de televisión por cable estaban bloqueando su servicio por razones anticompetitivas). También hay ejemplos de operadores que frenan el uso de protocolos peer-to-peer específicos, como BitTorrent.[73] Como ejemplos de control o bloqueo motivados por la censura, tres incidentes se han vuelto particularmente conocidos. El PSI canadiense Telus bloqueó el acceso a un sitio web de un sindicato en huelga. AT&T eliminó parte de un concierto en vivo por Internet de Pearl Jam cuando la banda criticó a George Bush. (Mueller, et al., s.f.).

En este contexto, de acuerdo con la literatura en la materia, se pueden clasificar las técnicas de censura en Internet en 3 principales tipos, a saber:

[72] The Madison River Company was quickly sanctioned and fined by the Federal Communications Commission. U.S. Federal Communications Commission, Consent Decree, In the matter of Madison River Communications LLC, and affiliated companies, File No. EB-05-IH-0110, FRN: 0004334082. http://www.fcc.gov/eb/Orders/2005/DA-05-543A2.html

[73] 12 The most recent case involved cable ISP Comcast deliberately interfering with BitTorrent users; see Harold Feld's incisive analysis of this incident at his blog: http://www.wetmachine.com/item/912. Also see Michael Geist blog, "The unintended consequences of Rogers' packet shaping." http://www.michaelgeist.ca/content/view/1859/125/

- Censura basada en el cliente

Se considera como el bloqueo de acceso a contenido en línea por medio de aplicaciones ejecutadas en el mismo sistema del cliente de la aplicación en la red. Una propiedad característica de la censura basada en el cliente es que las funcionalidades del sistema de censura están ligadas al sistema del cliente, por lo que puede ser difícil que se detecte. Se implementa por diferentes medios, como aplicaciones independientes similares a un *Keylogger* (Dispositivo que registra las pulsaciones en un teclado para memorizarlas en un archivo o enviarlas a Internet), los cuales mediante palabras clave pueden finalizar ciertas aplicaciones. Otra manera de implementarla es el control parental o los filtros de aplicación de control de políticas de la empresa que se ejecutan en un firewall personal. También se puede implementar con versiones modificadas de aplicaciones, los cuales pueden contar con características de vigilancia, algunas de ellas pueden ser TOM-Skype o SinaUC. (Giuseppe Aceto, 2015, p. 4)

- Censura basada en el servidor

La censura basada en el servidor se aplica en el nodo final de la ruta de comunicación sin interrumpir la mecánica de la comunicación, el censor elimina, oculta o impide acceder al contenido específico directamente en el servidor. Se puede ejecutar ordenando al administrador del servidor que cumpla con la solicitud de censurar información. Los PSI reconocen que en ocasiones hay existencia de esta acción de censura, tal es el caso del informe de transparencia de Google[74], en las cuales se divulga un resumen de solicitudes del gobierno o de propietarios de los derechos de autor para bloquear acceso a contenido especifico. Igualmente es difícil detectarlo, ya que su mecánica se ejecuta de manera interna en el servicio, y no es expuesta a los usuarios. (Giuseppe Aceto, 2015, p. 4)

- Censura basada en la red

Este tipo de censura se ejecuta entre el host del cliente y el host en donde se ejecuta la parte correspondiente al servidor. Esta proporciona al censor una cobertura más amplia de la red con mayor eficiencia, lo que permite el control de un gran número de comunicaciones a través de la gestión de pocas puertas de enlace o concentradores.

Al respecto, algunas herramientas para la detección del “censorship” en Internet permiten realizar mediciones con las que se genera un censo que contiene un listado temas, servicios y sitios web que han sufrido algún tipo de bloqueo o filtro a los cuales el usuario final no puede acceder libremente (Thiago Garrett, 2018).

[74] Informe de transparencia Google. Retirada de contenido por infracciones de derechos de autor. Disponible en: https://transparencyreport.google.com/copyright/overview?hl=es

Content Modification

En la misma línea que el "censorchip" se encuentra Content Modification o modificación de contenido, y se entiende como la inyección de paquetes falsos en una comunicación con los hosts finales, lo cual altera la información contenida en los paquetes; en algunos casos, se puede detectar si el Content Modification se genera por los usuarios finales o por los PSI para discriminar el tráfico no deseado o para obtener algún tipo de ventaja, como la inyección de paquetes para terminar la comunicación entre hosts. (Thiago Garrett, 2018)

V. Mecanismos de monitoreo de la QoS del SAI existentes en el Instituto Federal de Telecomunicaciones

Como se ha señalado previamente, de la experiencia internacional se advierte la existencia de parámetros de QoS del SAI en el contexto de la neutralidad de la red. Esto es que, para dar cumplimiento al principio de neutralidad de la red, los reguladores han establecido ciertos parámetros asociados con la QoS, bajo la premisa de que la aplicación de gestión de tráfico puede ser observable a través de la variación de dichos parámetros.

Ahora bien, en México existe regulación específica respecto de la QoS del SAI fijo y móvil. Sin embargo, dicha regulación no fue establecida con el objetivo de monitorear el cumplimiento del principio de neutralidad de la red.

A continuación, se describen brevemente las características del marco regulatorio nacional en torno a la QoS del SAI fijo y móvil.

V1 Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo (Lineamientos de calidad del SAI fijo)

El 25 de febrero de 2020 se publicó en el DOF el "Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones emite los Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo"[75], a través de dichos lineamientos, el Instituto, en ejercicio de sus facultades, estableció los índices y parámetros de la calidad del SAI[76] fijo con la intención de contar con único instrumento regulatorio homologado. (IFTc, 2020)

En este contexto los Lineamientos de calidad del SAI fijo establecen parámetros de calidad de acuerdo con especificaciones técnicas (IFTc, 2020):

[75] Disponibles en: http://www.ift.org.mx/sites/default/files/conocenos/pleno/sesiones/acuerdoliga/dof131119647acc.pdf

[76] Si bien en los Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo, se incluye al servicio de telefonía fijo, las referencias en este estudio solo se consideran para el servicio de acceso a Internet fijo, toda vez que es para este servicio al que resulta aplicable el principio de neutralidad de la red.

- ETSI ES 202 057-4: "Aspectos del Procedimiento del Habla, Transmisión y Calidad (STQ); Definiciones y mediciones de parámetros de calidad del servicio relacionados con el usuario; Parte 1: Acceso a Internet", emitida por el ETSI, y
- El parámetro de pérdida de paquetes se establece con base en la recomendación UIT-T Y.1540 "Servicio de comunicación de datos con protocolo Internet- Parámetros de calidad de funcionamiento relativos a la disponibilidad y a la transferencia de paquetes de protocolo Internet".

Aspectos generales de los Lineamientos de calidad del SAI fijo

Sujetos obligados

Los prestadores del Servicio de Acceso a Internet fijo[77]

Parámetros de Calidad del SAI

I. **Tasa de Transmisión de Datos Promedio de Descarga** (*download speed*). Cantidad promedio de datos que se descargan por segundo y que se obtiene dividiendo la Tasa de Transmisión de Datos acumulada de las sesiones exitosas entre el número total de sesiones.
II. **Tasa de Transmisión de Datos Promedio de Carga** (*upload speed*). Cantidad promedio de datos que se cargan por segundo y que se obtiene dividiendo la tasa de Transmisión de Datos acumulada de las sesiones exitosas entre el número total de sesiones.
III. **Latencia promedio**. Estimación del tiempo promedio de respuesta de un servicio entre dos puntos específicos (origen y destino) de una red de datos que se obtiene dividiendo el acumulado de dichos tiempos para cada sesión entre el número total de sesiones.
IV. **Proporción de Paquetes Perdidos**. Estimación del grado de fiabilidad del SAI con base en la determinación de la proporción de Paquetes de Datos perdidos con respecto al total de paquetes de datos enviados.

Carácter de los Parámetros de Calidad

I. Tasa de Transmisión de Datos Promedio de Descarga- **informativo**

[77] No obstante, los PSI sujetos a la Medición de los Eventos del SAI, solo se considerarán a aquellos PSI que cuenten con más de un millón de accesos a internet totales, conforme a la información del BIT.

II. Tasa de Transmisión de Datos Promedio de Carga- **informativo**
III. Latencia promedio- **informativo**
IV. Proporción de Paquetes Perdidos- **informativo**

Fallas y su evaluación

Se establecen los Parámetros de Calidad en la atención de Fallas a nivel de los usuarios finales.

I. **Proporción Reportes de Fallas**. Porcentaje de Reportes de Fallas recibidos a nivel mensual respecto al número total de accesos al SAI. El índice de calidad deberá ser menor o igual al **3.5%** al mes
II. **Proporción de reparación de Fallas en un día**. Porcentaje de Reportes de Fallas que fueron atendidos por el PSI y el servicio restaurado a nivel mensual. El índice de calidad asociado deberá ser mayor o igual al **85%**
III. **Proporción de reparación de Fallas en tres días**. Porcentaje de Reportes de Fallas que fueron atendidos por el PSI y el servicio restaurado a nivel mensual. El índice de calidad asociado deberá ser mayor o igual al **97%**
IV. **Tiempo promedio de reparación del SAI**. Cantidad de tiempo promedio necesario para restablecer un SAI por el PSI a nivel mensual. Este parámetro es de carácter informativo.

Algunas obligaciones

Obligación de los PSI respecto de poner a disposición del usuario final los mapas de cobertura del SAI, para cada tecnología de acceso de manera desagregada. Dichos mapas podrán ser consultados por los usuarios en el portal del PSI.

La velocidad de transferencia de datos publicitada para cada paquete de servicios de telecomunicaciones deberá corresponder a la Tasa de Transmisión de Datos promedio de Descarga, expresa en Mbps y no deberá referirse a las velocidades máximas.

Los PSI deben contar con un sistema de atención a usuarios finales, ya sea a través de centros de atención o vía telefónica y/o vía electrónica (chat en línea Y/o correo electrónico) para atender de manera gratuita consultas y quejas relativas al servicio, así como el seguimiento a estas.

Los PSI que operen sus propios sistemas de gestión y que puedan generar archivos de contadores de desempeño, deberán entregar de manera electrónica cada trimestre un reporte auditado.

Medición de los Parámetros de la Calidad del Servicio de Acceso a Internet

A efecto de llevar a cabo la medición de los parámetros de Calidad del Servicio de Acceso a Internet, los PSI deberán instalar la "Herramienta de Medición en los Equipos Terminales"[78] de los usuarios finales, siempre que esto sea técnicamente factible.

Los PSI deberán desarrollar una interfaz de programación de aplicaciones (API) en los Equipos Terminales del cliente que serán medidos, mediante la cual se deberá recolectar la siguiente información: velocidad de transferencia de datos contratada y el identificador único del usuario final.

Se establece un procedimiento de medición de los parámetros de calidad del SAI a partir de la determinación del tamaño de muestra y el número de eventos, considerando un muestreo aleatorio simple con un nivel de confianza del 95%. Cada ejercicio de medición se llevará a cabo a lo largo de un año natural para cada PSI que brinda el SAI en el domicilio de los usuarios finales y en horarios determinados. Adicionalmente, se establecen las características de la Herramienta de Medición, entre las que destacan: que no deberá recolectar datos personales de los usuarios finales ni invadirá la privacidad del usuario final y que no deberá interferir con la prestación habitual del servicio, ni con el funcionamiento del equipo terminal.

V2 Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio móvil (Lineamientos de calidad del SAI móvil)

El 17 de enero de 2018 se publicó en el DOF el "Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones aprueba y emite los lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio móvil y se abroga el Plan Técnico Fundamental de Calidad del Servicio Local Móvil publicado el 30 de agosto de 2011, así como la metodología de mediciones del Plan Técnico Fundamental de Calidad del Servicio Local Móvil publicada el 27 de junio de 2012", a través de dichos lineamientos el Instituto estableció parámetros y, en su caso, índices de calidad que resulten en una mejor calidad del servicio para los usuarios, de acuerdo con las recomendaciones de la UIT, las mejores prácticas internacionales y el despliegue y la evolución tecnológica de las redes del servicio móvil en el país (IFTd, 2018). Además, con lo anterior, el Instituto

[78] Instrumento automatizado capaz de llevar a cabo las pruebas y el procesamiento de la información necesaria para efectos de realizar la medición de los parámetros de calidad del servicio de acceso a internet previstos en los lineamientos.

consideró una amplia difusión de los resultados de las mediciones de calidad con el fin de fomentar la competencia y empoderar al usuario reduciendo las asimetrías en la información.

Aspectos generales de los Lineamientos de calidad del SAI[79] móvil

Sujetos obligados
Concesionarios que presten el servicio móvil[80]
Parámetros de Calidad del SAI

I. Proporción de intentos de sesión fallidos FTP. Estimación del grado de falta de accesibilidad del servicio, con base en la determinación del porcentaje de intentos de establecimiento de sesión fallidos bajo el protocolo FTP
II. Tasa de Transmisión de Datos promedio de descarga (*throughput*). Cantidad promedio de datos descargada por segundo desde el servidor de pruebas hacia el equipo terminal móvil respecto a la duración de la sesión FTP.
III. Tasa de Transmisión de Datos promedio de carga (*throughput)*. Cantidad promedio de datos cargada por segundo desde el equipo terminal móvil hacia el servidor de pruebas con respecto a la duración de la sesión FTP establecida.
IV. Latencia promedio. Estimación del tiempo promedio de respuesta de un servicio entre dos puntos específicos (origen y destino) de una red evaluado mediante la diferencia del tiempo de envío hacia el punto destino y el punto de recepción en el punto origen de un Paquete de datos a través del ICMP.
V. Proporción de paquetes perdidos. Estimación del grado de fiabilidad del Servicio de Transferencia de Datos, con base en la determinación de la proporción de paquetes de datos perdidos con respecto al total de paquetes de datos enviados durante la descarga.

[79] Si bien en los Lineamientos no se hace referencia al Servicio de Acceso a Internet de forma explícita, sí se hace referencia al Servicio de Transferencia de Datos como el servicio de telecomunicaciones que permite el intercambio de información dentro una red pública de telecomunicaciones a través del protocolo IP.

[80] Entendiendo el servicio móvil como el servicio de telecomunicaciones prestado a usuarios finales, que se brinda a través de Equipos Terminales Móviles que no tienen una ubicación geográfica determinada.

Carácter de los Parámetros de Calidad

V. Proporción de intentos de sesión fallidos FTP- **informativo**
VI. Tasa de Transmisión de Datos Promedio de descarga- **informativo**
VII. Tasa de Transmisión de Datos promedio de carga- **informativo**
VIII. Latencia- **informativo**
IX. Proporción de Paquetes Perdidos- **informativo**

En el caso de estos lineamientos no se definen índices de calidad respecto de los parámetros.

Algunas obligaciones

Los PSI deben poner a disposición del usuario final información acerca de los mapas de cobertura garantizada, así como los mapas de cobertura diferenciada para cada tecnología, de manera desagregada.

La velocidad de transferencia de datos publicitada deberá corresponder a la Tasa de Transmisión de Datos promedio de descarga de la hora cargada pico, expresada en Mbps, para cada tecnología de acceso.

Los PSI deberán informar a sus usuarios finales el medio para consultar en sus centros de atención y/o en su portal de Internet, los mapas de cobertura garantizada para cada tecnología de acceso, así como los mapas de cobertura diferenciada.

Los PSI deberán contar con un sistema de atención a usuarios finales en sus centros de atención, así como vía telefónica y/o vía electrónica (chat o correo electrónico) para atender de manera gratuita consultas y quejas relativas al servicio móvil, así como el seguimiento a estas.

Medición de los Parámetros de Calidad del SAI móvil

Para realizar las mediciones y, eventualmente, evaluar el cumplimiento, se diseñó una metodología basada en un muestreo estadístico con el objetivo de obtener una muestra representativo que permita inferir el comportamiento de las redes a nivel nacional. Dicha metodología establece un modelo estadístico compuesto de dos etapas, la primera, se utiliza un muestreo aleatorio estratificado mediante el cual se dividen las entidades federativas para después seleccionar el número de ubicaciones geográficas donde se llevarán a cabo las medicines. La segunda etapa, hace

uso de un muestreo aleatorio simple para determina el tamaño de la muestra de eventos a efectuar en cada entidad federativa. Adicionalmente, se establecen las características técnicas de los equipos de medición y las características de la evaluación.

V3 Plataforma "Soy Usuario"

Soy Usuario[81] es un medio de pre-conciliación a través del cual los usuarios de servicios de telecomunicaciones pueden ingresar una inconformidad para tener un trato directo con su prestador de servicios. La finalidad de esta herramienta es contar con un medio rápido y eficiente en la resolución de las problemáticas que enfrentan los usuarios, ya que todo el proceso se realiza a través de Internet. (IFT, 2021)

La herramienta, de acuerdo con lo señalado por la Coordinación General de Política del Usuario, es resultado del Convenio de Colaboración suscrito entre el IFT y la Procuraduría Federal del Consumidor (PROFECO) en el año 2014, y renovado el 20 de septiembre de 2016, el cual tiene como objetivos establecer las bases de colaboración, coordinación y concertación, dentro del ámbito de sus respectivas atribuciones; establecer líneas de trabajo conjunto y realizar acciones para asegurar la protección de los derechos e interés de los consumidores como usuarios de los servicios de telecomunicaciones; y fomentar el intercambio de información que facilite el cumplimiento eficaz de las acciones que, en el ámbito de sus atribuciones y competencias, les corresponda realizar. (IFT, 2021)

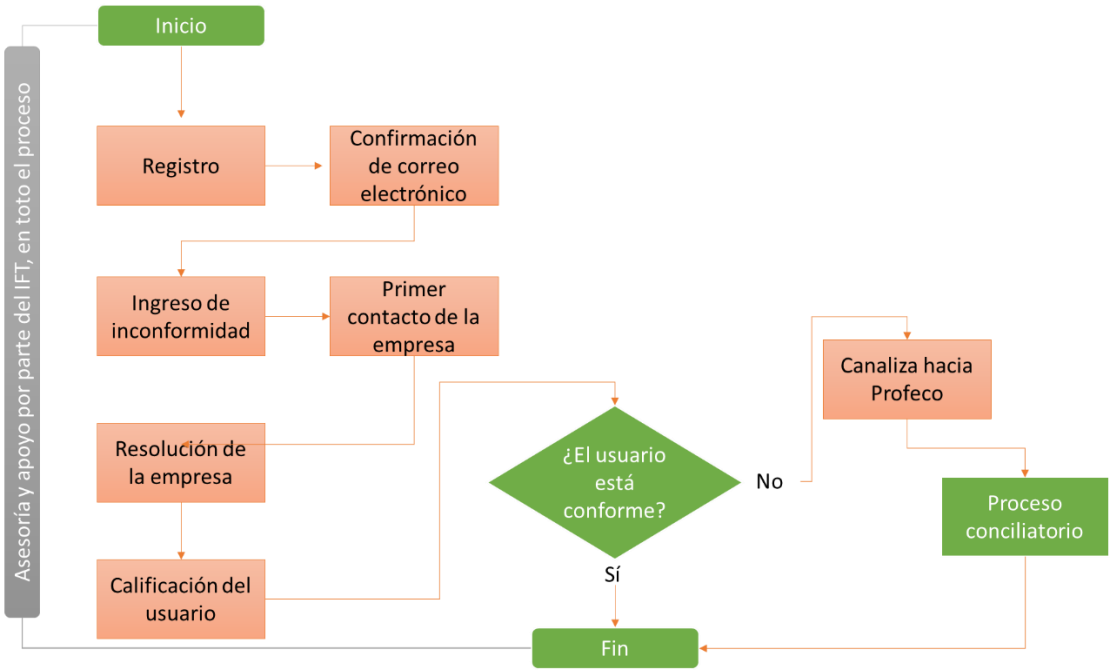
Uno de los elementos más relevantes de dicha plataforma es que si el interesado no queda satisfecho con la atención brindad por el operador, puede solicitar la formalización del procedimiento conciliatorio ante la PROFECO.

PROFECO, por su parte cuenta con dos medios de atención, a saber: la vía electrónica a través de la plataforma electrónica Concilianet, si es que el proveedor cuenta con convenio para el uso de este tipo de medios; o bien, de manera presencial en cualquier de sus Oficinas de Defensa del Consumidor (ODECO) ubicadas al interior de la República Mexicana. (IFTg, 2022). Una vez presentada la queja (por cualquiera de las dos opciones), los consumidores pueden solicitar que el procedimiento conciliatorio sea desahogado a través de un Acuerdo Telefónico Inmediato; en el caso de que el proveedor cuente con convenio para tal procedimiento. Dicho procedimiento consiste en realizar un enlace telefónico con el proveedor de servicios de telecomunicaciones, a través de un conciliador de la PROFECO quien da fe de las manifestaciones, y en caso de llegar a un acuerdo, este será formalizado mediante un convenio en el que se plasma la obligación contraída por el operador. (IFT, 2021)

[81] La plataforma obtuvo un reconocimiento de Buenas Prácticas 2016 por parte del Foro Latinoamérica de entes Reguladores de Telecomunicaciones (regulatel), además del premio WSIS Champion otorgado por la UIT en el marco del Foro de la Cumbre Mundial sobre la Sociedad de la Información 2017.

El proceso general de atención a inconformidades en el sistema "Soy Usuario" se describe en el siguiente diagrama:

Ilustración 20 Proceso general de atención a inconformidades en el sistema Soy Usuario[82]



Cabe destacar que el IFT, a través de la Coordinación General de Política del Usuario, otorga asesoría y seguimiento a las y los usuarios sobre las problemáticas presentadas en la plataforma "Soy Usuario" y funge como vínculo entre los proveedores y los interesados a fin de verificar la atención que recibe cada una de las inconformidades. Particularmente, en los temas relacionados con portabilidad numérica, la Coordinación General de Política del Usuario (CGPU) da seguimiento puntual hasta su correcta conclusión. A través del seguimiento y administración de la plataforma, el IFT obtiene insumos para monitorear la calidad general de los servicios[83]. (IFTg, 2022)

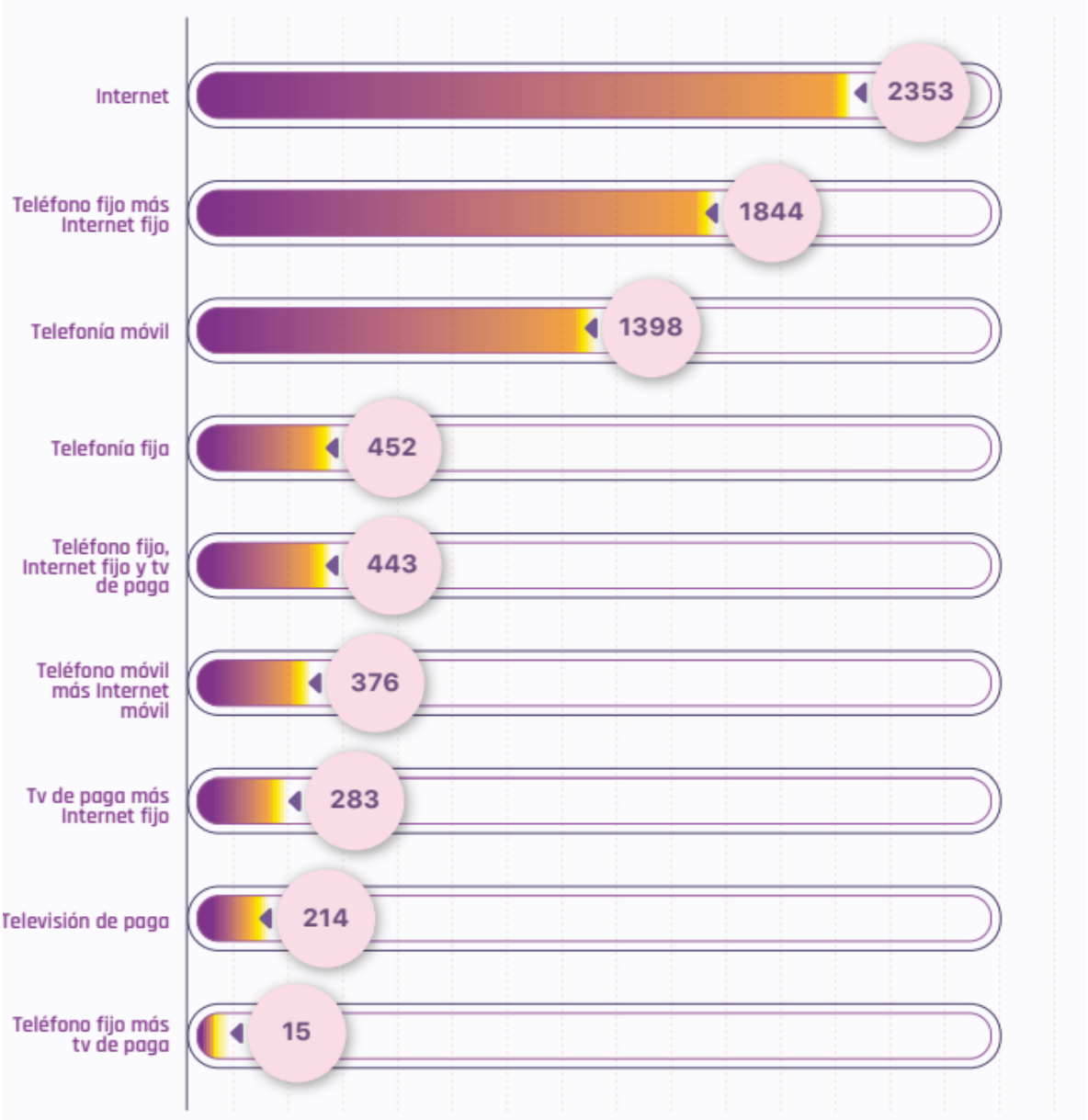
Al respecto, el IFT emite reportes trimestrales. Particularmente, el informe del 4T del 2021 señala que en 2021 más de 28 mil usuarios utilizaron la plataforma "Soy Usuario" como medio de preconciliación. Del total de inconformidades registradas en el periodo octubre a diciembre de 2021, se resolvieron 6 mil 133, 474 se encontraban en proceso, 621 fueron canceladas por duplicidad o por los propios usuarios y 149 se desecharon por falta de seguimiento de los interesados. (IFTg, 2022)

[82] (IFT, 2021)

[83] Comunicado disponible en: http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/en-2021-mas-de-28-mil-usuarios-utilizaron-la-plataforma-soy-usuario-como-medio-de-reconciliacion

Asimismo, el informe de referencia advierte que, por tipo de servicio, el de Internet fue el más recurrido, seguido de la combinación teléfono e internet fijos, tal y como se muestra en la siguiente gráfica.

Ilustración 21 Inconformidades por tipo de servicio[84]



[84] (IFT, 2021)

V4 Conoce tu Velocidad

Otra de las herramientas con las que cuenta el Instituto respecto del monitoreo de la calidad del servicio de acceso a Internet es la herramienta "Conoce tu velocidad", la cual fue presentada en febrero de 2021, como parte de las acciones del IFT en favor de los usuarios. Dicha herramienta permite saber las características de velocidad de carga, descarga, la latencia y la variación que, en ocasiones, presentan los servicios de acceso a Internet controlados.

Uno de los principales objetivos de "Conoce tu Velocidad" refiere a la posibilidad de que los usuarios conozcan, en un lenguaje sencillo, cuál podría ser su experiencia la navegar en Internet, jugar en línea, realizar llamadas por Internet, video conferencias o reproducción de videos; por lo que dichos usuarios podrán reconocer si sus servicios de telecomunicaciones se ajustan a sus necesidades.

Es de mencionar que la herramienta incluye consejos para mejorar la conexión, así como acceso a la Plataforma "Soy Usuario" y que los resultados mostrados por esta herramienta son de carácter informativo y tienen como única finalidad reflejar la calidad de la experiencia de los usuarios del servicio de acceso a Internet fijo. (IFT, 2021)

Ilustración 22 Captura de pantalla de la herramienta "Conoce tu Velocidad"[85]

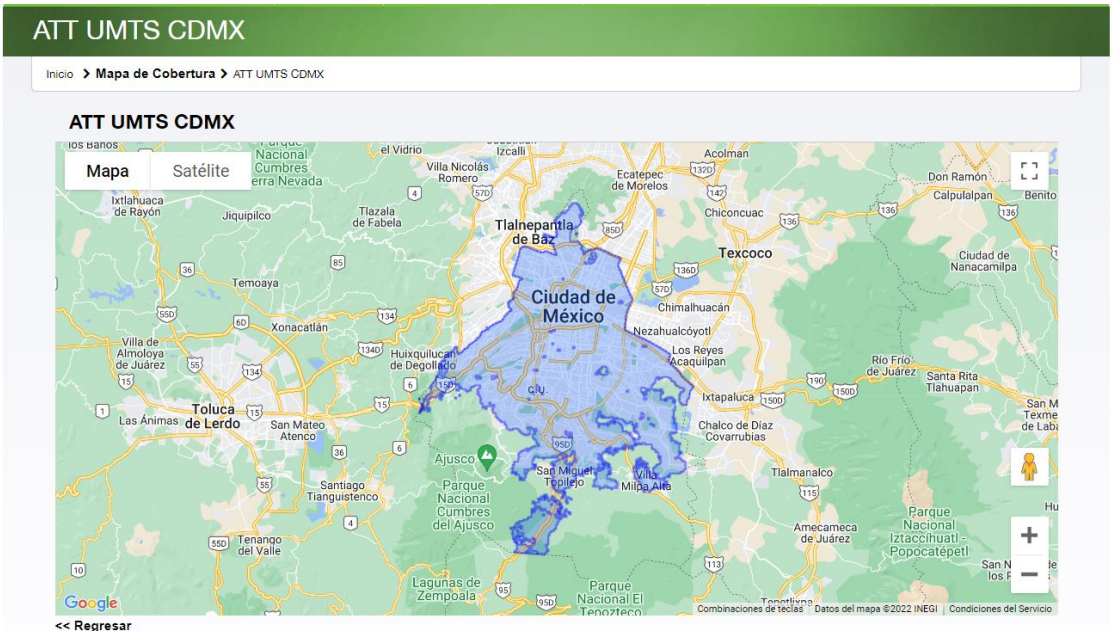
[85] (IFT, 2021)

V5 Mapas de cobertura

En el portal de Internet del IFT, específicamente, en la sección "Usuarios y Audiencias", se encuentran los "Mapas de Cobertura Garantizada[86] Móvil", dichos mapas, de acuerdo con los Lineamientos de calidad del SAI móvil constituyen una representación geográfica del área en la que los prestadores del servicio móvil ofrecen servicios móviles, entre estos el SAI, correspondientes a cierta tecnología de acceso, en donde señalan que cumplen con todos los Índices de Calidad establecidos en los referidos lineamientos.

Los mapas de cobertura garantizada pueden ser consultados por los usuarios finales, por operador móvil (AT&T, UNEFON, Movistar y Telcel), por Estado de la República Mexicana y por tecnología (3G y 4G).

Ilustración 23 Mapas de cobertura móvil garantizada[87]



[86] De acuerdo con información del micrositio "Mapas de Cobertura", se señala que dentro de la Cobertura Garantizada pueden presentarse condiciones que afecten el servicio, debido a las características técnicas y al estado de conservación del equipo móvil del usuario o a su uso en el interior de algunos edificios, sitios subterráneos, elevadores, helicópteros, o en lugares que presenten una concentración inusual de usuarios.

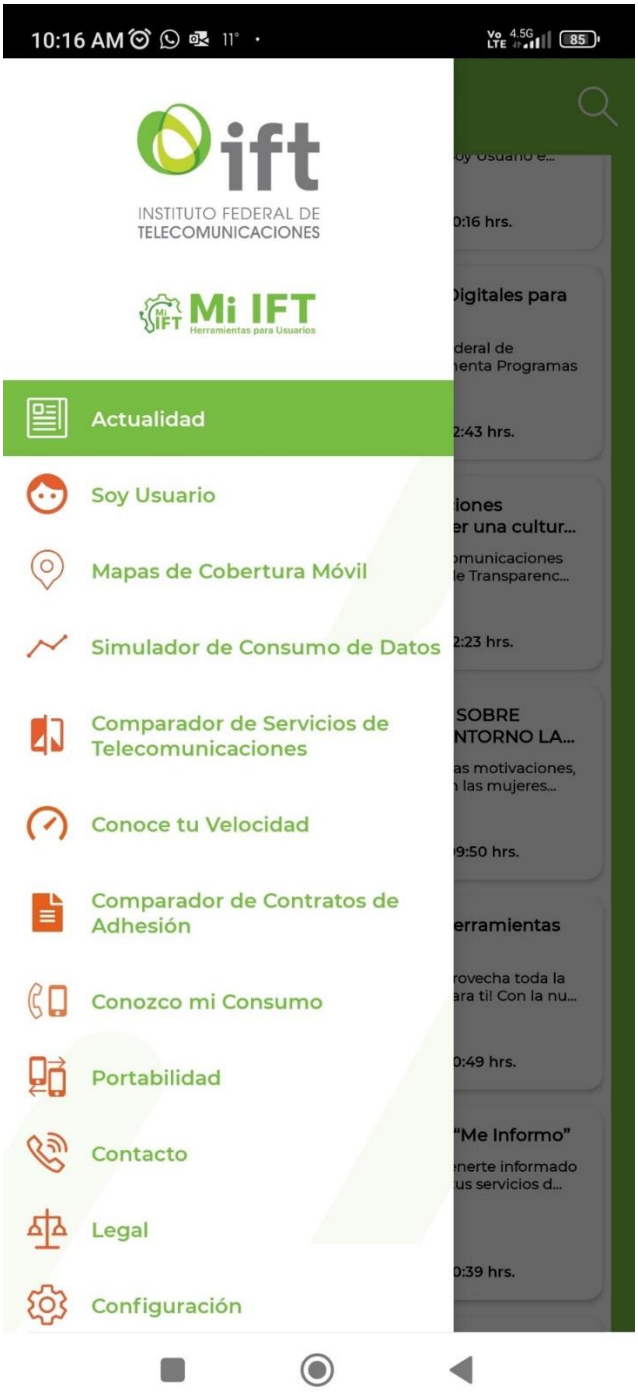
[87] La captura de pantalla corresponde al operador móvil AT&T en la Ciudad de México para la Tecnología 3G. La consulta se realizó el 20 de junio de 2022. Disponible en: http://www.ift.org.mx/mapa-de-cobertura/iusacell-hspa-cdmx

Es preciso señalar que hoy en día el IFT cuenta con un catálogo de herramientas adicionales a las descritas en la presente sección, entre estas: “Conozco mi Consumo”, “Comparador de Contratos”, “Catálogo de Equipos Homologados”, “Catálogo de Dispositivos Móviles Accesibles” y “Comparador de Tarifas”, las cuales permiten a los usuarios finales acceder a información transparente y sencilla, con el objetivo de que cuenten con mayores elementos que les permitan tomar decisiones informadas, y puedan ejercer sus derechos, como la libre elección, que si bien están orientadas a empoderar a los usuarios en cada una de las fases de la relación de consumo de los servicios de telecomunicaciones, en la presente investigación solo se han considerado aquellas que se asocian de manera directa con los mecanismos que se pudieran implementar por parte del IFT para monitorear el cumplimiento de la neutralidad de la red a través de los parámetros asociados con la calidad del servicio de acceso a internet fijo y móvil.

Adicionalmente, en junio de 2021, el Instituto presentó, a través de la CGPU, la Aplicación Móvil “Mi IFT: Herramientas para Usuarios”, dicha aplicación se suma a los esfuerzos que el IFT realiza para garantizar los derechos de los usuarios de los servicios de telecomunicaciones. La aplicación se encuentra disponible para usuarios de Android y iOS.

Mi IFT integra algunas de las herramientas antes descritas y, con ello, posibilita a los usuarios finales el uso de diversas herramientas, tales como: “Soy Usuario”, “Mapas de Cobertura Móvil”, “Simulador de Consumo de Datos”, “Comparador de Servicios de Telecomunicaciones”, “Conoce tu Velocidad”, “Comparador de Contratos de Adhesión”, “Conozco mi Consumo”, “Portabilidad”, así como temas de actualidad, cursos, estudios y otros elementos de carácter informativo.

Ilustración 24 Mi IFT[88]



[88] (Mi IFT, 2022)

VI. Conclusiones y Recomendaciones

La neutralidad de la red es un tema complejo y controversial, pero fundamental para la existencia de un "Internet abierto", en el que se garantice el derecho de los usuarios finales de acceder libremente a cualquier contenido, aplicación o servicio disponible en Internet, además de que se favorezca el desarrollo sostenible de la infraestructura de telecomunicaciones como motor de innovación del ecosistema digital.

Como se describió a lo largo de esta investigación, existen diversos sistemas normativos en torno al principio de neutralidad de la red. Sin embargo, se advierten, al menos, cuatro elementos considerados como constantes en dichos sistemas, a saber:

1. Existe la necesidad de gestionar el tráfico cursado por Internet, toda vez que las redes de telecomunicaciones disponen de recursos finitos y para asegurar la calidad del servicio contratada por los usuarios finales, es necesario gestionar dichos recursos;
2. En la aplicación de la gestión de tráfico y las prácticas comerciales asociadas a ello, los PSI deben garantizar el derecho de los usuarios a acceder libremente a cualquier contenido, aplicación o servicio disponible en Internet;
3. Es prioritaria la existencia de obligaciones de transparencia de cara al usuario final, respecto de la aplicación de gestión de tráfico;
4. El monitoreo de los parámetros de QoS del servicio de acceso a Internet puede ser empleado por los reguladores como una herramienta para monitorear el cumplimiento del sistema normativo respecto del principio de neutralidad de la red.

Ahora bien, desde el punto de vista de esta investigadora, 3 de los 4 elementos listados, forman parte del sistema normativo establecido por el Instituto respecto de la neutralidad de la red. Mientras que el monitoreo del cumplimiento del principio de neutralidad de la red, desde el aspecto técnico, es en este momento un área de oportunidad para el Instituto.

No obstante, se ha dado cuenta de la existencia de diversos mecanismos regulatorios creados por el Instituto en diferentes momentos y para atención de objetivos regulatorios relacionados con la calidad de los servicios de telecomunicaciones, entre estos, el servicio de acceso a Internet, que podrían ser empleados por el regulador para monitorear el cumplimiento del principio de la neutralidad de la red, en cuanto a la gestión de tráfico se refiere. Lo anterior, encuentra fundamento en que los parámetros definidos por el Instituto en los instrumentos como los Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores de los servicios fijo y móvil, tales como, el ancho de banda, *delay, packet loss rate, throughput* y *jitter*, corresponden a los parámetros definidos por la ETSI y son los recomendados por BEREC para las mediciones de la QoS en el marco de la neutralidad de la red. Y no solo eso, sino que la detección de una acción contraria al principio de neutralidad se basa en las mediciones de dichos parámetros, toda vez que su variación

puede indicar la presencia de técnicas de gestión de tráfico y estas pueden ser positivas si mejoran la calidad del SAI, o negativas si, por el contrario, degradan la calidad de dicho servicio.

Adicionalmente, las metodologías previstas por el Instituto para la medición de los parámetros e índices de calidad del SAI fijo y móvil son metodologías que cumplen con los criterios de la OCDE en relación con la Guía para el Cumplimiento Regulatorio y las Inspecciones, en tanto que fomentan el cumplimiento basado en evidencia, tienen un enfoque de riesgos y promueven la integración de la información y una gobernanza transparente.

En este contexto, es importante precisar que la identificación de la aplicación de la gestión de tráfico a través de los parámetros de calidad del servicio, *per se* no constituiría un elemento contrario a los Lineamientos de NN, puesto que en dichos lineamientos se contempla la posibilidad de gestionar el tráfico de Internet, particularmente atendiendo a los siguientes objetivos:

A. Asegurar la calidad, capacidad y velocidad del servicio de acceso a Internet contratado por los usuarios finales, y
B. Preservar la integridad y seguridad de la red.

En consecuencia, el Instituto, a través del monitoreo de los parámetros de QoS del SAI fijo y móvil podría inferir la aplicación de técnicas de gestión de tráfico y, a partir de ello, determinar si dicha gestión se encuentra en línea o no con los Lineamientos de NN.

Por otro lado, como se ha mostrado a lo largo del presente estudio, existe una marcada tendencia por parte de los reguladores internacionales en cuanto al empoderamiento de los usuarios finales respecto de las garantías y mecanismos para asegurar que los PSI además de cumplir con la calidad del servicio contratado, aseguren que dichos usuarios pueden acceder libremente a cualquier contenido, aplicación y/o servicio disponible en Internet. Tales mecanismos van desde procedimientos de atención de quejas y micrositios en los que se informan a los usuarios sobre sus derechos, hasta plataformas complejas para medir las velocidades de subida y bajada del servicio de acceso a Internet de forma individual y colaborativa y se despliegan los resultados a través de mapas de cobertura. Todo lo anterior, acompañado, por ejemplo, en el caso de Alemania, de un protocolo de medición e indicadores de calidad para diversos parámetros.

Al respecto, también se ha hecho evidente que el Instituto no ha sido ajeno a tal tendencia, sino que por lo contrario ha desarrollado diversas herramientas, tales como: “Soy Usuario”, “Conoce tu Velocidad”, “Mapas de Cobertura” y “Mi IFT” que fueron creadas con el objetivo de que los usuarios cuenten con mayores elementos que les permitan tomar decisiones informadas y que puedan ejercer sus derechos, como el de la libre elección y, que a consideración de esta investigadora, podrían ser empleados por el regulador para empoderar/informar a los usuarios del SAI en relación con el principio de neutralidad de la red. Las herramientas antes mencionadas, entre otras cosas,

constituyen una forma de monitoreo de la calidad de los servicios de telecomunicaciones, así como un medio de atención de quejas por parte de los usuarios finales técnicamente válida.

Por otro lado, también se ha hecho notar la existencia de mecanismos/algoritmos creados específicamente para inferir la diferenciación de tráfico aplicada por cierto PSI. Pero, mientras los mecanismos basados en la QoS tienen amplias aplicaciones, los de detección de diferenciación de tráfico son reducidos en cuanto a que la mayoría de estos están limitados a ambientes de prueba.

No resulta óbice señalar que si bien podría ser sumamente factible que el Instituto empleara los mecanismos antes sugeridos. Lo anterior, tendría que ser formalizado por el propio Instituto a través del Acuerdo de Pleno que al efecto se estimara pertinente.

VII. Bibliografía

3CX, 2022. *3CX.* [En línea]
Available at: https://www.3cx.es/voip-sip/sip/
[Último acceso: 06 06 2022].

Agencia Federal de Redes, 2021. *Breitbandmessung.* [En línea]
Available at: https://www.breitbandmessung.de/
[Último acceso: 05 05 2022].

America, G. L., 2013. *GSM.* [En línea]
Available at: https://www.gsma.com/latinamerica/wp-content/uploads/2013/04/qos-spa.pdf

Anon., 2021. *CRTC.* [En línea]
Available at: https://crtc.gc.ca/eng/internet/traf.htm

Anon., 2022. *ITU.* [En línea]
Available at: (https://www.itu.int/br_tsb_terms/#?q=QoS&sector=T,R&from=2002-04-13&to=2022-04-13&status=Recommended&page=1

ARCEP, 2017. *J'alert a l'Arcep.* [En línea]
Available at: https://jalerte.arcep.fr/
[Último acceso: 12 06 2022].

ARCEP, 2018. *arcep.fr.* [En línea]
Available at: https://en.arcep.fr/news/press-releases/view/n/net-neutrality.html
[Último acceso: 01 05 2022].

ARCEP, 2021. *Bilan annuel de la plateforme « J'alerte l'Arcep » : enseignements et actions du régulateur dans un contexte de crise sanitaire,* Paris: Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse.

ARCEP, 2021. *arcep Las redes como bien común.* [En línea]
Available at: https://www.arcep.fr/la-regulation/grands-dossiers-internet-et-numerique/la-neutralite-de-linternet/la-boite-a-outils-de-larcep.html
[Último acceso: 01 06 2022].

ARCEP, 2021. *L'état d'Internet en France,* Paris, Francia: ARCEP.

ARCEP, 2021. *www.arcep.fr.* [En línea]
Available at: https://www.arcep.fr/actualites/les-communiques-de-presse/detail/n/internet-ouvert-211220.html
[Último acceso: 06 06 2022].

Banco Mundial, 2022. *Banco Mundial.* [En línea]
Available at: https://datos.bancomundial.org/indicador/IT.NET.USER.ZS
[Último acceso: 1 mayo 2022].

BEREC, 2011. *Guidelines on transparency in the scope of net neutrality: best practices and recommended approaches.,* s.l.: s.n.

BEREC, 2014. *Monitoring of Internet access services in the context of net neutrality,* s.l.: s.n.

BEREC, 2015. [En línea]
Available at: https://berec.europa.eu/eng/open_internet/specialised_services/

BEREC, 2018. *BEREC opinion for the evaluation of the application of Regulation EU and the BEREC Net Neutrality Guidelines.* [En línea]
Available at:
https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/8317-berec-opinion-for-the-evaluation-of-the-application-of-regulation-eu-20152120-and-the-berec-net-neutrality-guidelines

Black, J., Hopper, M. & Band, C., 2007. Making a success of Principles-based regulation. *Law and Financial Markets Review,* Mayo.pp. 191-206.

Brown, C. S. a. C., 2010. *Regulatory Capacity and Networked Governance.* [En línea]
Available at:
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1043.7799&rep=rep1&type=pdf#:~:text=Regulatory%20capacity%2C%20then%2C%20is%20the,state%20and%20non%2Dstate%20actors.

Bundesnetzagentur, 2021. *Net Neutrality in Germany,* s.l.: s.n.

Bundesnetzagentur, 2021. *Net Neutrality in Germany. Annual Report 2020/2021,* s.l.: s.n.

Callo-Müller, M. V., 2020. *Micro, Small and Medium enterprises and the Digital Economy,* s.l.: s.n.

CCTS, 2022. *Comisión de Quejas de las Telecomunicaciones y Televisión.* [En línea]
Available at: https://www.ccts-cprst.ca/for-consumers/complaints/complaint-form/
[Último acceso: 27 04 2022].

CCTS, 2022. *For consumers.* [En línea]
Available at: https://www.ccts-cprst.ca/for-consumers/complaints/complaint-form/
[Último acceso: 14 Junio 2022].

Cervera, J., 2014. *Qué es la neutralidad de la red y por qué es tan importante.* [En línea]
Available at: https://gestion.pe/tecnologia/neutralidad-red-importante-64393-noticia/?ref=gesr

Chile, M. d. T. y. T., 2010. *Bibliote del Congreso Nacional de Chile.* [En línea]
Available at: https://www.bcn.cl/leychile/navegar?idNorma=1016570%26idVersion%3D2010-08-26

Chile, M. d. T. y. T., 2011. *Biblioteca del Congreso Nacional de Chile.* [En línea]
Available at:
https://www.bcn.cl/leychile/consulta/vinculaciones/reglamento?idNorma=1016570&fechaVigencia=2010-08-26&clase_vinculacion=REGLAMENTO

CISCO, 2018. *The Cisco Learning Network.* [En línea]
Available at: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKCaEAO/analizando-los-modelos-de-calidad-de-servicio

CISCO, s.f. *México, Cisco VNI 2014-2022,* s.l.: s.n.

Clark, D. D. & Braman, S., 2018. *The Basics of the Internet.* s.l.:MIT Press.

Colombia, C., 2021. *Estudio del Estado de la Neutralidad de la Red en Colombia,* s.l.: s.n.

CRTC, 2009. *Telecom Regulatory Policy CRTC 2009-657,* s.l.: s.n.

CRTC, 2017. *Política regulatoria de telecomunicaciones CRTC 2017-104,* s.l.: s.n.

CRTC, Enero-Marzo 2022. *Status Report-Complaints Related to Internet Traffic Management Practices (ITMPs).* [En línea]
Available at: https://crtc.gc.ca/eng/internet/pub.htm
[Último acceso: 14 Junio 2022].

Cullen, 2022. *US federal court upholds validity of California state net neutrality law,* s.l.: s.n.

Decreto 368, 2011. Reglamento que regula las características y condiciones de la neutralidad de la red.

Decreto N° 8771, 2016. Decreto N° 8771 del 11 de mayo de 2016. *Diário Oficial da União*.

Diario Oficial de la Federación, 2013. *"Decreto por el que se reforman y adicionan diversas disposiciones de los artículos 6o., 7o., 27, 28, 73, 78, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos en materia de Telecomunicaciones",* s.l.: s.n.

Díaz, A. P., 2013. *La Agenda Digital en México,* s.l.: ANFECA.

Duó, M., 2021. *Kinsta.* [En línea]
Available at: https://kinsta.com/es/blog/puerto-smtp/
[Último acceso: 06 06 2022].

Espinosa, O., 2022. *Redes Zone.* [En línea]
Available at: https://www.redeszone.net/tutoriales/configuracion-puertos/puertos-tcp-udp/
[Último acceso: 06 06 2022].

Europea, U., 2015. *Official Journal of the European Union.* [En línea]
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=en

Europeo, P., 2015. *Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas relativas al acceso abierto a Internet y se modifica la Directiva 2002/22/CE sobre el servicio universal y los derechos de los usu.* [En línea]
Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015R2120&from=EN

Fangfan Li, A. A. N. D. C. P. G. A. M., 2019. A Large-Scale Analysis of Deployed Traffic Differentiation Practices. *Proceedings of the ACM Special Interest Group on Data Communication*.

FCC, 2015. *Report and order on remand, declaratory ruling, and order,* Washington, D.C.: Federal Communications Commission .

FCC, 2017. *Restoring Internet Freedom,* Washington D. C.: Comisión Federal de Comunicaciones.

García, J. F., 2004. *El crecimiento económico en México y sus detonantes. Un análisis histórico.* s.l.:Hitos de de ciencias económico-administrativas.

Giuseppe Aceto, A. P., 2015. Internet Censorship Detection: a Survey. *Internet Censorship Detection: a Survey*.

Glorioso, J. C. D. M. a. A., 2008. The Neubot Project: A Collaborative Approach To Measuring Internet Neutrality. *IEEE International Symposium on Technology and Society*.

IBM, 2021. *IBM.* [En línea]
Available at: https://www.ibm.com/docs/es/i/7.3?topic=alternatives-l2tp-tunneling-support-ppp-connections
[Último acceso: 06 06 2022].

IFT, Estudio: Neutralidad de Red, 2019. *Estudio: Neutralidad de Red,* Ciudad de México: Instituto Federal de Telecomunicaciones.

IFT, 2021. *Conoce tu Velocidad.* [En línea]
Available at: http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/en-beneficio-de-los-usuarios-el-ift-presenta-la-herramienta-conoce-tu-velocidad-comunicado-142021-25
[Último acceso: 16 Junio 2022].

IFT, 2021. *Informe Estadístico Trianual Soy Usuario,* CDMX: s.n.

IFT, 2021. *Soy Usuario Cuarto informe trimestral 2021,* s.l.: IFT.

IFT, 2022. ACUERDO mediante el cual el Pleno del Instituto Federal de Telecomunicaciones establece los términos y formato relativos al informe que deberán presentar los concesionarios y autorizados que presten el servicio de acceso a Internet. *Diario Oficial de la Federación*, 30 03, p. https://www.dof.gob.mx/nota_detalle.php?codigo=5647351&fecha=30/03/2022#gsc.tab=0.

IFTa, 2021. *Lineamientos para la gestión de tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet.* [En línea]
Available at:
https://www.dof.gob.mx/nota_detalle.php?codigo=5622965&fecha=05/07/2021#gsc.tab=0

IFTb, 2021. *Informe de consideraciones de la Consulta Pública del Anteproyecto de Lineamientos,* s.l.: s.n.

IFTc, 2020. *Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones emite los Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo..* [En línea]
Available at:
http://www.ift.org.mx/sites/default/files/conocenos/pleno/sesiones/acuerdoliga/dof131119647acc.pdf
[Último acceso: 16 Junio 2022].

IFTd, 2018. *IFT.* [En línea]
Available at:

https://www.dof.gob.mx/nota_detalle.php?codigo=5510754&fecha=17/01/2018#gsc.tab=0 [Último acceso: 16 Junio 2022].

IFTg, 2022. *La plataforma Soy Usuario como medio de preconciliación,* s.l.: IFT.

International, C., 2022. *BEREC consults on zero rating and on sustainability in the telecoms sector.* [En línea]
Available at: https://www.cullen-international.com/client/site/documents/FLTEEP20220007

ITU, 2021. *ITU.* [En línea]
Available at: (https://www.itu.int/br_tsb_terms/#?q=QoS&sector=T,R&from=2002-04-13&to=2022-04-13&status=Recommended&page=1

Ivanti, 2018. *Ivanti.* [En línea]
Available at: https://help.ivanti.com/wl/help/es_ES/AVA/6.2/Avalanche/Appendices/ports.htm [Último acceso: 06 06 2022].

J. Saltzer, D. R. a. D. C., 1984. *End-to-end Arguments in System Design.* s.l.:s.n.

Koukoutsidis, I., 2015. Public QoS and Net Neutrality Measurements: Current Status and Challenges Toward Exploitable Resultas. *Journal of Inofrmation Policy,* Volumen 5, pp. 245-286.

Lessig, M. y., 2006. No hay peajes en Internet. *Washington Post*.

Ley 20453, 2010. *Consagra el principio de neutralidad en la red para los consumidores y usuarios de Internet,* s.l.: s.n.

Ley 27.078, 2014. *Ley Argentina Digital,* s.l.: s.n.

Ley 5050, 2011. *Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014,* s.l.: Diario Oficial .

Ley N° 12.965, 2014. *Marco Civil da Internet,* s.l.: s.n.

Ley N° 12.965, 2014. *Marco Civil de Internet,* Brasilia: Diário Oficial da União.

Ley Orgánica de Telecomunicaciones, 2015. s.l.: Registro Oficial.

Ley. 21.046, 2017. *Ley que establece la obligación de una velocidad mínima garantizada de acceso a Internet,* Santiago de Chile: s.n.

LFTR, 2014. *Ley Federal de Telecomunicaciones y Radiodifución,* s.l.: s.n.

LFTR, 2014. *LFTR.* [En línea]
Available at:
https://www.gob.mx/cms/uploads/attachment/file/346846/LEY_FEDERAL_DE_TELECOMUNICACIONES_Y_RADIODIFUSION.pdf

Limbatto, 2022. *Net Neutrality.* [En línea]
Available at: https://www.cullen-international.com/client/site/documents/CTTELN20210061
[Último acceso: 25 04 2022].

M. Weber, V. S. Z. J. I. G. a. T. Z., 2013. Can HAKOMetar be used to increase transparency in the context of network neutrality?. *Proceedings of the 12th International Conference on Telecommunications*, pp. 309-316.

Mi IFT, 2022. *Mi IFT.* [En línea]
Available at: https://play.google.com/store/apps/details?id=com.ift.comparador&hl=es_MX&gl=US
[Último acceso: 11 06 2022].

MINECO, 2021. *Informe Sobre Supervisión en España de Normativa Europea en Materia de Acceso a una Internet Abierta (Neutralidad de la red) ,* Madrid: Ministerio de Asuntos Económicos y Transformación Digital.

MLab, 2022. *Internet measurement Tests.* [En línea]
Available at: https://www.measurementlab.net/about/
[Último acceso: 2022 06 06].

Mueller, M., Cogburn, D., Mathiason, J. & Hofmann, J., s.f. *Net Neutrality as Global Principle for Internet Governance,* s.l.: s.n.

OCDE(a), 2019. *Implementación del Análisis de Impacto Regulatorio en el Gobierno.* s.l.:s.n.

OCDE, 2019. *Análisis de Impacto Regulatorio en el Ciclo de Gobernanza Regulatoria,* s.l.: s.n.

OCDE, 2019. *Guía de la OCDE para el cumplimiento regulatorio y las inspecciones.* Paris: OCDE.

OCDE, 2020. *OECD Digital Economy Outlook 2020,* Paris: OECD Publishing.

OEA, 2011. *Declaraciones Conjuntas.* [En línea]
Available at: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2

OFCOM, 2017. *Mobile and broadband checker.* [En línea]
Available at: https://checker.ofcom.org.uk/
[Último acceso: 06 15 2022].

OFCOM, 2019. *Ofcom's approach to assessing compliance with net neutrality rules: Frameworks for assessing zero rating offers and traffic management measures for compliance with the Open Internet Regulation,* Londres: OFCOM.

OFCOM, 2021. *Monitoring compliance with the Open Internet Regulation,* Londres: OFCOM.

OFCOM, 2021. *ofcom.com.* [En línea]
Available at: https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/net-neutrality
[Último acceso: 12 06 2022].

OFCOM, 2021. *ofcom.com.* [En línea]
Available at: https://www.ofcom.org.uk/research-and-data/telecoms-research/mobile-smartphones/mobile-matters/maps-2021/4g-uk
[Último acceso: 14 06 2022].

OFCOM, 2021. *UK Home Broadband Performance (Technical Annex),* Londres, Inglaterra: s.n.

OFCOM, 2021. *UK home broadband performance, measurement period March 2021,* Londres, Inglaterra.: OFCOM.

olprod, m. y., 2022. *Microsoft.* [En línea]
Available at: https://docs.microsoft.com/es-es/exchange/um-protocols-ports-and-services-exchange-2013-help
[Último acceso: 06 06 2022].

OPSITEL, 2020. RESOLUCIÓN: N° 0064487-2020-TRASU/OSIPTEL. *El Peruano*, 19 06, p. Art. 28.

OPSITEL, 2021. *osiptel.gob.pe.* [En línea]
Available at: https://www.osiptel.gob.pe/portal-del-usuario/trasu-2da-instancia-apelacion/qu%C3%A9-es-el-trasu/
[Último acceso: 06 06 2022].

OPSITEL, 2022. *Checa tu Internet Móvil.* [En línea]
Available at: https://checatuinternetmovil.osiptel.gob.pe/

OSIPTEL, 2021. N° 00001-2021-TRASU/SP/OSIPTEL. *El Peruano*, 17 08.

Palmer, G., 2021. *Techlandia.* [En línea]
Available at: https://techlandia.com/puerto-81-info_206077/
[Último acceso: 06 06 2022].

QCA, 2018. *Monitoreo y verificación de medidas de control.* [En línea]
Available at: https://qcsolutions.com.ar/monitoreo-y-verificacion-de-medidas-de-control/

Rammneek, y otros, 2017. Emerging network technologies and network neutrality perfomrnace. pp. 31-36.

Reglamento de la Neutralidad de la Red, 2016. s.l.: s.n.

Resolución 5969, 2020. s.l.: Diario Oficial.

S. Floyd and K. Fall, 1999. Promoting the use of end-to-end congestion control in the Internet. *Promoting the use of end-to-end congestion control in the Internet,* pp. 458-472.

Sáez, I. P., 2019. *incibe-cert.* [En línea]
Available at: https://www.incibe-cert.es/blog/protege-tus-peticiones-dns-dns-over-tls
[Último acceso: 06 06 2022].

SB-822, 2018. *Communications: broadband Internet access service,* s.l.: s.n.

SiteGround, 2021. *SiteGround.* [En línea]
Available at: https://es.siteground.com/tutoriales/email/protocolos-pop3-smtp-imap/
[Último acceso: 06 06 2022].

Tapia, A. D. R. & Acosta, C. R. E., 2015. Latencia en las redes celulares, y su influencia en las aplicaciones. *Revisa Tecnológica ESPOL,* pp. 162-178.

TechTarget, 2022. *Computer Weekly.* [En línea]
Available at: https://www.computerweekly.com/es/definicion/Calidad-de-servicio-o-QoS

TechTarget, 2022. *WhatIs.* [En línea]
Available at: https://www.techtarget.com/whatis/search/query?q=QoS

Thiago Garrett, L. E. S. L. M. P. L. C. E. B. E. P. D. J., 2018. Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, 21 04, pp. 17-18.

Thiago Garrett, L. S. L. P. L. B. y. E. D. J., 2022. A survey of Network Neutrality regulations worldwide. *Computer Law and Security Law,* 44(105654), pp. 1-19.

Thiago Garrett, L. S. L. P. L. B. y. E. D. J., 2022. Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, 21 04, pp. 17-18.

UIT, 2005. *Indicadores calbe de las tecnologías de la Información y de las Comunicaciones,* s.l.: s.n.

UIT, 2008. *Rec. UIT-T E.800.* [En línea]
Available at: https://www.itu.int/rec/T-REC-E.800-200809-I/es

UITa, 2017. *Quality of Service. Regulation Manual.* s.l.:s.n.

UITa, 2022. *UIT Terms and Definitions.* [En línea]
Available at:
https://www.itu.int/br_tsb_terms/#?q=undefined&sector=T,R&from=undefined&to=undefined&status=Superseded&page=1

Vitali Bashko, N. M. A. S. J. S., 2013. BonaFide: A Traffic Shaping Detection Tool for Mobile Networks. *Computer Science, Jacobs University Bremen*.

Wu, T., 2003. Network Neutrality, Broadband Discrimination. *Journal of Telecommunications and High Technology Law.*

Wu, T., 2003. Network Neutrality, Broadband Discrimination. *J. on Telecomm. & High Tech,* pp. 141-179.

Xiao, D., Li, H. & Wang, W., 2003. QoS Management Network. *IEEE ICCT2003,* pp. 320-323.

Yiannis Yiakoumis, S. K. a. N. M., 2016. Neutral Net Neutrality. *Proceedings of the 2016 ACM SIGCOMM Conference*, Agosto.

Yiannis Yiakoumis, S. K. a. N. M., 2016. Neutral Net Neutrality. *Proceedings of the 2016 ACM SIGCOMM Conference*, Agosto.

VIII. Anexos

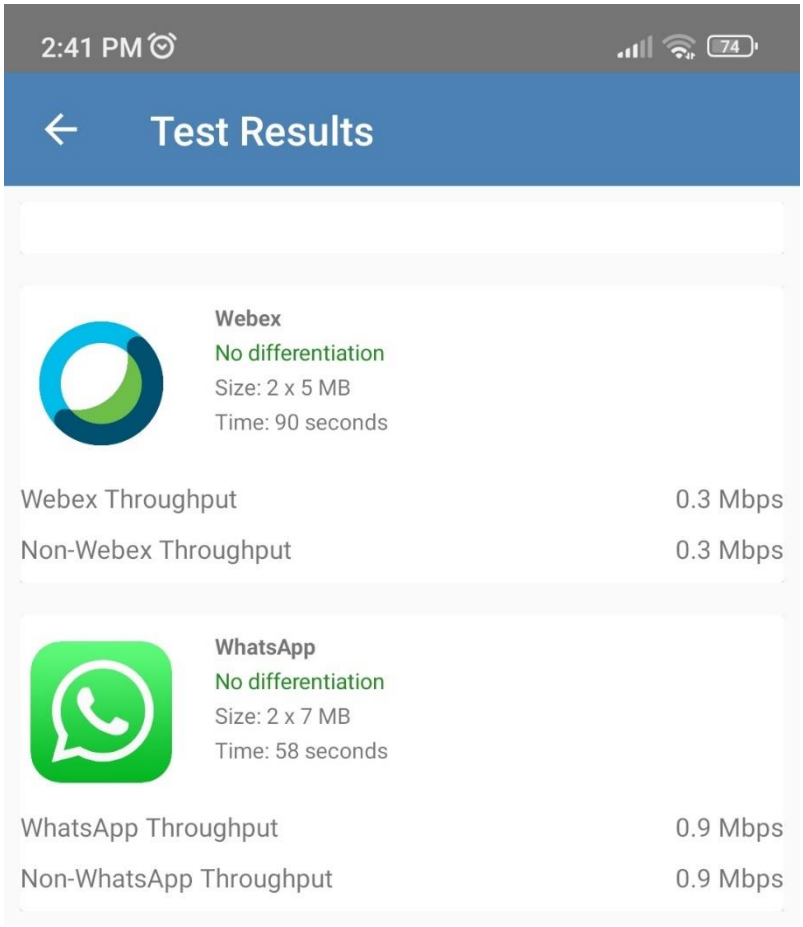
Anexo 1a “Pruebas de detección de diferenciación de tráfico con sistemas IOS y Android”

Dispositivo Android Versión 11, Redmi Note 11S, Red Wifi: operador fijo Totalplay

Aplicaciones de la categoría “conferencing”

- Webex y WhatsApp

Ilustración 1a 1 Detección de diferenciación de tráfico para dos aplicaciones Android 11 Redmi Note 11S



- Webex, WhatsApp, Google Meet, Microsoft Teams, Skype y Zoom.

Ilustración 1a 2 Detección de diferenciación de tráfico para 6 aplicaciones de la categoría "conferencing"

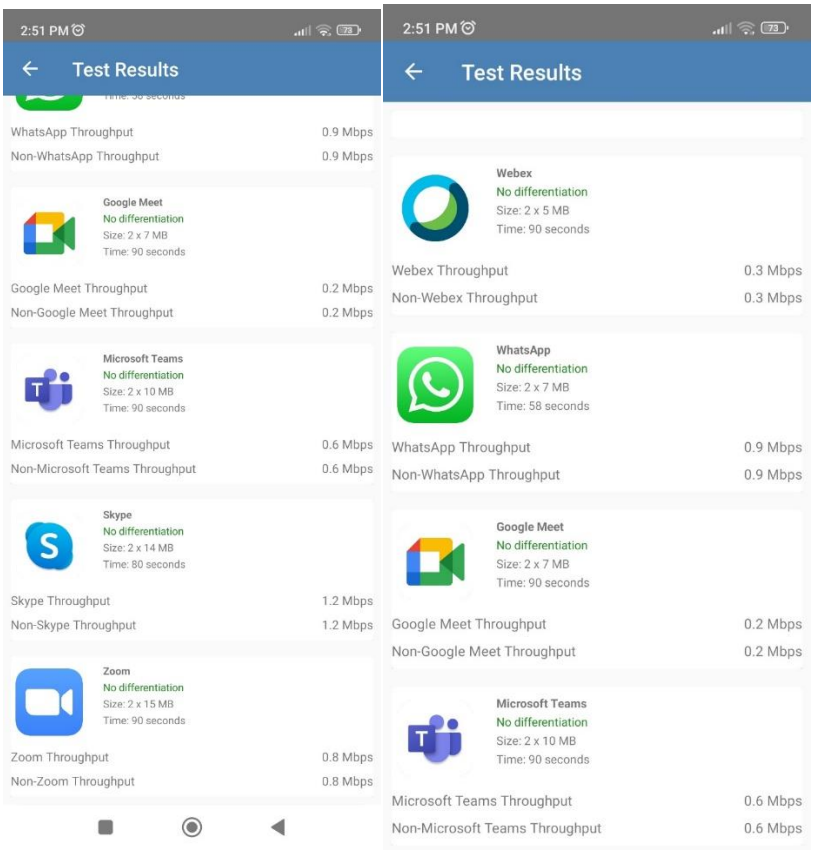
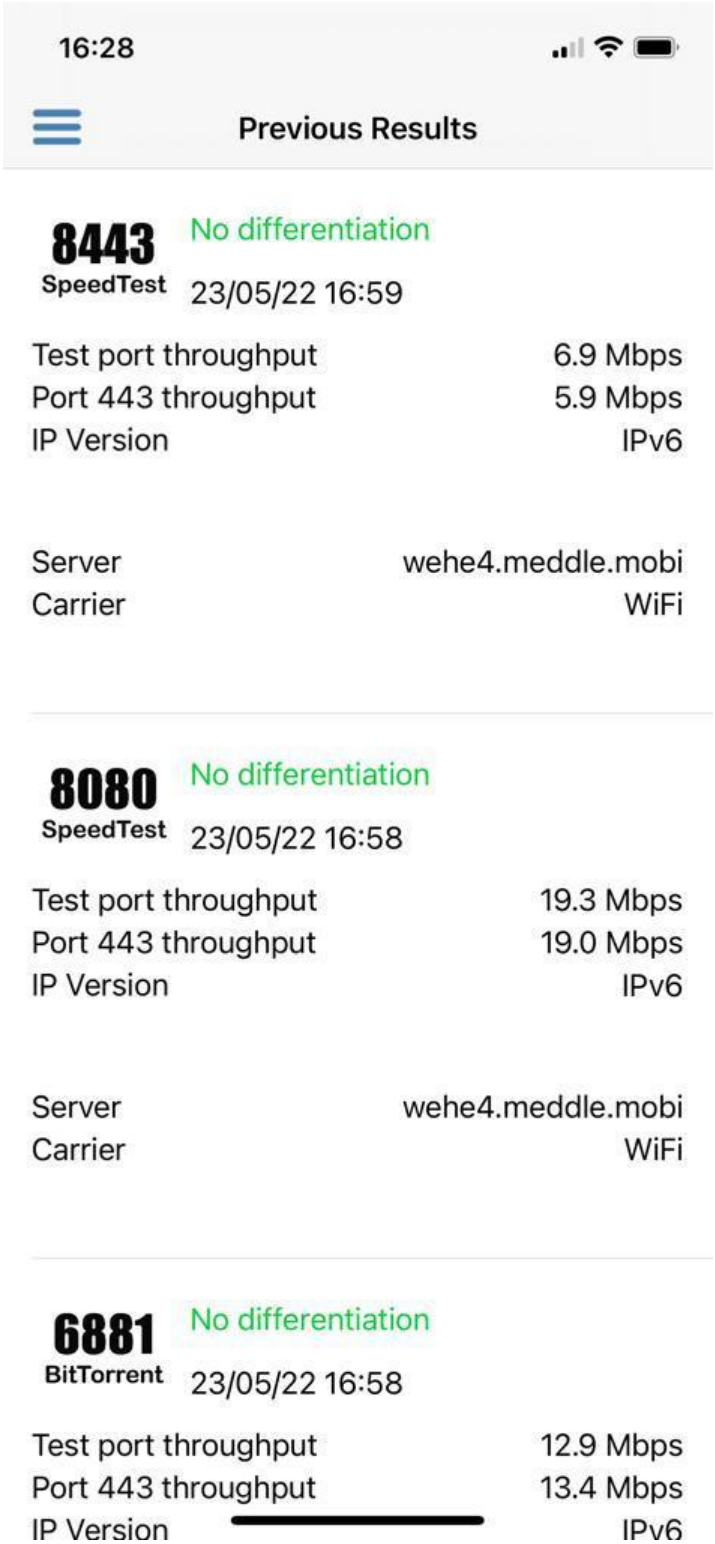
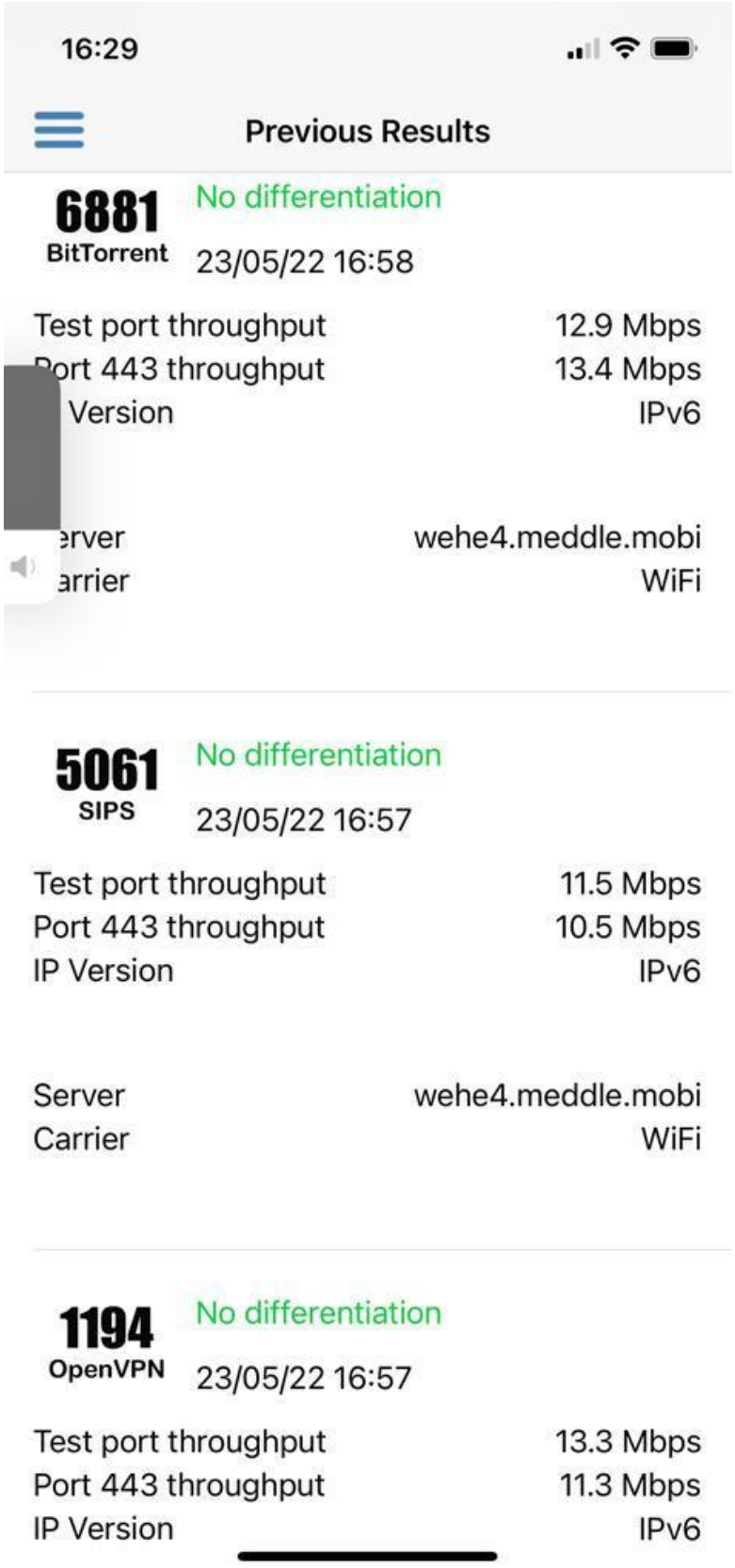
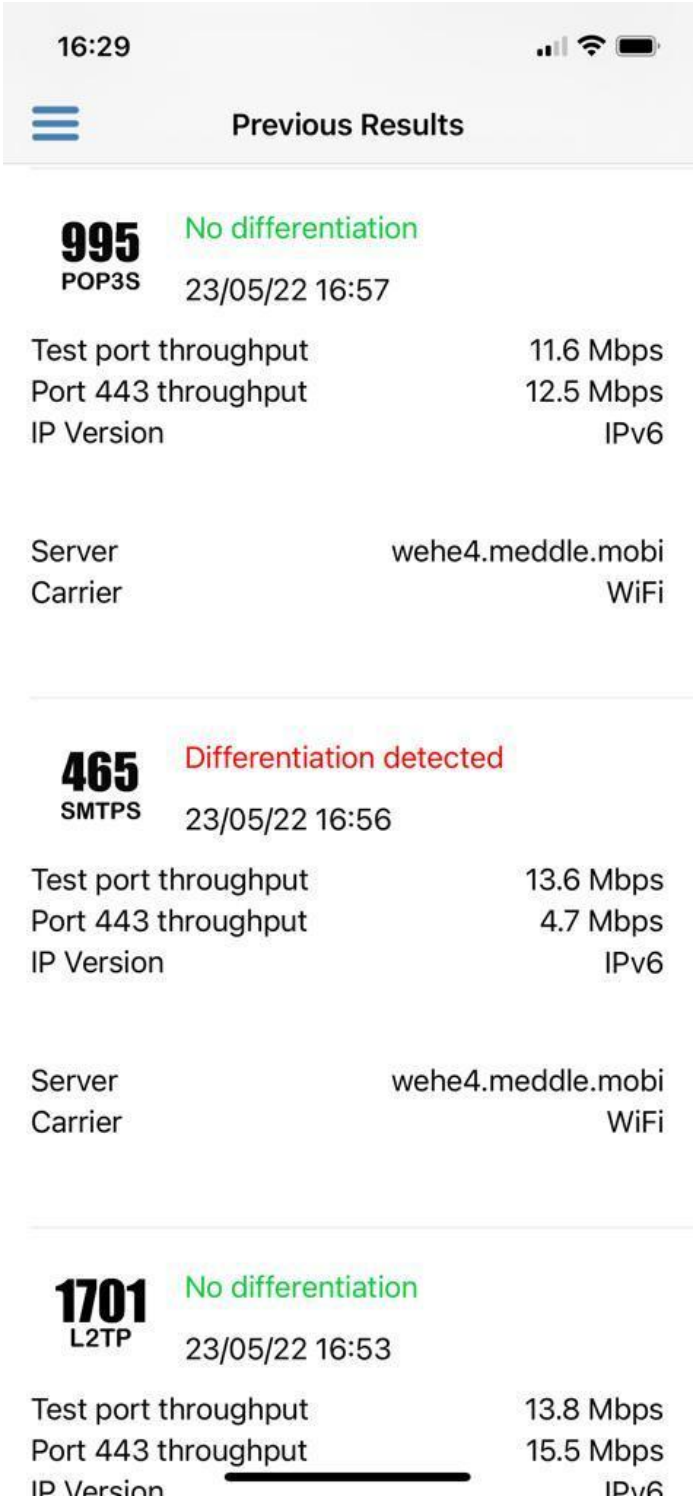


Ilustración 1b 1 Prueba de puertos




16:29
Previous Results
6881
BitTorrent
No differentiation
23/05/22 16:58
Test port throughput 12.9 Mbps
Port 443 throughput 13.4 Mbps
Version IPv6
erver wehe4.meddle.mobi
arrier WiFi
5061
SIPS
No differentiation
23/05/22 16:57
Test port throughput 11.5 Mbps
Port 443 throughput 10.5 Mbps
IP Version IPv6
Server wehe4.meddle.mobi
Carrier WiFi
1194
OpenVPN
No differentiation
23/05/22 16:57
Test port throughput 13.3 Mbps
Port 443 throughput 11.3 Mbps
IP Version IPv6


16:29
Previous Results
995
POP3S
No differentiation
23/05/22 16:57
Test port throughput 11.6 Mbps
Port 443 throughput 12.5 Mbps
IP Version IPv6
Server wehe4.meddle.mobi
Carrier WiFi
465
SMTPS
Differentiation detected
23/05/22 16:56
Test port throughput 13.6 Mbps
Port 443 throughput 4.7 Mbps
IP Version IPv6
Server wehe4.meddle.mobi
Carrier WiFi
1701
L2TP
No differentiation
23/05/22 16:53
Test port throughput 13.8 Mbps
Port 443 throughput 15.5 Mbps

Anexo 1b Tribunal de Justicia de la Unión Europea y las tarifas de *zero rating*

Recientemente el Tribunal de Justicia de la Unión Europea TJUE emitió una decisión respecto de la interpretación del artículo 3, apartados 1 a 3 del Reglamento, en estos términos el artículo de referencia señala lo siguiente:

> "*1. Los usuarios finales tendrán derecho a acceder a la información y contenidos, así como a distribuirlos, usar y suministrar aplicaciones y servicios y utilizar los equipos terminales de su elección, con independencia de la ubicación del usuario final o del proveedor o de la ubicación, origen o destino de la información, contenido, aplicación o servicio, a través de su servicio de acceso a internet.*
>
> *[…]*
>
> *2. Los acuerdos entre los proveedores de servicios de acceso a internet y los usuarios finales sobre condiciones comerciales y técnicas y características de los servicios de acceso a internet como el precio, los volúmenes de datos o la velocidad, así como cualquier práctica comercial puesta en marcha por los proveedores de servicios de acceso a internet, no limitarán el ejercicio de los derechos de los usuarios finales establecidos en el apartado 1.*
>
> *3. Los proveedores de servicios de acceso a internet* **tratarán todo el tráfico de manera equitativa cuando presten servicios de acceso a internet, sin discriminación, restricción o interferencia, e independientemente del emisor y el receptor, el contenido al que se accede o que se distribuye, las aplicaciones o servicios utilizados o prestados***, o el equipo terminal empleado."*
>
> *Énfasis añadido*

Como parte de los elementos que analizó el Tribunal en uno de los tres casos, se señala que Telekom es una empresa que opera en el sector de las tecnologías de la información y de la comunicación. Desde el 19 de abril de 2017, ofrece a los clientes finales, para algunas de sus tarifas, una opción adicional (también denominada «add-option») que consiste en una opción tarifaria gratuita de «zero rating» llamada «Stream On» (que inicialmente existía en las variantes «StreamOn Music», «StreamOn Music Euratom Video», «MagentaEINS StreamOn Music» y «MagentaEINS StreamOn Music&Video»). La activación de esta opción permite no imputar el volumen de datos consumido por el streaming de audio y de vídeo difundido por socios de contenidos de Telekom al volumen de datos incluido en la tarifa básica; una vez que este volumen de datos se agota, ello conlleva generalmente a una reducción de la velocidad de transmisión. Al activar la opción tarifaria «StreamOn», el usuario final acepta una limitación del ancho de banda a una tasa máxima de 1,7 Mbit/s para el streaming de

vídeo, ya se trate de vídeos difundidos por proveedores de contenidos asociados o por otros proveedores.

Sobre el particular, la Bundesnetzagentur mediante resolución de 15 de diciembre de 2017, declaró que la opción tarifaria de que se trata ***no cumplía con las obligaciones derivadas del artículo 3,*** apartado 3, del Reglamento, puesto que iba acompañada de una reducción de la tasa de transmisión de datos para el streaming de vídeo a una velocidad máxima de 1,7 Mbit/s. En consecuencia, la Bundesnetzagentur prohibió a Telekom dos cosas: i) limitar el ancho de banda para el *streaming* de vídeo incluido en dicha opción tarifaria y, ii) utilizar cláusulas que establezcan una reducción del ancho de banda, tanto en los contratos celebrados con los proveedores de contenidos como en los contratos celebrados con los clientes finales.

En estas circunstancias, el Verwaltungsgericht Köln (Tribunal de lo Contencioso-Administrativo de Alemania), al considerar necesaria una interpretación del Derecho de la Unión Europea para resolver el litigio principal, decidió suspender el procedimiento y solicitar al TJUE su interpretación al respecto.

Así las cosas, el Tribunal de Justicia, señaló, entre otras cosas que:

- El párrafo primero del artículo 3, apartado 3, del Reglamento, interpretado a la luz de su considerando 8, impone a los PSI una obligación general de tratar el tráfico de manera equitativa, sin discriminación, restricción o interferencia, obligación que, en ningún caso, puede ser obviada mediante prácticas comerciales puestas en marcha por estos proveedores o mediante acuerdos que estos celebren con usuarios finales (sentencia de 15 de septiembre de 2020, Telenor Magyarország, C 807/18 y C 39/19, EU:C:2020:708, apartado 47);
- Del segundo párrafo del artículo 3, apartado 3, del Reglamento 2015/2120, y de su considerando 9, a la luz del cual debe interpretarse ese párrafo, resulta que, sin dejar de estar sujetos a esta obligación general, los proveedores de servicios de acceso a Internet conservan la posibilidad de aplicar medidas razonables de gestión del tráfico. No obstante, esta posibilidad queda supeditada, entre otros, al requisito de que tales medidas se basen en «requisitos objetivamente diferentes de calidad técnica del servicio para categorías específicas de tráfico» y no en «consideraciones comerciales»;
- Una opción tarifaria de «zero rating» como la controvertida en el litigio principal realiza una distinción en el tráfico de Internet basada en consideraciones comerciales, al no imputar a la tarifa básica el tráfico con destino a aplicaciones asociadas. Por consiguiente, esta práctica comercial no cumple la obligación general de trato equitativo del tráfico, sin discriminación ni interferencia, enunciada en el artículo 3, apartado 3, párrafo primero, del Reglamento 2015/2120, y
- El incumplimiento que resulta de la propia naturaleza de esa opción tarifaria por la incitación que supone, persiste con independencia de la eventual posibilidad de continuar el acceso

libre al contenido proporcionado por los socios del proveedor de acceso a Internet una vez agotada la tarifa básica.

Lo anterior, supone que, con independencia de la modalidad de la tarifa de *zero rating*, para el TJUE esta tarifa por su naturaleza realiza una distinción en el tráfico de Internet basada en consideraciones comerciales y, en consecuencia, la considera contraría a la obligación de trato equitativo del tráfico, sin discriminación ni interferencia, señalada en el artículo 3, apartado 3, párrafo primero del Reglamento2015/2120. Lo anterior, en virtud de que para no imputar a la tarifa básica el tráfico con destino a las aplicaciones asociadas, resulta necesario hacer una discriminación del tráfico generado por el mismo usuario final.

Adicional a lo anterior, el TJUE analizó otros dos casos relacionados con tarifas de *zero rating*, así las cosas, las sentencias del TJUE afirman que las prácticas de dos operadores móviles alemanes (Telekom Deutschland y Vodafone) son incompatibles con el Reglamento de Internet Abierta de la UE.

En este contexto, BEREC señaló que sus Lineamientos para la Implementación de la Regulación de la Internet Abierta deberán revisarse a la luz de la decisión del Tribunal para reflejar la interpretación de la sentencia del TJUE.

Anexo 1c Facultades de supervisión y verificación del Instituto Federal de Telecomunicaciones[89]

De acuerdo con el artículo 15, fracción XXVIII de la LFTR, el Instituto para el ejercicio de sus atribuciones le corresponde ejercer **facultades de supervisión y verificación**, a fin de garantizar que la prestación de los servicios se realice con apego a la LFTR y a las disposiciones legales, reglamentarias y administrativas aplicables, a los títulos de concesión y a las resoluciones expedidas por el propio Instituto.

Para ello, el Instituto también se encuentra facultado, artículo 15, fracción XXX de la LFTR, para imponer sanciones por infracciones a las disposiciones legales, reglamentarias o administrativas; o por incumplimiento a lo dispuesto en los títulos de concesión o a las resoluciones, medidas, lineamientos o disposiciones emitidas por el Instituto, dictar medidas precautorias y declarar, en su caso, la pérdida de bienes, instalaciones y equipos en beneficio de la Nación.

De lo anterior, se advierte que, si bien el Instituto cuenta con facultades de supervisión y verificación del cumplimiento de los Lineamientos de neutralidad de la red y, en su caso, para imponer sanciones por su incumplimiento, los mecanismos a través de los cuales se realizará dicha supervisión y verificación deben ser aquellos que promuevan el cumplimiento del marco regulatorio en un ambiente de transparencia y certeza jurídica para los sujetos obligados.

[89] El presente anexo no pretende ser un análisis jurídico exhaustivo, toda vez que no es el *expertis* de la investigadora. Sin embargo, se considera necesario señalar que el Instituto cuenta con las facultades para monitorear el cumplimiento de la regulación que emite en torno al principio de neutralidad de la red.

Anexo 1d Imágenes en idioma original

Ilustración Id 1 Medidor de velocidad de la Agencia Federal de Redes (Página en alemán)

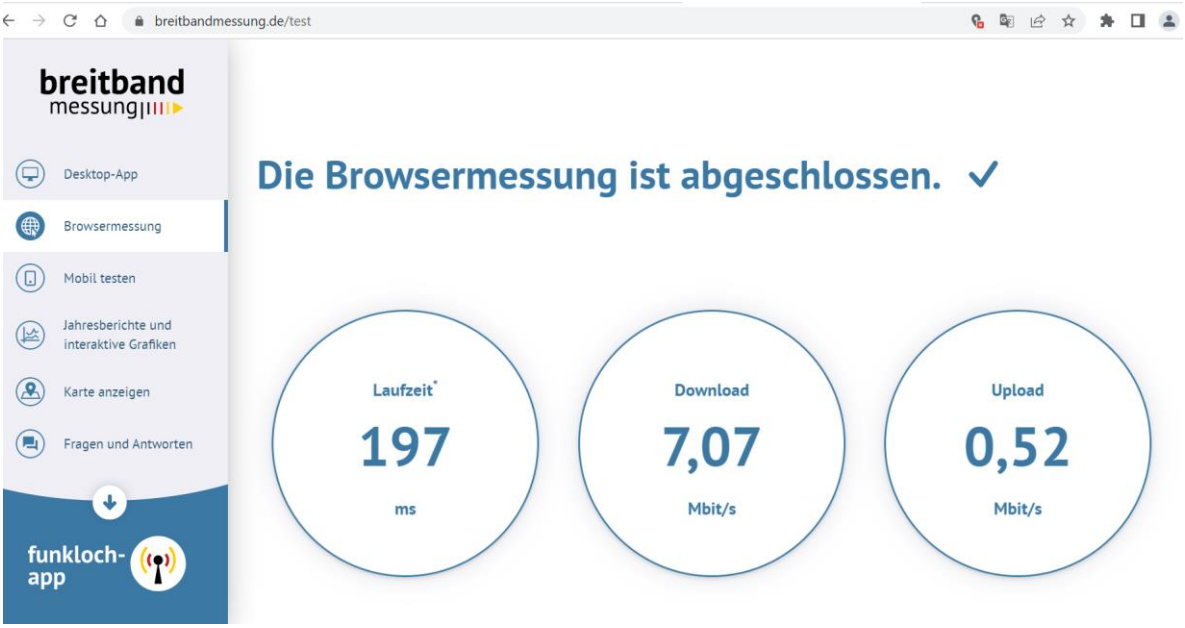


Ilustración Id 2Ejemplo de un mapa que despliegue los resultados de las mediciones del medidor de velocidad (Página en alemán)

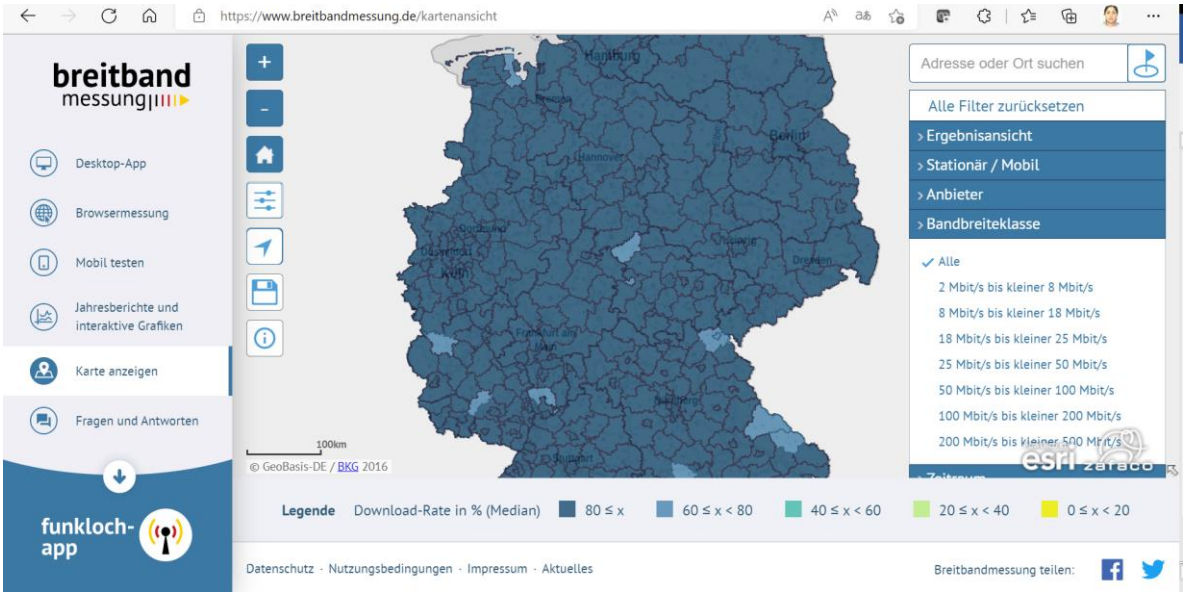


Ilustración Id 3 Estatus del reporte sobre las quejas relacionadas con las prácticas de gestión de tráfico en Canadá (Página en inglés)

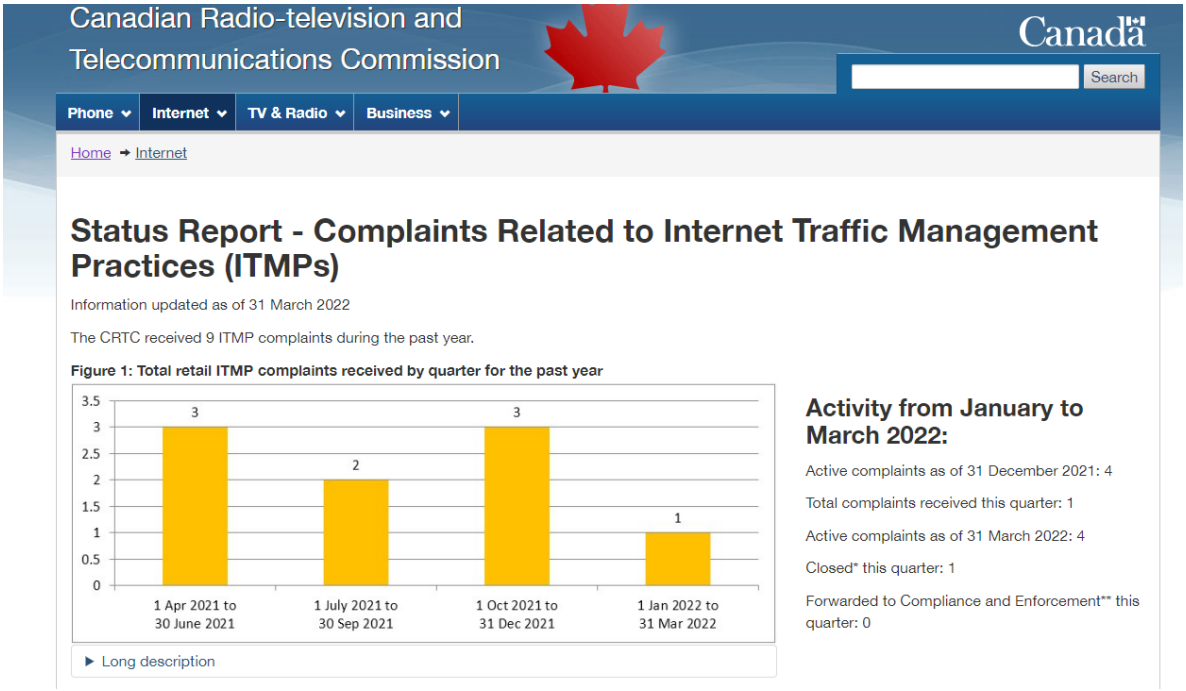


Ilustración Id 4 Cuestionario Interactivo de la CCTS (Página en inglés)

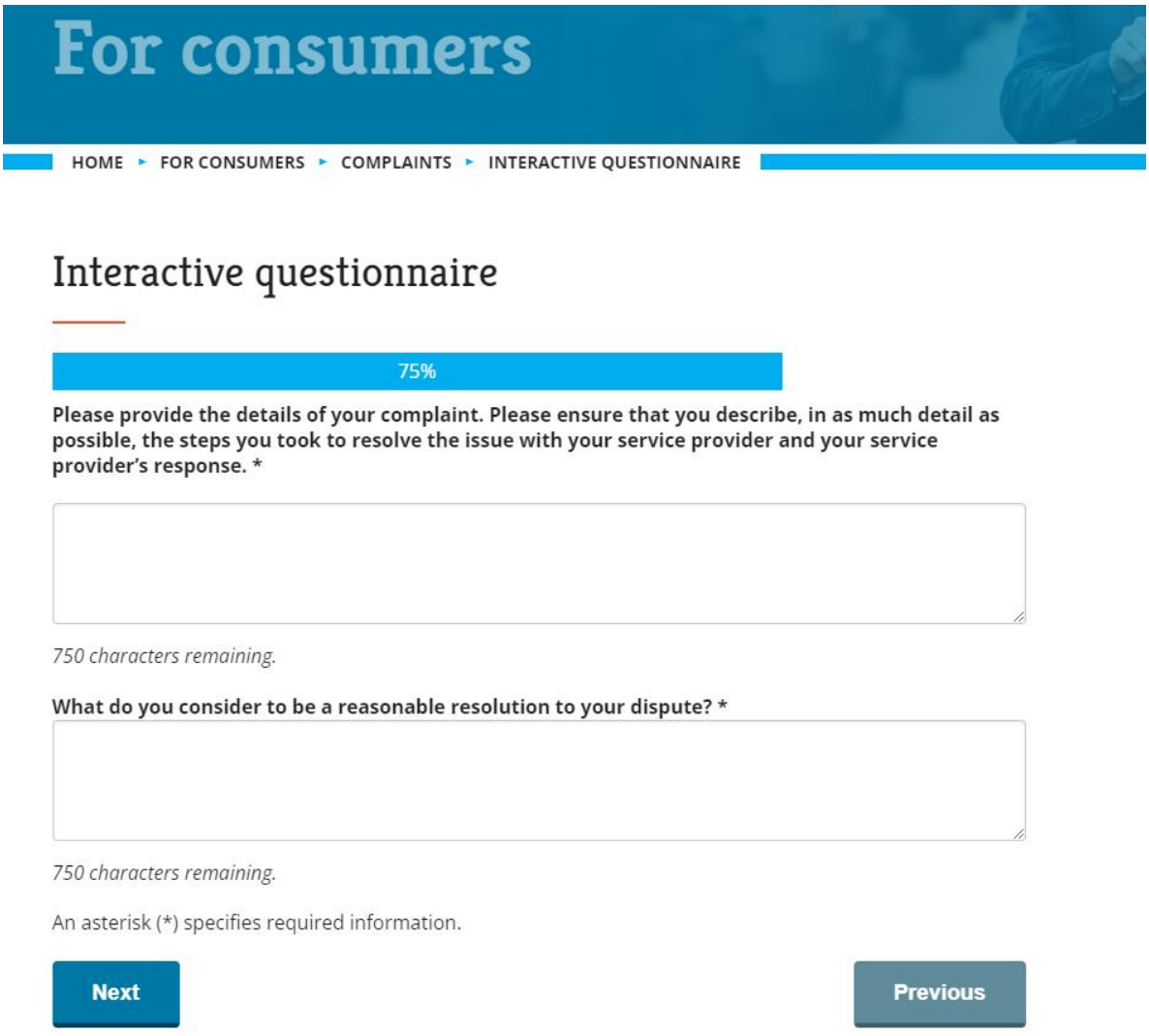
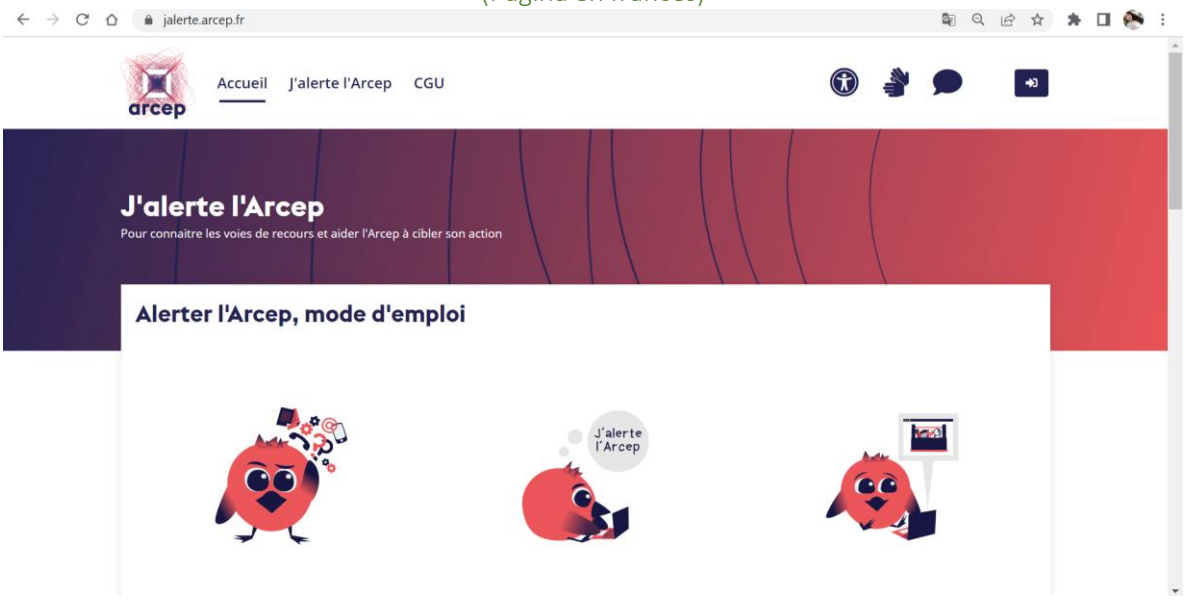


Ilustración Id 5 Alertas ante violaciones a los derechos de los usuarios y regulación J'alert a l'Arcep (Página en francés)



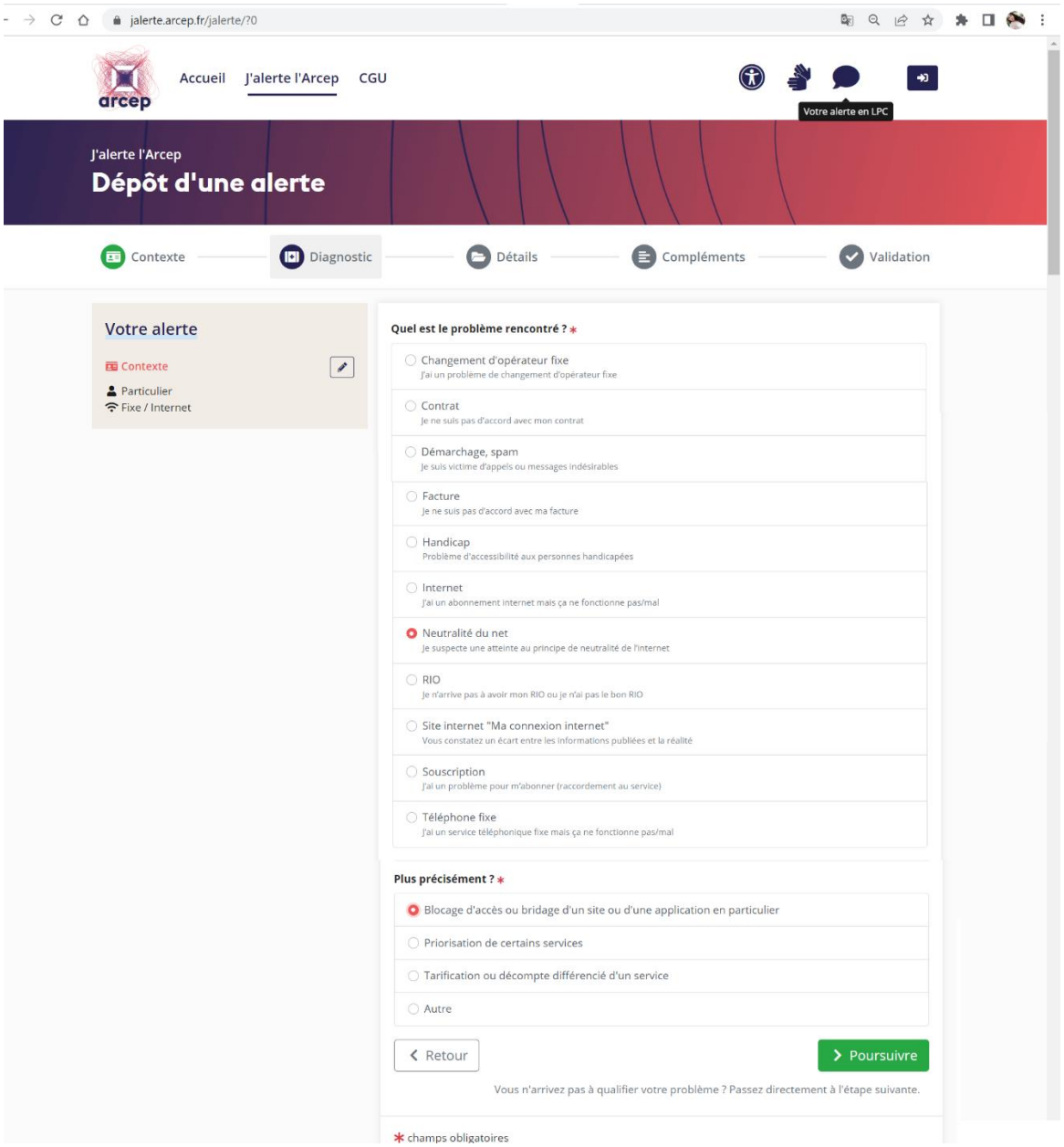

jalerte.arcep.fr/jalerte/?0
Accueil
J'alerte l'Arcep
CGU
Votre alerte en LPC
J'alerte l'Arcep
Dépôt d'une alerte
Contexte
Diagnostic
Détails
Compléments
Validation
Votre alerte
Contexte
Particulier
Fixe / Internet
Quel est le problème rencontré ? *
Changement d'opérateur fixe
J'ai un problème de changement d'opérateur fixe
Contrat
Je ne suis pas d'accord avec mon contrat
Démarchage, spam
Je suis victime d'appels ou messages indésirables
Facture
Je ne suis pas d'accord avec ma facture
Handicap
Problème d'accessibilité aux personnes handicapées
Internet
J'ai un abonnement internet mais ça ne fonctionne pas/mal
Neutralité du net
Je suspecte une atteinte au principe de neutralité de l'internet
RIO
Je n'arrive pas à avoir mon RIO ou je n'ai pas le bon RIO
Site internet "Ma connexion internet"
Vous constatez un écart entre les informations publiées et la réalité
Souscription
J'ai un problème pour m'abonner (raccordement au service)
Téléphone fixe
J'ai un service téléphonique fixe mais ça ne fonctionne pas/mal
Plus précisément ? *
Blocage d'accès ou bridage d'un site ou d'une application en particulier
Priorisation de certains services
Tarification ou décompte différencié d'un service
Autre
Retour
Poursuivre
Vous n'arrivez pas à qualifier votre problème ? Passez directement à l'étape suivante.
* champs obligatoires

Ilustración Id 6 Mapas Interactivos de Internet Móvil en Reino Unido (Página en inglés)

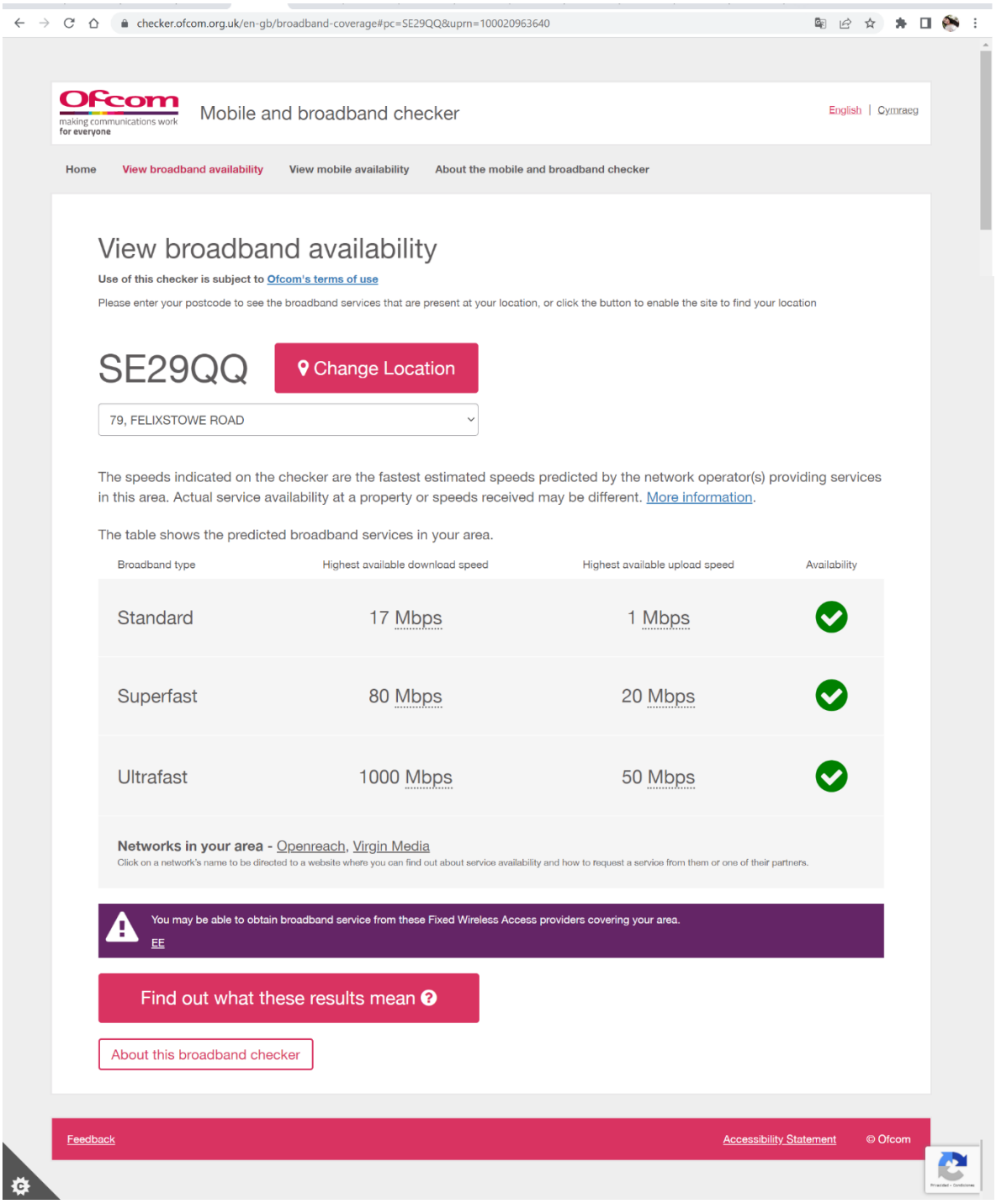


Ilustración Id 7 Mapas Interactivos de Internet Móvil en Reino Unido (Página en inglés)