PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR - MATRIZ

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

TRABAJO DE TITULACIÓN PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN ADMINISTRACIÓN DE EMPRESAS CON MENCIÓN EN GERENCIA DE LA CALIDAD Y PRODUCTIVIDAD

LA NEUTRALIDAD DE RED Y EL DESAFÍO PARA EL DESARROLLO DE LA NORMATIVA REGULATORIA EN EL ECUADOR

ING. XIMENA ALEXANDRA CORDERO SOSA

DIRECTOR: ING. EDWIN SUQUILLO, MSc.

LÍNEA DE INVESTIGACIÓN: ESTUDIOS COMPARADOS COMPLEJOS

QUITO, ENERO 2019

DIRECTOR:

Ing. Edwin Suquillo, MSc.

INFORMANTES:

Ing. Genoveva Zamora, MBA

Ing. Héctor Carrillo, MBA

DEDICATORIA

A Dios, por permitirme tener la enorme bendición de vivir y de este modo ser mi guía en cada paso que doy.

A mi familia, mis padres Fernando y Pilar, mi hermana Verito, personas por demás maravillosas a quienes admiro y por quienes su amor, enseñanzas y grandes ejemplos soy lo que soy.

A Roberto, por estar a mi lado, por creer en mí y en nosotros juntos.

Con especial cariño, a la memoria de mis abuelitos Marianita y Manuel de quienes recibí siempre cariño y amor.

A ustedes con toda mi gratitud y amor…

Ximena

AGRADECIMIENTO

En primer lugar, a Dios y a mi familia

A todas las personas que directa o indirectamente me brindaron su apoyo con sus ideas para el desarrollo de este Trabajo de Titulación, así como su apoyo en mi carrera estudiantil, profesional y personal.

A mis profesores y Director de Tesis que con sus enseñanzas y dirección me han permitido culminar con mis estudios y con el presente Trabajo de Titulación.

Finalmente, mi más sincero agradecimiento y gratitud a esta prestigiosa Universidad por haberme brindado la oportunidad de cursar por sus aulas recibiendo en ellas una formación académica de excelencia.

Ximena

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El presente trabajo examina los aspectos relacionados con el principio de la neutralidad de la red, considerando para ello el ecosistema que opera alrededor de la red Internet como son: su aspectos técnicos básicos, la cadena de integrantes que participan en su funcionamiento, posturas que existen en diferentes lugares del mundo con relación a dicha neutralidad de la red, luego de lo cual, se efectuará una propuesta de documento sobre las mejores prácticas llevadas a cabo en torno a la neutralidad de la red y que sirva como referencia para desarrollar normativa al respecto.

En el capítulo uno se describe de manera general los rasgos relacionados con el nacimiento de la red Internet con varias estadísticas alrededor del mundo incluyendo a Ecuador con lo cual se establecen las primeras bases del objetivo fundamental de este trabajo que es la neutralidad de la red; en razón de este último principio se brinda un detalle descriptivo de los puntos de debate que se tratan a nivel mundial que en lo posterior es analizado para regulaciones que se han generado en otros lugares del mundo.

En el capítulo dos se recopila de manera general la información de los marcos regulatorios sobre la neutralidad de la red, tanto para el Ecuador, como principalmente en países de América Latina, Norte América y Europa, con el objetivo de conocer de manera más detallada el tratamiento que se brinda a este principio; con base en ello y criterios de organismos internacionales en el sector de las telecomunicaciones se realizará importantes comparaciones entre los diferentes países y regiones que permitirán desarrollar algunas reflexiones importantes.

Con base en los resultados obtenidos de las revisiones previas, en el capítulo tres se propone un documento referencial sobre los aspectos que en materia de neutralidad de la red se podrían llevar a cabo en la implementación reglas y normativa específica en el Ecuador sobre este principio en el futuro; además se aporta con recomendaciones basadas en los resultados anteriores obtenidos para los diferentes actores que forman parte del ecosistema que abarca la neutralidad de la red.

En el capítulo cuatro, se presentan las conclusiones y recomendaciones obtenidas como resultado del desarrollo del presente trabajo de titulación.

INTRODUCCIÓN

Desde su origen como una red abierta por el año 1989, el Internet se ha ido desarrollando de una manera vertiginosa hasta el día de hoy gracias a la evolución tecnológica, la innovación y las prestaciones que ofrece esta potente herramienta difundidas a nivel mundial, incluyendo al Ecuador; muestra de ello es la cantidad de conexiones que existen actualmente en el país, pues según los datos que presenta el Instituto Nacional de Estadísticas y Censos (INEC), al 2017, el 58,3% de la población desde 5 años en adelante han utilizado Internet en ese periodo anual de tiempo; y que decir a nivel mundial, el reporte digital del año 2018 señala que a inicios de este año, se estipula que existe alrededor de 4 billones de usuarios de Internet con una penetración del 53%, lo que significa un 7% más en relación al inicio del año 2017.

Dentro del ecosistema de Internet se identifican varios involucrados como son: los usuarios y comunidad social en general, proveedores del servicio de Internet (ISP), las conexiones técnicas y la propia red como un conjunto mundial de computadoras conectadas entre sí a través del protocolo TCP/IP; con lo cual, tiene sentido el aparecimiento del principio denominado como neutralidad de la red que sostiene básicamente que los paquetes de datos que circulan a través de la red de Internet deben moverse de forma libre e imparcial y sin restricción alguna, sin tener en cuenta el contenido, origen o destino.

Bajo la concepción del principio de la neutralidad de la red es de considerar algunos puntos clave de debate que se generan en torno a él alrededor del mundo; entre ellos, la importancia que tiene para cualquier usuario en el mundo o empresas, el hecho de poder acceder a la información que se encuentra en Internet sin restricciones que puedan básicamente vulnerar sus derechos de disponer de toda la información que le sea de utilidad y de acuerdo a sus necesidades.

Como aristas importantes de revisión en este trabajo se encuentran: la gestión de tráfico de Internet y la priorización que se podría generar para los diferentes tipos de contenidos; la transparencia, por lo cual se establece que los usuarios tienen el derecho de conocer de

manera detallada las condiciones del servicio que reciben; bloqueo de contenido que puede tener relación con varios factores tales como condiciones sociales, protección de las red y contenido ilegal y por último el propio contenido que circula en Internet que puede ser de distinta índole desde simples archivos hasta información que puede ser considerada como censurable por Gobiernos de diferentes países en el mundo.

La neutralidad de la red es un tema que se ha tornado complejo y controvertido, de tal manera que se han generado amplias discusiones sobre este tema alrededor del mundo y sobre lo cual es factible realizar un vistazo más detallado; en el Ecuador por ejemplo, la Ley Orgánica de Telecomunicaciones (LOT) establece apenas rastros de una regulación hacia este principio siendo a criterio de algunos críticos que no se garantiza en su totalidad la neutralidad. En otros lugares como la Unión Europea y países de Latinoamérica también se pueden identificar que se establecen de uno u otro modo las consideraciones que debe tener la neutralidad de la red.

Un caso particular de análisis es la reciente decisión en el año 2018 de Estados Unidos por reformular las características de la neutralidad de la red y cómo dicha decisión incidirá posiblemente en otros países en el mundo.

Se debe tomar en cuenta que paralelamente a los propios Gobiernos y unidades reguladoras de los diferentes países, existen varios organismos y las propias empresas proveedoras del servicio de acceso a Internet que cuentan con su propio criterio, ya sea a favor o en contra de la llamada neutralidad de la red.

El conjunto de conclusiones y criterios propios acerca del tratamiento del principio de neutralidad de la red alrededor del mundo dará lugar a la propuesta de un documento sobre las que se considerarían mejores prácticas en torno a dicho principio que podrían ser evaluadas en lo posterior bajo el contexto de aplicación de normativas orientadas a delinear las características de cumplimiento que deberán tener los diferentes actores parte del ecosistema de la neutralidad de la red en el Ecuador.

1 FUNDAMENTOS Y ORIGEN DE LA NEUTRALIDAD DE RED

Los humanos por esencia somos seres sociales y con necesidad de comunicación; en tal sentido, en el transcurso de los tiempos se han generado inventos que han facilitado la misma, pasando desde el habla y la escritura hasta las telecomunicaciones con la fascinante era digital actual en donde se encuentran las comunicaciones con tecnología inteligente e Internet.

En la actualidad, las redes telecomunicaciones a nivel mundial ofrecen la creación de medios dedicados para ahorro de tiempo en la comunicación eficiente y su implementación se ha encontrado a cargo de los Gobiernos y de las diferentes empresas de telecomunicaciones. En el Ecuador, es desarrollo de las telecomunicaciones también ha formado parte de nuestros días, pues, la Constitución de la República del Ecuador define en su artículo 313 como sectores estratégicos a aquellos que por su trascendencia tienen decisiva influencia económica, social, política o ambiental y se consideran como tal a la energía en todas sus formas, las telecomunicaciones, los recursos naturales no renovables, el transporte y la refinación de hidrocarburos, la biodiversidad y el patrimonio genético, el espectro radioeléctrico, el agua, y los demás que determine la ley (Asamblea Nacional, 2008).

Tanto a nivel nacional como internacional el sector de las telecomunicaciones se encuentra regido por la normativa internacional y aquella que es propia para cada uno de los países; para el Ecuador, por la Constitución, y luego por normativa internacional, leyes y normas de carácter nacional.

Con el vertiginoso desarrollo de las telecomunicaciones se tiene de la mano que la historia de Internet tiene su origen por los años 60, donde un grupo de científicos de la defensa militar de los Estados Unidos comenzó a trabajar en la *"Red de la Agencia de Proyectos Avanzados de Investigación"* o Advanced Research Projects Agency Network (ARPANET) por sus siglas en inglés, con la finalidad de crear una red de computadoras para unir los centros de investigación de defensa en caso de ataques y que pudieran mantenerse comunicadas entre sí (Universidad de Chile, 1996).

A partir de ello, estas conexiones fueron expandidas y utilizadas por Gobiernos, universidades y diferentes centros académicos, hasta que en el año 1969 se utilizaron estas redes para el envío de tráfico de paquetes de información entre el Massachusetts Institute of Technology (MIT) y la Stanford Research Inst. U. de California los Ángeles (UCLA) (BIWEBZONE, 2018), dando paso a las redes interconectadas conocidas actualmente como Internet, que permite el uso de correo electrónico, uso de la Web (World Wide Web), conversaciones en línea, compartición de archivos, intercambio de información, creación de páginas; en fin, la Internet es al día de hoy una herramienta poderosa para la difusión de información a nivel mundial y un medio de colaboración para la sociedad en general.

En principio, Internet ha sido creado como una red de comunicaciones completamente abierta, a través de la cual la información puede fluir sin discriminación de su contenido; sin embargo, el paso del tiempo y su éxito han provocado que se genere interés por su control por parte de los Gobiernos y proveedores del servicio de Acceso a Internet.

Con las tecnologías actuales, hoy en día es factible diferenciar Internet con base al tipo de tráfico que circula por ella y dispositivos empleados, pudiendo dejar de lado los principios de igualdad de acceso. A este control sobre la información contenida en Internet es lo que comprende el debate principal de la neutralidad de la red. En los siguientes numerales se detallará acerca de la neutralidad en la red, sus aspectos técnicos y su regulación, tomado como base los aspectos de telecomunicaciones en otras regiones del mundo y Ecuador.

1.1 Los servicios de telecomunicaciones en el Ecuador

Las telecomunicaciones en el Ecuador iniciaron a fines del siglo pasado, se considera el 09 de julio de 1884, cuando por primera vez se realizó una transmisión de un mensaje telegráfico entre Quito y Guayaquil por vía alámbrica (SUPERTEL, 2017).

Desde este acontecimiento, el crecimiento de las telecomunicaciones en el país ha tenido un importante despunte tanto en aspectos tecnológicos como normativos que han tenido como fundamento la Constitución de la República del Ecuador y las leyes desarrolladas para este efecto.

La Ley Orgánica de Telecomunicaciones (en adelante LOT) que fue expedida el 18 de febrero de 2015 y publicada en el registro oficial n° 439 define al servicio de telecomunicaciones como aquel que es soportado sobre redes de telecomunicaciones para permitir y facilitar la transmisión y recepción de signos, señales, textos, vídeo, imágenes, sonidos o información de cualquier naturaleza, para satisfacer las necesidades de telecomunicaciones de los abonados, clientes, usuarios.

Así mismo, la LOT define servicios de radiocomunicación como aquellos que transmiten, emiten y reciben señales de imagen, sonido, multimedia y datos, a través de estaciones del tipo público, privado o comunitario, con base a lo establecido en la Ley Orgánica de Comunicación. Dentro de estos servicios de señal abierta y por suscripción.

Actualmente y de acuerdo a lo dispuesto en esta normativa, le corresponde a la Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL) emitir la regulación correspondiente para la provisión de los servicios de telecomunicaciones en el Ecuador de conformidad a lo señalado en la Constitución y políticas que en este sector sean determinadas por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL).

Posteriormente con Resolución N° 05-03-ARCOTEL-2016, publicada en Registro Oficial N° 749 de 06 de mayo de 2016, la ARCOTEL emitió el "*Reglamento para la prestación de servicios de telecomunicaciones y servicios de radiodifusión por suscripción"*; en el mismo, se indica que los servicios de telecomunicaciones y servicios de radiodifusión por suscripción son inicialmente los siguientes: Servicio Móvil Avanzado (SMA), Servicio de Telefonía Fija, Portador, Móvil Avanzado a través de Operador Móvil Virtual (OMV), Telecomunicaciones por Satélite, Transporte internacional, Valor Agregado, Acceso a Internet, Troncalizados, Comunales, Audio y video por suscripción, Otros que determine el Directorio de la ARCOTEL, previo informe de la Dirección Ejecutiva de dicha Agencia.

A continuación, se describe brevemente el concepto de los diferentes servicios de acuerdo al reglamento antes en mención y las estadísticas actuales correspondientes.

1.1.1 Servicio de Telefonía Fija

Se define como aquel servicio que conduce tráfico telefónico conmutado a través de equipos terminales que tienen una ubicación geográfica determinada; su acceso puede ser alámbrico e inalámbrico.

1.1.2 Servicio Móvil Avanzado

Servicio móvil terrestre que permite toda transmisión, emisión y recepción de signos, señales, escritos, imágenes, sonidos, voz, datos o información de cualquier naturaleza. Los prestadores de SMA requieren de la asignación de frecuencias esenciales de espectro radioeléctrico.

1.1.3 Servicio Portador

Los Servicios Portadores son los que proporcionan a terceros la capacidad necesaria para la transmisión de señales entre puntos de terminación de red definidos, pueden ser suministrados a través de redes públicas conmutadas o no conmutadas integradas por medios físicos, ópticos y electromagnéticos.

1.1.4 Servicio de Acceso a Internet

Servicio que permite la provisión del acceso a la red mundial Internet, por medio de plataformas y redes de acceso implementadas para tal fin.

1.1.5 Servicio de Audio y Video por Suscripción

El servicio de audio y video por suscripción es aquel que se ofrece a través de sistemas de audio y video por suscripción bajo modalidades de cable físico, televisión codificada terrestre y televisión codificada satelital a un público particular de suscriptores.

Conforme se despende de lo descrito, en la normativa existe regulación para los diferentes servicios de telecomunicaciones en el Ecuador.

1.2 Internet y sus agentes de la cadena de valor

La historia de Internet a través de los últimos periodos de tiempo abarca una serie de desarrollos revolucionarios, tal que a nivel sectorial, este servicio sea utilizado actualmente en una multitud de ocasiones.

En los siguientes acápites se describirá de una manera más formal la definición de Internet, así como los aspectos que se encuentran directamente relacionados a éste.

1.2.1 Definición de Internet

La Unión Internacional de Telecomunicaciones (UIT), a través de su recomendación UIT-T Y.101 (2000) referente a "Terminología de la infraestructura mundial de la información: Términos y definiciones", misma que se encuentra contenida a su vez en la Recomendación N° UIT-T Y.2091 (2007), define al Internet como: "Conjunto de redes interconectadas que utilizan el protocolo de Internet, que les permite funcionar una única y gran red virtual"

La definición formal que brinda la UIT puede complementarse en el sentido mismo del propósito actual de esta red, siendo una herramienta poderosa que actúa como medio de comunicación autosuficiente y de acceso a toda clase de información y contenidos para millones de personas en el mundo.

1.2.2 Elementos que forman parte del Ecosistema Internet

Con la definición formal que brinda la UIT respecto a Internet, es importante ahora realizar la descripción de los elementos que intervienen para concretar la conexión a esta gran red mundial y participan en ella; de esta manera, son elementos para conexión y que intervienen en Internet, los siguientes: Hardware; Software; Protocolo TCP/IP; Proveedores de Internet, contenido y aplicaciones; usuarios y Gobierno. Anexo 1 (DATATECA, 2018)

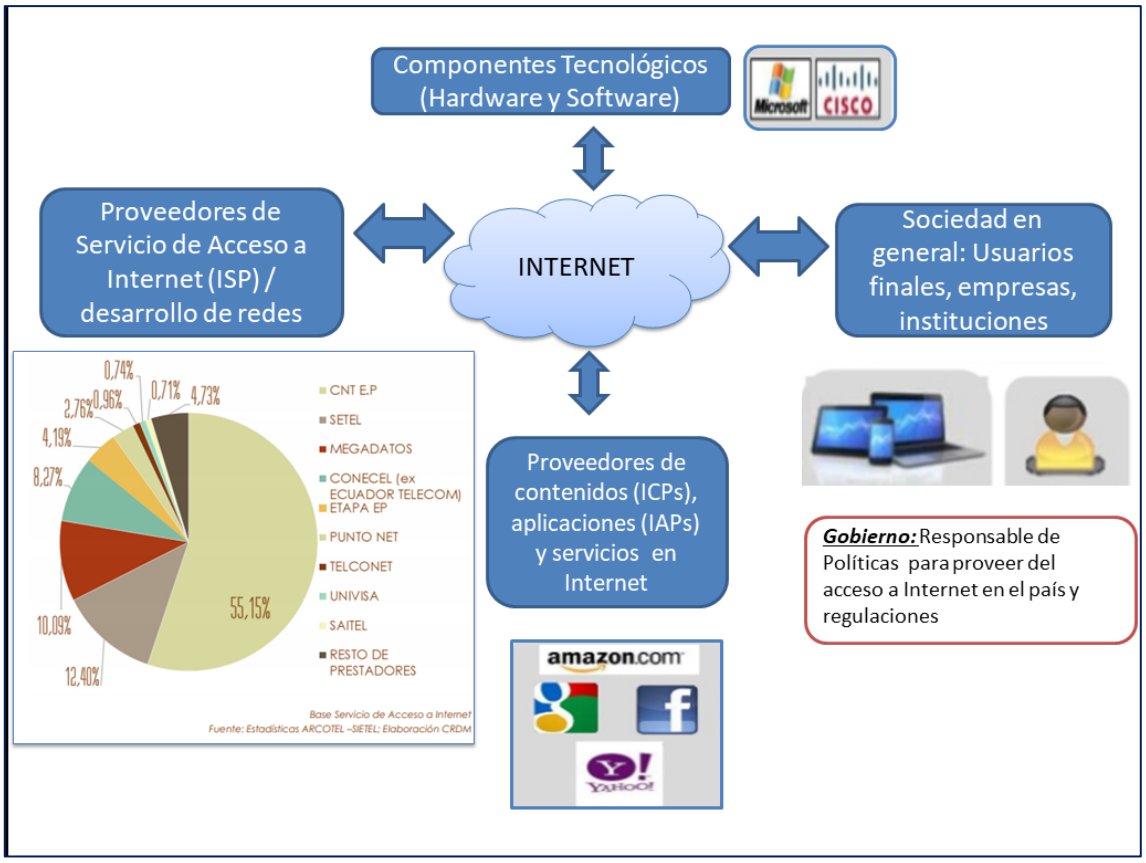

Figura 1: Ecosistema de Internet – Intervinientes en la Neutralidad de la Red (NR)

1.2.3 Situación del Acceso a Internet a nivel mundial

Con el rápido desarrollo de Internet en los últimos tiempos y las bondades que ofrece a través de la información que se encuentra contenida en la misma, se han generado diversas experiencias de desarrollo de la sociedad; de esta manera es interesante como antesala al análisis de la neutralidad de red realizar un vistazo a las estadísticas mundiales de usos y penetración de Internet.

El conjunto de informes de Global Digital para el año 2018 indica que en la actualidad hay más de 4 mil millones de usuarios de Internet en todo el mundo, lo que representa más de la mitad de la población mundial. A continuación, conforme se aprecia de la Figura 1, se visualiza la penetración de Internet a nivel mundial y por región:

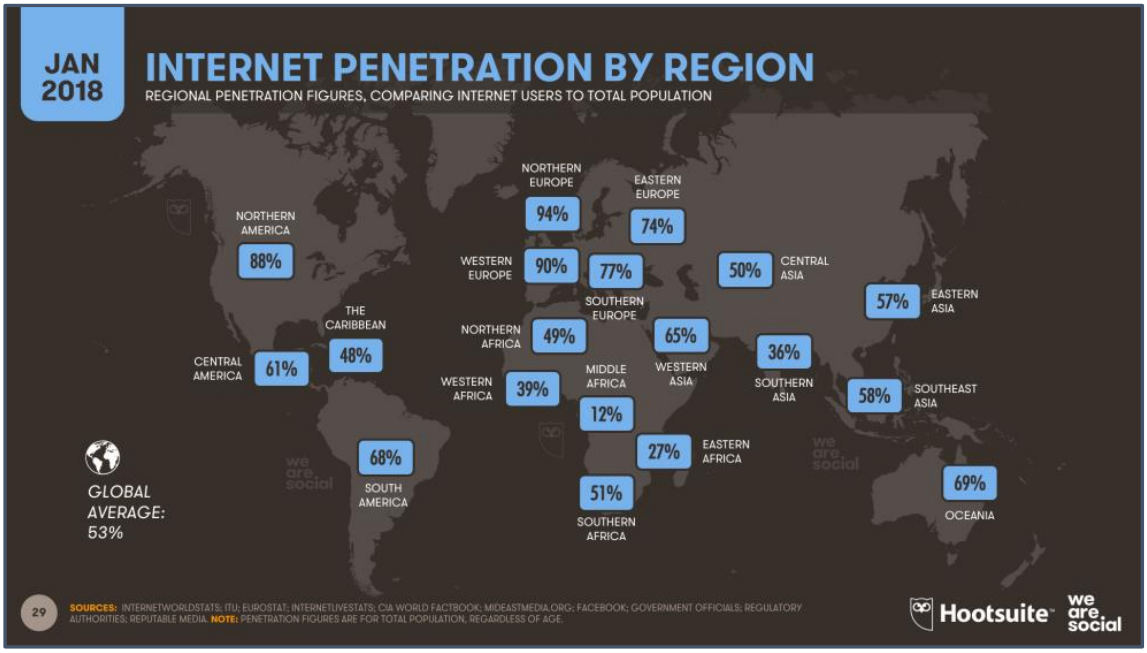

Figura 2: Penetración de Internet a nivel mundial a enero de 2018

Fuente: (Global Digital, 2018)

De las estadísticas precedentes, se pueden obtener una variedad de hallazgos interesantes, tales como (Global Digital, 2018):

- En el año 2017, casi 250 millones de nuevos usuarios se conectaron a Internet.

- El número de usuarios de Internet en 2018 sería un 7% mayor en relación al año 2017, con 4.021 mil millones que representa el 53% de la población mundial.

- El total de usuarios activos en Internet desde dispositivos móviles es de 3.722 mil millones, que representa a su vez el 49% de la población mundial.

- La cantidad de usuarios en redes sociales en 2018 sería un 13% mayor en relación al año 2017, con 3.196 mil millones.

- A nivel de las diferentes regiones del mundo, se presentas siguientes tablas:

Tabla 1: Uso de Internet en el mundo

Continente	Población	Usuarios de Internet	Usuarios de medios sociales	Conexiones móviles	Usuarios redes sociales en móvil
	Valores se indican en millones				
África	1.272	435	191	1.040	172
Crecimiento anual desde 2017		20%	12%	4%	15%
América	1.011	741	648	1.070	581
Crecimiento anual desde 2017		3%	8%	0,1%	9%
Asia Pacífico	4.214	2.007	1.779	4.318	1.713
Crecimiento anual desde 2017		5%	14%	8%	16%
Europa	843	674	448	1.106	376
Crecimiento anual desde 2017		6%	8%	0,5%	8%
Medio Oriente	252	164	130	323	115
Crecimiento anual desde 2017		11%	39%	3%	39%
Ecuador	16.74	13.47	11.00	15.23	10.00
Penetración		80%	66%	91%	60%

Fuente: (Global Digital, 2018)

1.2.4 Cifras de la situación del Acceso a Internet en el Ecuador

Según las estadísticas presentadas por el INEC en su información sobre tecnologías de la información y comunicación, el equipamiento de computadores de escritorio y portátiles (laptop y Tablet) en los hogares se ha incrementado desde un 8.1% en el año 2012 hasta el 11.2% en el año 2017 (INEC, 2018).

A su vez, el acceso a Internet a nivel nacional para el año 2017 se ha incrementado en 14.7 puntos con relación al año 2012 en área urbana (31.4% a 46.1%), mientras que en área rural este crecimiento es de 11.8 puntos (4.8% a 16.6%). En cuanto al uso de las computadoras por parte de las personas se tiene para el año 2017, que los usuarios de

entre edades de 16 a 24 años utilizan en mayor porcentaje las computadoras con un valor porcentual de 78.5%; y, quienes menos utilizan son las personas que se encontrarían entre 65 años y más con un 6.1% (INEC, 2018).

En lo que corresponde al uso de Internet, la población de 5 años o más ha utilizado Internet en el año 2017 es del 58.3% de la población total; el 66.9% dentro del área urbana y 39.6% en el área rural; ello se complementa con que el uso de Internet en mayor porcentaje (85.2%) se efectúa por parte de la población que se encuentra entre los 16 a 24 años (INEC, 2018).

Entre las primeras cinco (5) provincias del Ecuador que utilizan Internet tenemos: Galápagos (81.3%), Pichincha (68.7%), Azuay (64.5%), Guayas (63.7%) y El Oro (61.9%) (INEC, 2018).

1.2.5 Servicios que se ofrecen por Internet

En función de las estadísticas mundiales, se puede dilucidar en cuanto a las actividades de Internet que la tendencia mundial es para la obtención de información, entretenimiento y comunicación; seguido de acceso a contenidos, redes sociales, lectura de periódicos, revistas o libros; y, finalmente para interactuar con autoridades, compra de productos y operaciones bancarias en línea.

Tabla 2: Clasificación sitios web más visitados

CLASIFICACIÓN DE LOS SITIOS WEB QUE ATRAVIESAN EL MAYOR VOLUMEN DEL TRÁFICO WEB EN EL MUNDO (Alexa ranking, basado en el promedio diario de visitantes y vistas de páginas)			
#	Sitio web	Categoría	Tiempo por día
1	GOOGLE.COM	búsqueda	7:35
2	YOUTUBE.COM	video	8:18
3	FACEBOOK.COM	red social	10:20
4	BAIDU.COM	búsqueda	7:32
5	WIKIPEDIA.ORG	referencias	4:16
6	REDDIT.COM	red social	15:47
7	YAHOO.COM	noticias	4:03
8	GOOGLE.CO.IN	búsqueda	7:05
9	QQ.COM	noticias	4:34
10	AMAZON.COM	compras	8:29

Fuente: (Global Digital, 2018)

Al igual que en el resto del mundo, en el Ecuador también se puede identificar las razones por las cuales las personas acuden al uso de Internet; en este sentido se presenta la siguiente Figura 3.

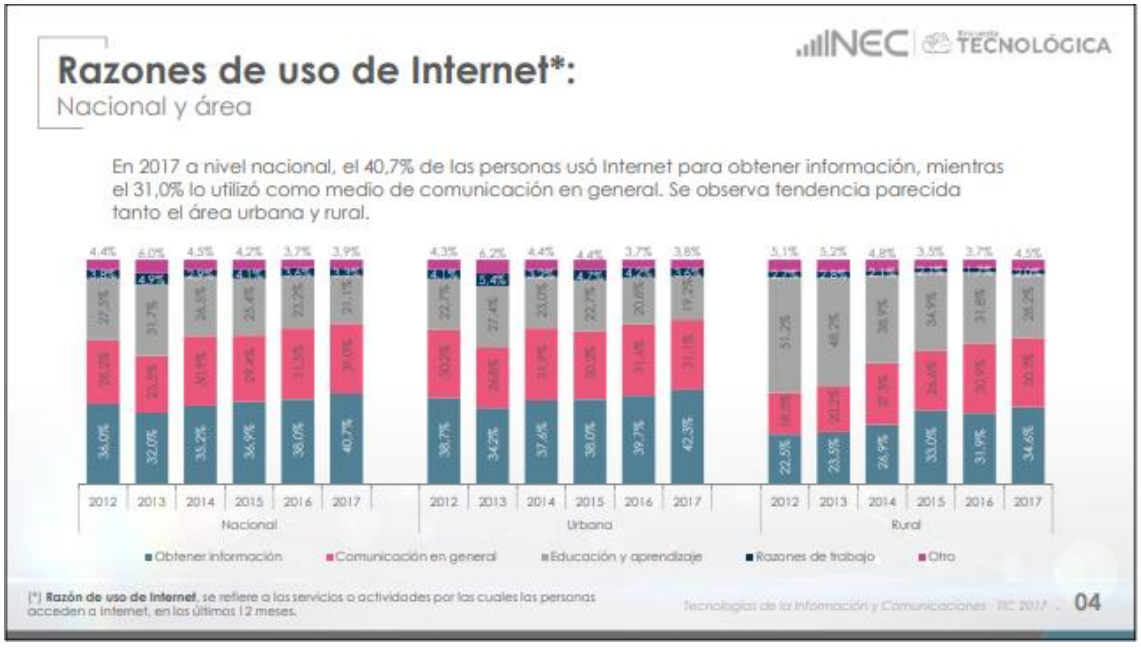

Figura 3: Razones del uso de Internet a periodo 2012 -2017

Fuente: (INEC, 2018)

Adicionalmente, a continuación se muestra la Figura 4, por medio de la cual se evidencia que con relación a la frecuencia de uso de Internet, en el año 2017 se tiene que las personas acceden a Internet, al menos una vez al día.

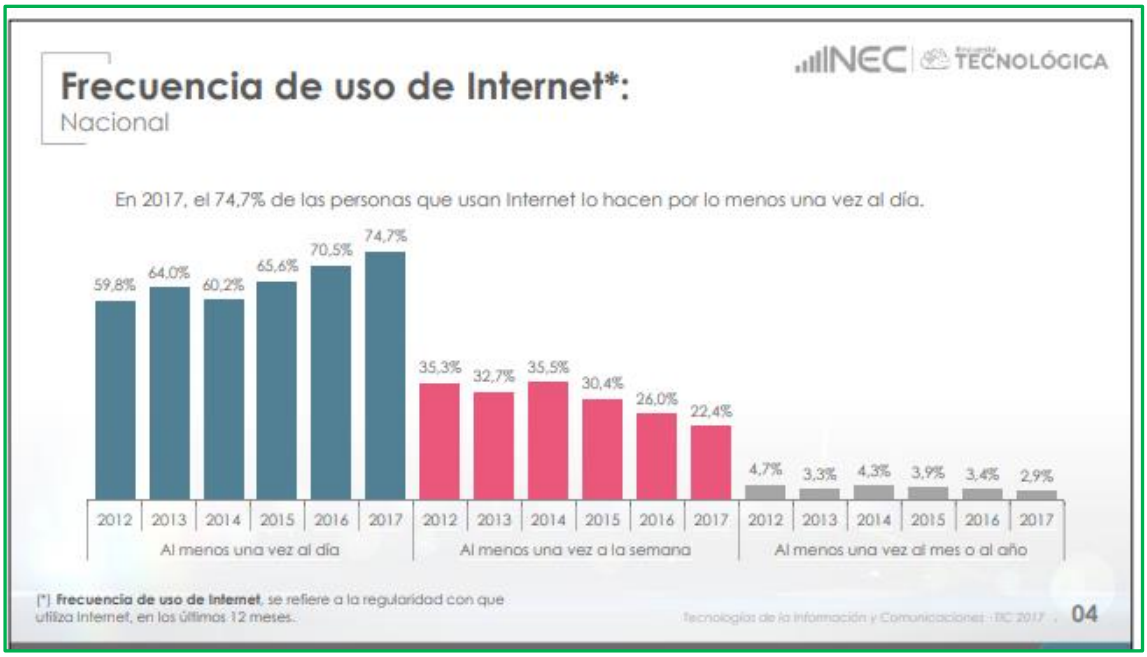

Figura 4: Frecuencia de uso de Internet a periodo 2012 -2017

Fuente: (INEC, 2018)

1.2.6 Proveedores de acceso a Internet

Entre los actores que forman parte de la prestación del servicio de Internet, se encuentran los antes ya mencionados, proveedores de acceso a Internet (ISP por siglas en inglés), mismos quienes como empresas son aquellas que brindan las facilidades necesarias para la conexión hacia Internet a los usuarios.

Mundialmente, el acceso fue facilitado por empresas de gran tamaño desde la década de 1990 y por tanto, su crecimiento desde entonces ha sido sumamente importante en razón de la propia evolución de Internet. En el Anexo 2, se detallan algunos ISP que existen en diferentes países.

En el Ecuador, el servicio de acceso a Internet es uno de los de mayor crecimiento y demanda en el país debido a la existencia de la alta cantidad de contenido, información,

aplicaciones, redes sociales que se genera y se encuentra disponible en la red para todos los usuarios.

De esta forma, en el país, la regulación del sector de las telecomunicaciones establece el Acceso Universal entre otros servicios, al de Internet y de esta manera, a través de las acciones que se encuentran establecidas en el Plan Nacional de Telecomunicaciones y Tecnologías de información del Ecuador para el periodo 2016 – 2011, se busca alcanzar metas importantes del uso de Internet a nivel nacional (MINTEL, 2016).

En consecuencia, en el país existen varios proveedores de acceso a Internet, cuya participación se puede destacar de la siguiente manera al cierre del año 2017:

- El operador público corporación nacional de telecomunicaciones CNT EP con el 53,49%.

- SETEL S.A. (marca comercial GRUPO TV CABLE), con el 12,21%.

- MEGADATOS (marca comercial NETLIFE), con el 11,30%.

- CONECEL S.A. (marca comercial CLARO), con el 8,26%, ETAPA con el 4,11%, Puntonet con 3,10% y resto de operadores con el 7,53% (ARCOTEL, 2017).

1.2.7 Proveedores de Contenido

En el contexto del desarrollo de Internet y una vez que existen los factores que permiten a los usuarios acceder a él, los proveedores de contenidos se convierten en fuertes impulsadores del consumo de este servicio; tal es el caso, que existe actualmente una presencia cada vez más creciente de información de contenido digital que adquiere un papel importante en la vida social y cotidiana que a su vez conlleva a transformaciones de la propia sociedad en su mentalidad a cambio de mayores conocimientos.

Con ello, existe un multitud de contenidos a nivel mundial a los cuales los usuarios pueden acceder a través de los diferentes portales o denominados sitios web, en donde las personas, empresas, entidades gubernamentales facilitan una enorme cantidad de

información, misma la cual puede reunir varias características como datos en tiempo real, información útil y con valores añadidos o hasta personalizada.

Los contenidos en Internet pueden cubrir una amplia demanda de requerimientos como búsqueda de información en diversos idiomas, documentación, contenidos de redes sociales, actualidad, contenidos personalizados, multisoporte (contenidos en HTML, XML, WAP, vía e-mail, multimedia), etc.

Con base en la diversidad de contenido que existe en Internet, se describe en el Anexo 3 de manera general algunos de ellos para una mejor referencia (ONTSI, 2017).

El estudio de comportamiento de compra por Internet en Ecuador para el 2017 realizado por la UEES muestra las actividades que se realizan con mayor frecuencia en Internet por parte de los usuarios:

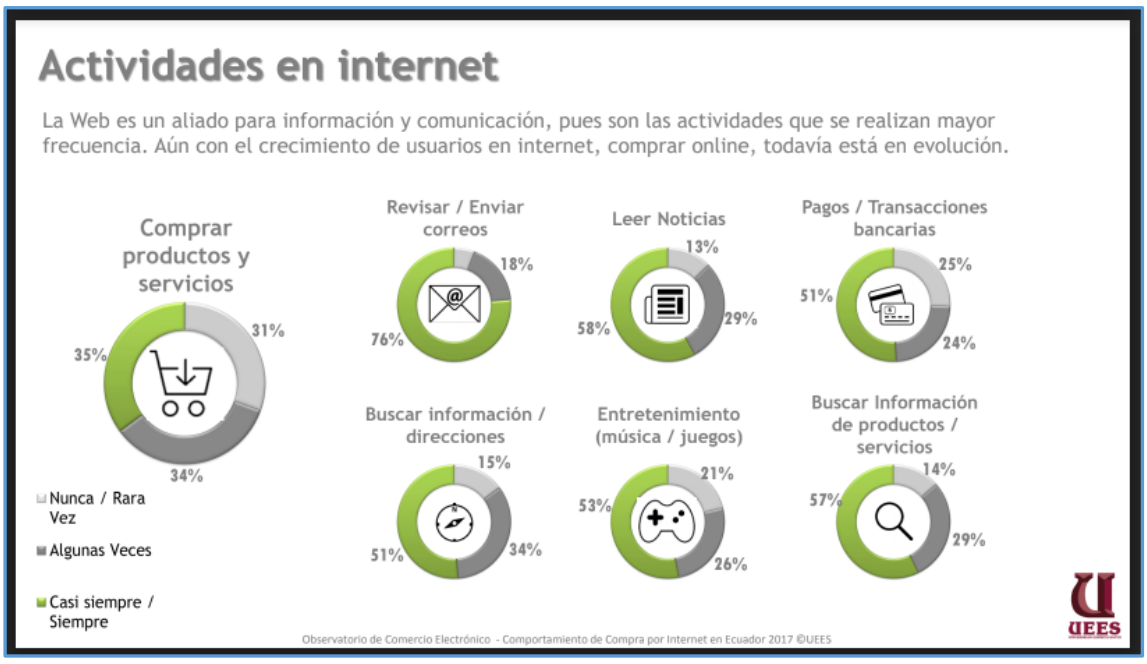

Figura 5: Actividades realizadas por Internet en Ecuador

Fuente: (UEES, 2017)

1.2.8 Reguladores e Instituciones

Con el importante desarrollo de Internet en los últimos tiempos como un fenómeno a nivel mundial, los Gobiernos de los diferentes países tienen un reto muy interesante de la mano

con sus respectivos organismos reguladores para fines de trabajar en un entorno digital en donde se convierten en temas de alta relevancia la seguridad de las redes, la privacidad, protección de datos, calidad en la entrega de servicios a los usuarios.

A su vez, los organismos reguladores toman como principio de aplicación las políticas institucionales que se desarrollan a nivel nacional y por tanto, esto significa un reto significativo para encausar los objetivos alcanzados en beneficio de todas las personas en diferentes campos de acción ya sea la salud, educación, desarrollo de nuevas tecnologías.

Ahora mismo, en varios países a nivel mundial se promueve el servicio de acceso a Internet y en consecuencia de ello, se promueve la facilidad para acceso de los diferentes contenidos.

En cuanto a organismos reguladores, en América Latina por ejemplo existen organismos reguladores independientes en el ámbito de telecomunicaciones en 28 países y entre los desafíos para una regulación entorno a la digitalización se encuentran la eficiencia de mercado, gestión de los recursos definidos como escasos, protección de derechos del consumidor (CEPAL, 2018)

Por otra parte, existen instituciones que se relacionan de manera muy estrecha con Internet, de las cuales se realiza en el Anexo 4 una descripción general de las mismas (Guerrero & Chávez, 2015).

1.2.9 Impacto en la sociedad con base en el uso de Internet

Lo cierto de Internet es que, conforme se ha descrito en numerales precedentes, ésta es una inmensa red global que permite el acceso a una innumerable cantidad de información como su pilar fundamental y de este modo, la comunicación en los últimos periodos de tiempo ha tenido un despunte importantísimo convirtiéndose en lo que se está denominando como “nueva era de la información” para los usuarios.

Socialmente, se puede evidenciar que hay factores positivos tanto como negativos en el uso de Internet y el uso de su información; de esta manera se mencionan de manera general algunos de ellos en el Anexo 5.

1.3 Neutralidad de la Red (NR)

Como se evidencia de lo observado en los numerales precedentes, se puede afirmar que Internet a más de ser la red de comunicaciones más grande que existe en el mundo, es actualmente la red en la cual se incluye a cada segundo que pasa una inmensa cantidad de información que resulta importante no solo para los usuarios, sino para la sociedad en general.

El flujo de información que existe en Internet permite que la información viaje de un punto a otro de manera libre; de este modo, en lo subsiguiente, se abordará el análisis acerca de la "neutralidad de la red", un principio que no es nuevo, sin embargo del cual en la actualidad se tienen importantes debates a nivel mundial.

1.3.1 Antecedentes

Los antecedentes del principio de la neutralidad de la red se remontan hace un tiempo, con el inicio de del telégrafo en los EE.UU., en donde la ley americana establecía en 1860 subvenciones para las líneas telegráficas costa a costa:

> "(...) los mensajes recibidos de cualquier individuo, empresa, o corporación, o de cualquier línea de conexión de telégrafo con esta línea en cualquiera de sus extremos, se transmitirá de manera imparcial en el orden de su recepción, a excepción que los despachos del gobierno deberán tener prioridad" (Espinoza & González, 2015).

Luego, con el aparecimiento de Internet a principio de los años noventa, el mundo ha tenido la mayor revolución tecnológica, con una inmensa evolución de la red, información creada por usuarios, intercambio de datos de distinta índole por medio de mensajes que son divididos en pequeños paquetes (datagramas) y que viajan de punto a punto bajo una concepción de un flujo libre.

De esta forma, para Internet no había sido necesaria ninguna regulación, sino simplemente aquellas directrices que podrían referirse a su interoperabilidad y competencia y, a aquella que tuviera que ver con su diseño de extremo a extremo; no obstante, a finales de los años noventa surgió la necesidad de mayor confianza y seguridad

en la banda ancha, por cuanto aparecieron los correos electrónicos basura, virus y otra cantidad de riesgos; con ello, el principio de extremo a extremo ha dado paso gradual a mecanismos de confianza por medio de los cuales, los agentes de confianza (proveedores de servicio de Internet - ISP), receptan los mensajes sustituyendo al receptor final.

Estos agentes (ISP) entonces, pueden eliminar información antes de que lleguen a los usuarios finales, pero, existiría la facultad de no entregar la información dañina únicamente, sino aquella que podría representar interés particular por parte de algún sector, o realizar la priorización de paquetes o de servicios.

Estos agentes (ISP) entonces, pueden eliminar información antes de que lleguen a los usuarios finales, pero, existiría la facultad de no entregar la información dañina únicamente, sino aquella que podría representar interés particular por parte de algún sector, o realizar la priorización de paquetes o de servicios, lo cual se aleja de una condición necesaria de una Internet libre y abierta (Marsden, 2012).

Conociendo que con las diferentes tecnologías y la propia arquitectura de Internet que sí es posible diferenciar los tipos de tráfico que circulan en esta red, los ISP juegan un papel fundamental ya que se encuentra en sus manos el poder de efectuar una diferenciación en este tipo de tráfico que podría ir en contra de la igualdad en Internet, de la libre expresión, generación de contenidos, etc.

Esto es lo que constituye la base para el debate que se halla en torno a este principio y que en lo siguiente se analiza de una manera más detallada.

1.3.2 Concepto

En lo que corresponde al concepto mismo de la “neutralidad de la red”, se puede decir que este principio tiene varias maneras de ser contextualizado, sin que se haya establecido un significado único; sin embargo, suele asociarse a los principios sobre el tratamiento del tráfico en las redes de Internet, esto es, que sea tratada con igualdad y de manera independiente de su naturaleza, origen, o destino (José Luis González San Juan, 2016).

A continuación, se mencionarán algunas definiciones efectuadas en torno a la neutralidad de la red:

Para (Wu, 2015), este principio se define como:

> Neutralidad de red se define como un principio de diseño de la misma red. La idea es que las redes de información pública deben de tratar todos los contenidos, todos los sitios y todas las plataformas por igual, esto permite a las redes transportar todo tipo de información y todo tipo de aplicaciones. Este principio sugiere que las redes de información aportan más valor cuando son menos complejas, cuando son una plataforma de múltiples usos, presentes y futuros.

La Comisión Interamericana de Derechos Humanos (CIDH), dentro del libro que corresponde al capítulo III del Informe Anual 2016 de la Relatoría Especial para la Libertad de Expresión de marzo de 2015 por la CIDH, reconoce a la neutralidad de la red como: "una condición necesaria para ejercer la libertad de expresión en internet en los términos del artículo 13 de la convención americana", siendo que este principio brinde la libertad de acceso y elección de los usuarios para el uso, envío, recepción de cualquier contenido legal por medio de Internet, sin que estas actividades se encuentren condicionadas de cualquier forma.

Se sostiene de igual manera en esta Relatoría que: "El principio de neutralidad es un principio de diseño de internet, por el cual se maximiza la utilidad de las redes, tratando a todos los "paquetes de datos" en forma igualitaria sin distinción alguna. de ahí que en internet se describa como una "red boba" cuya especialización se da en los extremos – el contenido o la aplicación se genera en un extremo, se traslada por la red en distintos paquetes, sin discriminación, y el contenido o la aplicación se rearma en el punto de destino."

Se sostiene de igual manera en esta Relatoría que:

> El principio de neutralidad es un principio de diseño de internet, por el cual se maximiza la utilidad de las Sin embargo, la Relatoría Especial para la Libertad de Expresión sostuvo en 2013 que este principio podría considerar excepciones, de tal modo que no debería haber discriminación alguna del tráfico en Internet "a menos que sea estrictamente necesario y proporcional para preservar la integridad y seguridad de la red; para prevenir la transmisión de contenidos no deseados por expresa solicitud –

libre y no incentivada– del usuario; y para gestionar temporal y excepcionalmente la congestión de la red. en este último caso, las medidas empleadas no deben discriminar entre tipos de aplicaciones o servicios (CIDH, 2013).

Adicionalmente, la Asociación GSM (GSMA), señala que esta expresión se emplea a menudo para hacer referencia a los problemas relacionados con la optimización del tráfico que se encuentra en la red de Internet; sostiene además que existen los defensores de la neutralidad de la red, quienes afirman la necesidad de establecer por ley que todo el tráfico que circule por la red deba recibir un tratamiento igualitario, mientras tanto, otros piensan que existiría una mejoría en la experiencia al usuario el hecho de ofrecer distintos niveles de servicio para distintas aplicaciones (GSMA, 2018).

1.4 Retos para la Neutralidad de Red (NR)

Con la popularización de la red de Internet y el aparecimiento del principio de la neutralidad de la red que aboga esencialmente como hemos visto de las concepciones precedentes, principalmente por un acceso a esta red sin restricción en cuanto al tráfico, se evidencia que dicho principio se relaciona con un conjunto de aspectos, tales como:

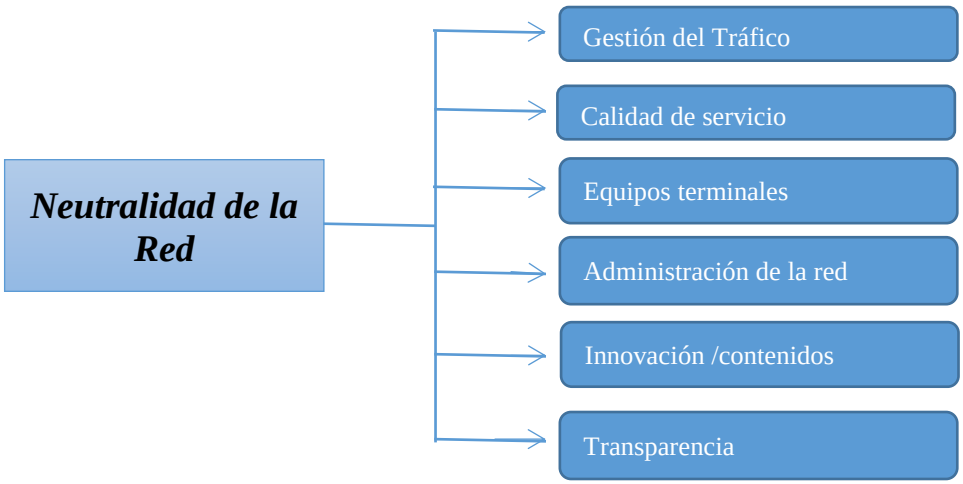

Figura 6: Elementos con los cuales se relaciona la neutralidad de la red

Fuente: (REGULATEL, 2015)

Así mismo, se puede indicar que la neutralidad en la red tiene en la mira fundamentalmente cuestiones de controversia que forman parte del debate actual que se detallará de mejor manera en el transcurso de esta sección:

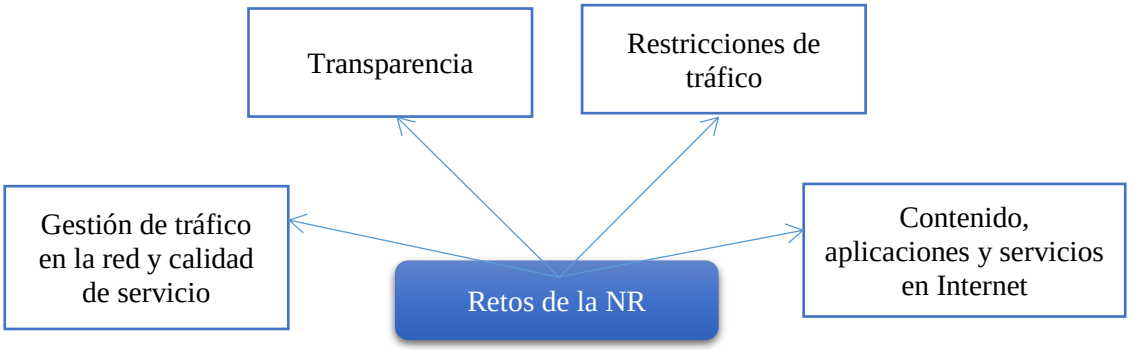

Figura 7: Retos de la neutralidad de la red

1.4.1 Gestión de tráfico la red y calidad de servicio

Con el creciente desarrollo de Internet se evidencia el incremento de tráfico, contando con una increíble cantidad de información correspondiente a servicios, datos, aplicaciones, información en general que exige preguntarse sobre la gestión de dicho tráfico que permita garantizar una experiencia con calidad en el momento de recepción por parte de los usuarios.

A diferencia de los inicios de Internet en donde no existían métodos sofisticados para gestionar el tráfico que circula por esta red, actualmente existen varias técnicas para ello; según lo explica Ruiz Gómez (2014) en su análisis de la competencia y neutralidad de la red, las formas de realizar esta gestión son de diferentes tipos:

- Diferenciación de paquetes que a su vez permite una calidad de servicio mínima para los usuarios finales.

- Diferenciación de rutas (encaminamiento IP) para evitar congestión en las mismas.

- Diferenciación por filtrado para distinción por parte de los proveedores de servicio de Internet del tráfico <<seguro>> del <<inseguro>>, con la finalidad de bloquear este último antes de ser entregado a su destino final.

- Además puede existir la diferenciación de carácter económico que se encuentran relacionadas con las tarifas de acceso a los recursos que son consumidos por los usuarios (Fundación Telefónica, 2011).

Con ello, uno de los aspectos de debate es acerca de las características de debe considerarse para realizar, en todo caso, una gestión del tráfico de circula en la red aceptable que, al mismo tiempo no perjudique la experiencia de los usuarios y mantenga a Internet con la característica de ser una red abierta.

1.4.2 Transparencia

En principio, los usuarios del servicio de Internet, así como de cualquier otro servicio que decidan contratar tienen el derecho de elegir libremente a su proveedor, así como conocer con exactitud las características de lo que reciben en cuanto a precios, calidad, posibles restricciones y demás.

En el Ecuador, por ejemplo, la LOT establece entre sus principios (Art. 4) que: "La provisión de los servicios públicos de telecomunicaciones responderá a los principios constitucionales de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad así como a los principios de solidaridad, no discriminación, privacidad, acceso universal, transparencia, objetividad, proporcionalidad, uso prioritario para impulsar y fomentar la sociedad de la información y el conocimiento, innovación, precios y tarifas equitativos orientados a costos, uso eficiente de la infraestructura y recursos escasos, neutralidad tecnológica, neutralidad de red y convergencia."; por lo que, se evidencia que la transparencia debe ser práctica en la prestación de los diferentes servicios de telecomunicaciones, incluyendo el de Acceso a Internet.

Adicionalmente, resulta importante mencionar que en la normativa que se deriva de la LOT, se establecen además condiciones que se enfocan a la neutralidad de la red y transparencia para la prestación de servicios a los usuarios; estas condiciones serán materia de análisis en acápites más adelante.

1.4.3 Restricciones de Tráfico

Las prácticas de bloqueo o restricciones en el tráfico compromete el hecho de que los usuarios finales reciban y generen información de forma libre.

La gestión sobre la red de Internet podría ser empleada para frenar algunos tipos de páginas o tráfico; un ejemplo puede constituir aquel relacionado con la ralentización del video de manera continua, degradando de esta forma la calidad de servicio que perciben los clientes.

Según el artículo de la Internet Society (ISOC) sobre perspectivas sobre el bloqueo del contenido en Internet, se señala que entre las motivaciones para el bloqueo de contenido que circula en la red se encuentra el bloqueo debido a políticas públicas que se utilizan para restringir el acceso a información que es ilegal en una jurisdicción determinada y que a su vez representa una amenaza para el orden público u objetable en audiencias particulares (Society, 2017).

El segundo de los motivos que plantea la ISOC sobre las motivaciones para bloqueo del tráfico que se encuentra en Internet es la de evitar o responder a las amenazas a la seguridad de la red que tienen que ver con ingreso de malware o tráfico malicioso a las redes, filtrado de correo electrónico con bloqueo de mensajes masivos no deseados e información maliciosa; la tercera motivación corresponde a la administración del uso de las redes que se relaciona con la administración en aspectos de tiempo, redes o anchos de banda, como por ejemplo ocurre en las restricciones para acceso a redes sociales por parte de las personas dentro de una organización o restricciones de contenido según las contrataciones realizadas por los usuarios.

1.4.4 Contenido, aplicaciones y servicios en Internet

En las épocas actuales, es innegable la <<infinita>> cantidad de información que se introduce y genera en la red de Internet, pero ¿Qué tipo de información es?, ¿La información es segura y legal?; al respecto es importante reflexionar que la red Internet puede albergar información de todo tipo: documentos, imágenes, videos, sonidos, información que en efecto, resulta dañina e ilegal etc.; bajo este contexto se han generado debates alrededor del mundo sobre cómo efectuar el control del mismo y en el caso de la neutralidad de la red, preguntarse acerca de la decisión de priorizar, discriminar y bloquear.

Con ello, el contenido, aplicaciones y servicios que circulan o se encuentran disponibles en Internet ha sido objeto de varios intentos de regulación en los últimos tiempos, sin llegar a una definición sobre ello hasta el momento; las causas principales para no lograr este cometido se han centrado en movimientos multitudinarios, además de la afectación propia que podría causarse a la Declaración Universal de los Derechos Humanos (en adelante DUDH), en cuyo artículo 19 se establece que: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión." (Naciones Unidas, 2015)

A continuación, se muestra en forma general cómo se encuentra la situación de restricciones de contenido en el mundo a través de la Figura 7:

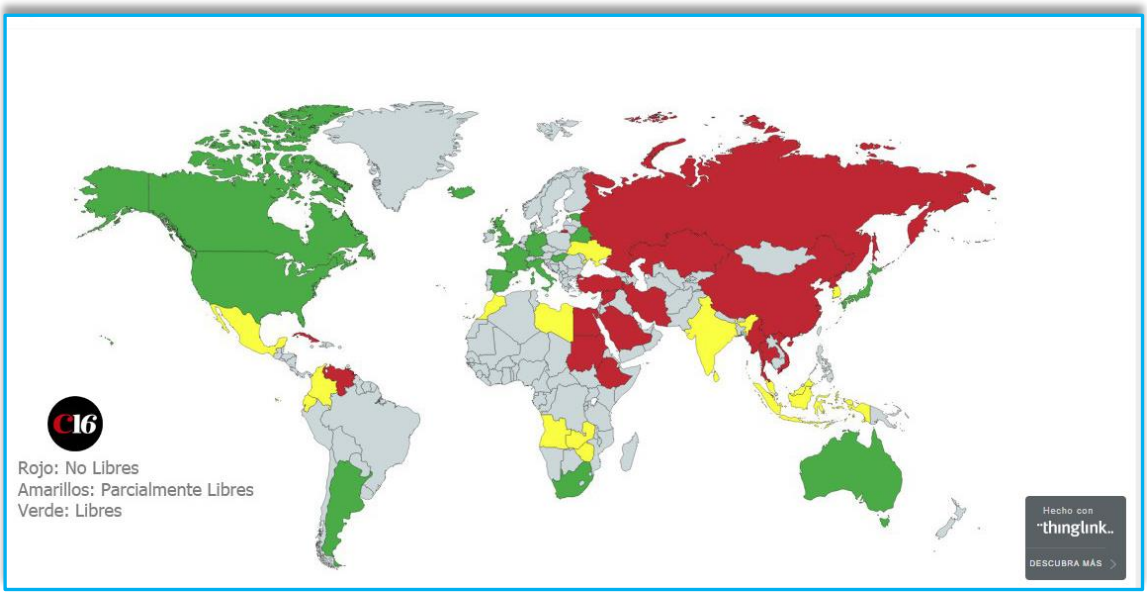

Figura 8: Censura en Internet - 2018

Fuente: (Cambio 16, 2018)

Tabla 3: Censura en Internet en el Mundo - Estadísticas

# Países que restringen / Continente	África	Asia	Europa	América
Torrent Sites (sitios web considerados peligrosos)	29	16	31	23
pornografía	6	5*	2	1
Noticias políticas	1	1	1	3
Medios sociales	1	3	2	2
(*). Incluye al conjunto de países Árabes -Musulmanes				

Fuente: (Cambio 16, 2018)

Como consecuencia, se puede concluir que no obstante que no existe normativa expresa para el contenido que existe en Internet, de acuerdo a sus características puede ser objeto de bloqueo o de alguna clase de restricción, sujeta a varios factores como los sociales, políticos que coexisten en la actual prestación del servicio de acceso a Internet.

2 ANÁLISIS DE LA NEUTRALIDAD DE RED

En esta parte se realizará el análisis de las diferentes posturas alrededor del mundo que se tienen en torno al principio de la neutralidad de la red, tomando en cuenta los criterios que se tiene en Ecuador, algunos países Latinoamericanos, en países de Norte América y la Unión Europea; además de realizar un vistazo a algunos casos relevantes en referencia a este tema en el mundo y razonamientos que existen por parte de organismos y empresas de telecomunicaciones frente a la neutralidad de la red, obteniendo finalmente los análisis comparativos de la aplicación de este principios evidenciando similitudes y diferencias.

2.1 Casos relevantes sobre la neutralidad de la red

Previo a efectuar el análisis de cómo se maneja la neutralidad de la red en diferentes países, a continuación se presenta una breve descripción de algunos casos relevantes que han ocurrido en la práctica sobre este controvertido tema.

2.1.1 Estados Unidos y Microsoft

Un caso que inició en 1998 y finalizó en el año 2002.

El tema fundamental se dio por cuanto los Estados Unidos demandó a Microsoft Corporation (“Microsoft”) por cuanto dicha corporación puso a la venta computadoras con un navegador web Internet Explorer, sosteniendo que esta acción limitaba el mercado de navegadores que debían ser comprados por los usuarios; en el juicio final se estableció que Microsoft desarrolle, distribuya, promocione, use, venda o licencie cualquier software que compita con el software de la plataforma de Microsoft y que las computadoras personales incluya un producto de sistema operativo Windows y un sistema operativo que no sea de Microsoft, ejerciendo cualquiera de las opciones dadas en juicio final (Departamento de Justicia de EE.UU., 2002).

2.1.2 Madison River y Vonage

Sucedido hacia el año 2005, Madison River como una empresa que brinda servicios de Internet en el sureste medio este de EE.UU y la empresa Vonage como un proveedor de aplicaciones en Internet (IAP) de servicios de voz sobre Internet (VoIP); Vonage reclamó ante la Comisión Federal de Comunicaciones (FCC) que Madison River bloqueaba de manera reiterada el acceso a los usuarios a sus servicios. Luego de llevarse a cabo las investigaciones, se llegó a un acuerdo por el cual Madison River cesó el bloqueo al uso de estas aplicaciones. (Reicher, 2011)

2.1.3 Comcast y FCC

Sucedido en el año 2018. La FCC sancionó a Comcast por haber comprobado el bloqueo de tráfico de algunos clientes que utilizaban aplicaciones p2p de intercambio de archivos entre particulares. Comcast defendía su postura bajo el precepto de que intentaba gestionar el tráfico en sus redes para evitar deterioros para la mayor parte de usuarios (Reicher, 2011).

Con el desarrollo de estas investigaciones se llega a que Comcast habría indicado que modificaría sus prácticas de gestión para que todo el tráfico de Internet sea tratado con igualdad; sin embargo había solicitado a un tribunal de apelación la revisión sobre si la FCC tenía competencia para imponer restricciones en la gestión de las redes, ante lo cual el Tribunal estadounidense de apelaciones señaló que la FCC no consiguió demostrar aquello, siendo este caso considerado un revés para la neutralidad de la red (Reuters, 2010).

Con el desarrollo de estas investigaciones se llega a que Comcast habría indicado que modificaría sus prácticas de gestión para que todo el tráfico de Internet sea tratado con igualdad; sin embargo había solicitado a un tribunal de apelación la revisión sobre si la FCC tenía competencia para imponer restricciones en la gestión de las redes, ante lo cual el Tribunal estadounidense de apelaciones señaló que la FCC no consiguió demostrar aquello, siendo este caso considerado un revés para la neutralidad de la red.

Con base en lo ocurrido, en el año 2010, la FCC adoptó normas para un Internet abierto (Open Internet Rules), que son:

- Transparencia: obligando a todos los ISPs a divulgar públicamente información sobre sus prácticas de gestión en la red, rendimiento y los términos comerciales de sus servicios de Internet de banda ancha, con el objetivo de que los consumidores puedan tomar decisiones informadas sobre el uso de esos servicios.

- No bloqueo: por parte de los ISPs de contenido legal, aplicaciones, servicios o equipos no dañinos para la red, sujeto a términos que sean razonables para la gestión de red.

- No discriminación: no discriminar injustificadamente en la transmisión de tráfico de red legal a través de acceso a Internet de banda ancha de un consumidor; la gestión razonable de la red no constituye una discriminación irrazonable. (Reicher, 2011)

2.1.4 Voissnet y Telefónica

Esencialmente, Voissnet acusó a Telefónica de impedirle el paso de voz por Internet; Telefónica argumentó que Voissnet usó sus redes para ofertar servicios de voz sobre Internet, por lo cual la empresa española tendría derecho a recibir una remuneración por esta utilización; en el año 2007, la Corte Suprema prohibió a Telefónica adoptar cualquier técnica de bloqueo o degradación de servicio a los usuarios de servicios de telefonía sobre Internet (Espinoza & González, 2015).

2.2 La neutralidad de la red en el Ecuador

Como se indicó en el desarrollo inicial de este trabajo, la Constitución de la República del Ecuador estableció en su artículo 313 a los sectores estratégicos, entre ellos al de las telecomunicaciones; en este sentido, la regulación para los sectores estratégicos en el país se encuentra regida por la Pirámide de Kelsen (Figura 8), con la prevalencia de las normas jurídicas y principios de jerarquías.

Figura 9: Pirámide de Kelsen – Normas Jurídicas en Ecuador

Fuente: (Asamblea Nacional, 2008)

Es de resaltar que el artículo 424 de la Carta Magna establece claramente que: "la constitución y los tratados internacionales de derechos humanos ratificados por el estado que reconozcan derechos más favorables a los contenidos en la constitución, prevalecerán sobre cualquier otra norma jurídica o acto del poder público" y, el artículo 425 señala en relación al orden jerárquico de aplicación de normas, que los tratados y convenios internacionales se encuentra por encima de "las leyes orgánicas; las leyes ordinarias; las normas regionales y las ordenanzas distritales; los decretos y reglamentos; las ordenanzas; los acuerdos y las resoluciones; y los demás actos y decisiones de los poderes públicos", siendo que cualquier conflicto entre normas se resolverá mediante la aplicación de la norma jerárquicamente superior (Asamblea Nacional, 2008).

2.2.1 Tratados y convenios internacionales

Con fundamento en el concepto que se ha rescatado de diferentes autores sobre el principio de la neutralidad de la red y lo establecido en la Constitución de la República del Ecuador, se esbozará a continuación la normativa internacional principal relacionada con el mencionado principio en función de organismos internacionales del cual es miembro:

- Comisión Interamericana de Derechos Humanos (CIDH)

  La CIDH es un órgano principal y autónomo de la Organización de los Estados Americanos (OEA) y se encarga de la promoción y protección de los derechos humanos en el continente americano.

  En el año 2014, a través de la Declaración Conjunta sobre universalidad y el derecho a la libertad de expresión, se establece que: "Los Estados deberían promover activamente el acceso universal a Internet sin distinción política, social, económica o cultural, entre otras cosas, respetando los principios de neutralidad de la red y el carácter central de los derechos humanos para el desarrollo de Internet."

  Por lo que se evidencia la necesidad de garantizar el principio de la neutralidad de la red a todos los estados miembros, entre otras cosas también para promover el uso de Internet como una forma de comunicación (CIDH C. I., 2014).

  Por otra parte, la Convención Americana sobre Derechos Humanos (Suscrita en San José de Costa Rica el 22 de noviembre de 1969, en la Conferencia Especializada Interamericana sobre Derechos Humanos), conviene a los países miembros, entre otras cosas en su artículo 13 al derecho de la libertad de pensamiento y de expresión y comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole por cualquier procedimiento a elección. También en el mismo artículo se prohíbe por ley cualquier propaganda en favor de la guerra y toda apología de odio y acciones ilegales contra cualquier persona o grupo de personas (CIDH C. I., 1969).

- Pacto Internacional de Derechos Civiles y Políticos (PIDCP)

  Este "Pacto" cuenta con 168 países miembros, entre ellos el Ecuador; dentro de su articulado se establece el número 13 que refiere a que toda persona tiene derecho a la libertad de expresión de forma muy parecida a la Convención Americana sobre Derechos Humanos.

Asimismo, se especifica en su artículo 19 que el ejercicio del derecho a la libertad de expresión entraña deberes y responsabilidades especiales, de tal modo que, puede estar sujeto a restricciones que deben estar fijadas por ley para: a) "Asegurar el respeto a los derechos o a la reputación de los demás" y b) "La protección de la seguridad nacional, el orden público o la salud o la moral públicas." (Comisión Presidencial, 2011)

- Comunidad Andina de Naciones (CAN)

La Decisión 638, promulgada el 19 de julio de 2006 en Perú para los países miembros de la CAN, entre ellos Ecuador, establece ciertos lineamientos que son aplicables con la neutralidad de la red como que, los países miembros deben proteger a través de sus propias normativas internas la protección a los derechos de los usuarios tales como: el acceso a la prestación continua de los diferentes servicios de telecomunicaciones conforme normas de calidad establecidas por quien desempeñe el papel de autoridad competente; el trato igualitario y no discriminatorio en relación con el acceso, calidad y costos de los servicios; conocimiento de información veraz, suficiente y precisa sobre os servicios contratados.

2.2.2 Ley Orgánica de Telecomunicaciones y Código de Ingenios

Continuando con la aplicación de la normativa según nuestra pirámide de Kelsen se encuentra el análisis de las leyes orgánicas; de esta forma es de indicar que con fecha 18 de febrero de 2015 y Registro Oficial N° 439, el Pleno de la Asamblea Nacional de la República del Ecuador expidió la Ley Orgánica de Telecomunicaciones (LOT).

De este modo, se identifica que el principio de la neutralidad de la red se encuentra referida en la mencionada Ley dentro de los objetivos (Art. 3) y principios (Art. 4 y 66); de igual manera, el numeral 18 del artículo 22 establece como uno de los derechos de los abonados, clientes y usuarios:

A acceder a cualquier aplicación o servicio permitido disponible en la red de internet. Los prestadores no podrán limitar, bloquear, interferir, discriminar, entorpecer ni

> restringir el derecho de sus usuarios o abonados a utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, desarrollo o servicio legal a través de internet o en general de sus redes u otras tecnologías de la información y las comunicaciones, ni podrán limitar el derecho de un usuario o abonado a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales.

No obstante, a continuación este mismo numeral reconoce la capacidad que tiene el prestador para una gestión y se señala:

> Se exceptúan aquellos casos en los que el cliente, abonado o usuario solicite de manera previa su decisión expresa de limitación o bloqueo de contenidos, aplicaciones, desarrollos o servicios disponibles, o por disposición de autoridad competente, los prestadores pueden implementar las acciones técnicas que consideren necesarias para la adecuada administración de la red en el exclusivo ámbito de las actividades que le fueron habilitadas, para efectos de garantizar el servicio.

Por otra parte, el artículo 24 sobre las obligaciones que se establecen para los prestadores de servicios de telecomunicaciones, contiene como deber el numeral 17 que señala:

> No limitar, bloquear, interferir, discriminar, entorpecer, priorizar ni restringir el derecho de sus usuarios o abonados a utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, desarrollo o servicio legal a través de internet o en general de sus redes u otras tecnologías de la información y las comunicaciones, ni podrán limitar el derecho de un usuario o abonado a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales, salvo las excepciones establecidas en la normativa vigente;

Y a continuación:

> Se exceptúa aquellos casos en los que el cliente, abonado o usuario solicite de manera previa su decisión expresa de limitación o bloqueo de contenidos, o por disposición de autoridad competente. los prestadores pueden implementar las acciones técnicas que consideren necesarias para la adecuada administración de la red en el exclusivo ámbito de las actividades que le fueron habilitadas para efectos de garantizar el servicio.

Del mismo modo, el numeral 1 del artículo 64 establece que: “Los prestadores de los servicios podrán establecer planes tarifarios constituidos por uno o varios servicios o por uno o varios productos de un servicio, de conformidad con su o sus títulos habilitantes.”

Finalmente, se puede mencionar lo establecido en el Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación, más conocido como "Código de Ingenios", el cual fue emitido por la Asamblea Nacional el 01 de diciembre de 2016; el artículo 39 del Capítulo II correspondiente al acceso y soberanía del conocimiento en entornos digitales e informáticos señala:

> Art. 39.- acceso universal, libre y seguro al conocimiento en entornos digitales (…)
>
> El estado generará las condiciones necesarias para garantizar progresivamente la universalización del acceso a las tecnologías de la información y comunicación, priorizando el uso de tecnologías libres, bajo los principios de: soberanía tecnológica, seguridad, neutralidad de la red, acceso libre y sin restricciones a la información y precautelando la privacidad. estas condiciones serán respetadas sin perjuicio del proveedor del servicio. los organismos de control competentes vigilarán que se cumplan con estas condiciones.

2.3 Regulación internacional sobre el principio de neutralidad de red

Con la expedición de varias normativas internacionales que albergan el tratamiento de la neutralidad de la red, se evidencia que a nivel mundial y varios países se han generado foros, debates y discusiones normativas en torno a la aplicación de este principio sobre Internet; no obstante, la generación de las normativas propias de cada país, se encuentra con frecuencia que el Internet se define como un servicio de valor agregado, de información o de acceso a Internet, siendo que tiene un tratamiento diferente al de las redes fijas y móviles en las cuales se soporta, lo cual permitiría de alguna manera su exponencial desarrollo; sin embargo, se tomará en cuenta que los recientes cambios en los Estados Unidos han permitido que el Internet sea tratado como un servicio de telecomunicaciones (Rezende-Mediatelecom, 2018).

En lo subsiguiente se podrá identificar que las regulaciones han incorporado además de aspectos relacionados con la gestión de tráfico, temas sobre transparencia de información hacia el usuario, protección de datos, calidad de servicio. Iniciaremos con las regulaciones en algunos países de Latinoamérica luego de haber analizado la situación que actualmente se tiene en Ecuador; seguido, se analizará principalmente las iniciativas en países de Norte América y en la Unión Europea.

2.3.1 Chile (América latina)

Chile es considerado el primer país en el mundo que ha promulgado una legislación que consagra expresamente el principio de neutralidad de la red, con la denominada Ley 20.453 (Anexo 6), que se conoce como <<Ley de neutralidad en la red>> y fue promulgada el 18 de agosto de 2010 (Subsecretaría de Telecomunicaciones - SUBTEL, 2010) y modificó la Ley General de Telecomunicaciones referidos a los derechos de los usuarios en el uso del Internet, así como las obligaciones de los proveedores de servicios de Internet; esta Ley fue complementada con un reglamento(Anexo 7) que fue expedido el 15 de diciembre de 2010 (Subsecretaria de Telecomunicaciones - SUBTEL, 2010).

Estadísticas en síntesis

De acuerdo a las estadísticas de la Subsecretaría de Telecomunicaciones (SUBTEL) al año 2015, el acceso fijo a la red de Internet es más importante que el acceso móvil y se muestra según la Tabla siguiente:

Tabla 4: Acceso a Internet por tipo de conexión - Chile

Tipo de conexión	2015
Banda ancha fija / Wifi	56,0%
Banda ancha móvil	8,3%
Teléfono móvil o Smartphone con acceso propio a Internet	34,8%
Tablet con acceso propio a Internet	0,4%
Conexión satelital	0,5%

Fuente: (Latina & Intervozes, 2017)

Asimismo, las empresas ISP que participaban en el mercado hasta el año 2014, según información de la SUBTEL, se dividen en ISP dedicados a brindar conexión de característica residencial (22), conexiones de carácter móvil (9), orientados a empresas (15) y a entregar conexión internacional (2). Los grupos económicos más importantes en Chile hasta el 2016 que proveen el acceso a Internet, se concentran en: Grupo VTR (37,4%), Grupo Movistar (36,7%), Grupo Claro (12,2%) y otros (13,7%) (Latina & Intervozes, 2017).

Regulación de la neutralidad de la red

La Ley se generó en función de una moción parlamentaria de fecha 20 de marzo de 2007, con la pretensión de agregar tres artículos a la Ley N° 19.496 referente a la protección del consumidor; luego de los debates ocurridos, el proyecto de Ley fue aprobado por la Cámara el 11 de octubre de 2007 contando con 66 votos a favor, 0 en contra y 2 abstenciones.

Posteriormente, esta Ley fue presentada en modificación en el año 2008, retornando a la Cámara de Diputados y nuevamente aprobada, de tal manera que fue oficializada finalmente por el presidente Sebastián Piñera el 18 de agosto de 2010 y publicada en Diario Oficial el 26 de agosto del mismo año (Wikypedia, 2016).

La ley promulgada en Chile basa su contenido principalmente en los siguientes principios, según informe de Ex Subsecretario de Telecomunicaciones de la SUBTEL (Huichalaf, 2015):

- Transparencia: Obligación a los ISP de publicar en sus sitios web información detallada de sus planes de contratación de servicios, velocidad de subida y bajada, límite de descargas, medidas de control de tráfico y otras características del servicio.

- No bloqueo de Contenidos y Aplicaciones: Se permite la administración inteligente de la red, siempre y cuando las medidas de gestión de tráfico estén claramente especificadas en la oferta comercial de las compañías y no afecten la libre competencia; la ley garantiza el derecho a acceder libremente a cualquier tipo de contenido o aplicación, sin que el proveedor pueda negar o dificultar dicho acceso.

- Indicadores de calidad: Los ISP deben realizar mediciones de los indicadores técnicos de calidad de sus servicios de acuerdo a protocolos aprobados por la SUBTEL.

A su vez, la aplicación de estos principios derivaron en obligaciones para los ISP, reformando a Ley General de Telecomunicaciones a través de la inclusión de un nuevo artículo 24H:

- No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red.

- No podrán limitar el derecho de un usuario a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y que los mismos no dañen o perjudiquen la red o la calidad del servicio.

- Deberán ofrecer, a expensas de los usuarios que lo soliciten, servicios de controles parentales para contenidos que atenten contra la ley, la moral o las buenas costumbres, siempre y cuando el usuario reciba información por adelantado y de manera clara y precisa respecto del alcance de tales servicios.

Adicionalmente, la Ley le brinda facultad a la SUBTEL para sancionar las infracciones cometidas en relación a la aplicación de las obligaciones de implementación y funcionamiento de las directrices emitidas en relación a la neutralidad de la red.

Por su parte, la implementación de las obligaciones establecidas en la Ley de Telecomunicaciones se encuentran plasmadas en reglamento emitido mediante Decreto N° 368 del Ministerio de Transporte y Telecomunicaciones; en el mismo, se regula las características y condiciones de la neutralidad de la red para el servicio de acceso a Internet, definiendo conceptos de acceso a Internet y procedimientos técnicos que los ISP deben efectuar para realizar la medición de calidad de sus servicios y la publicación de los resultados obtenidos.

El artículo 8 de este reglamento describe como prácticas restrictivas al uso de contenidos, aplicaciones o servicios que se brinden sobre Internet y sujetas a sanción, las siguientes:

1) Toda aquella acción que, arbitrariamente, tienda a bloquear, interferir, entorpecer, restringir y/o de cualquier forma obstaculizar el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red, en especial, aquellas medidas de gestión de tráfico o administración de red que, en aquel carácter, afecten a los niveles de servicio contratados por el respectivo usuario.

2) Toda aquella acción que, arbitrariamente, tienda a priorizar o discriminar entre proveedores de contenidos, aplicaciones y/o usuarios. En todo caso, siempre se entenderá como arbitraria la acción de priorización o discriminación que afecte a proveedores de contenidos, aplicaciones y/o usuarios respecto de otros de similar naturaleza.

3) Toda aquella acción que impida o restrinja el derecho de los usuarios a acceder a la información veraz y actualizada relativa a las características de los servicios de acceso a Internet ofrecidos o contratados, según sea el caso, a que se refiere el artículo 5º del presente reglamento.

4) Toda aquella acción que impida, restrinja o limite el derecho de los usuarios a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y no dañen o perjudiquen la red o la calidad del servicio prestado a terceros.

Finalmente, el artículo 12 del reglamento establece que los usuarios pueden utilizar los mecanismos de reclamo señalados en el artículo 28 de la Ley y Reglamento para Tramitación y Resolución de Reclamos de Servicios de Telecomunicaciones, en el caso de incumplimiento de las obligaciones ya señaladas; de este último aspecto cabe resaltar que hasta el año 2015, se habrían establecido hasta 40 cargos por inobservancias a la normativa sobre neutralidad de la red (Huichalaf, 2015):

2.3.2 Colombia (América Latina)

En el presente apartado, se realiza una revisión sobre el tratamiento de la neutralidad de la red en Colombia; más adelante se detallará que en este país, este principio se encuentra previsto en ley y reglamentado a través de una resolución.

Estadísticas en síntesis

De manera general, se puede indicar que de acuerdo al Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) hasta el año 2017 casi el 60% de la población era usuaria de Internet y el un tercio de las residencias se encontraron conectadas.

Según datos del Boletín Trimestral de las TIC con cifras del Primer Trimestre del 2018 publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), se india que al finalizar el primer trimestre de 2018, el país alcanzó un total de 30,41 millones de Conexiones a Internet de Banda Ancha, de las cuales, 16,5 millones se realizaron mediante la modalidad de suscripción a redes fijas y móviles, y 13,9 millones, a través de conexiones móviles por demanda.

De igual manera, las mismas estadísticas señalan que en el primer trimestre del año 2018, el índice de penetración de las conexiones a Internet de Banda Ancha en Colombia aumentó 3,4 puntos porcentuales con relación al mismo periodo del 2017, alcanzando un 61,0% (MINTIC, 2018).

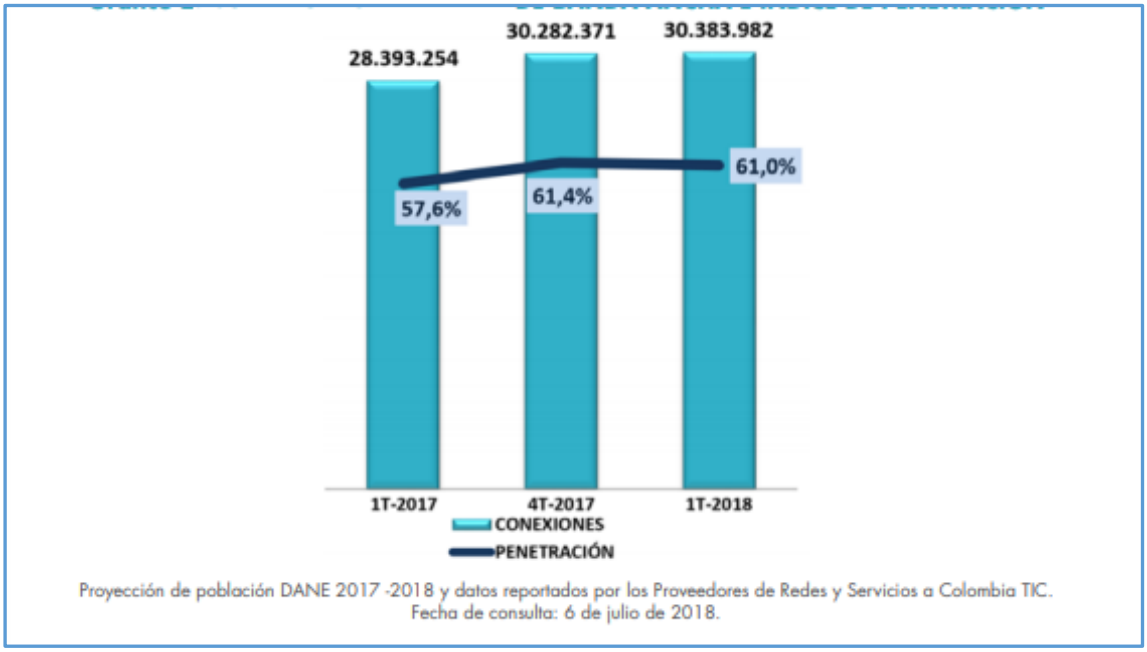

Figura 10: Conexiones a Internet de Banda ancha e índice de penetración - Colombia

Fuente: (MINTIC, 2018)

Regulación de la neutralidad de la red

La neutralidad de la red en Colombia se encuentra contenida en la Ley 1450 del año 2011 (Anexo 8), que fue aprobada por el Congreso de la República de ese país y complementada con la reglamentación a dicha Ley emitida con Resolución N° 3502 del año 2011, elaborada por la Comisión de Regulación de las Comunicaciones (CRC).

De esta forma, el artículo 56 de la Ley 1450 establece con relación a la neutralidad de la red, las siguientes prohibiciones:

> [...] no podrán bloquear, interferir, discriminar, ni restringir el derecho de cualquier usuario de internet, para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio lícito a través de internet. En este sentido, deberán ofrecer a cada usuario un servicio de acceso a internet o de conectividad, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de estos. Los prestadores del servicio de internet podrán hacer ofertas según las necesidades de los segmentos de mercado o de sus usuarios de acuerdo con sus perfiles de uso y consumo, lo cual no se entenderá como discriminación (...).

Se establece de igual manera en esta sección que los usuarios pueden utilizar cualquier dispositivo que sea legal, que permita además un control de restricción para contenidos que se encuentran en contra de la legislación vigente.

Con relación a los ISP, la normativa colombiana señala mecanismos de transparencia hacia los usuarios; es decir, los proveedores deben publicar información sobre el servicio ofrecido con velocidades, calidad de servicio y garantías del servicio, además de la obligación de implementar mecanismos para preservar la privacidad de los usuarios contra invasiones y robo de datos a través de mecanismos de seguridad de red.

Adicionalmente, los usuarios pueden solicitar de manera expresa si desean que los contenidos, contenidos, aplicaciones o servicios sean bloqueados.

Finalmente, la ley colombiana estableció que la Comisión de Regulación de las Comunicaciones (CRC) en los próximos seis meses de promulgada establecería la reglamentación de lo establecido en la ley, esto incluyendo los procedimientos para aplicación del principio de la neutralidad de la red; al respecto, la CRC lanzó en el mes de septiembre del año 2011 el documento denominado "Documento de consulta pública sobre la Neutralidad en Internet", sobre lo cual y en base al conjunto de opiniones recibidas en debate, en octubre de 2011, la CRC publicó para consulta pública un nuevo documento titulado "Neutralidad en Internet".

Los resultados de esta consulta pública influyeron en la promulgación de la resolución 3502 en diciembre del año 2011, de tal forma, se reglamentó el artículo 56 de la Ley 1450 a través del ítem 3.2 del Capítulo I de Cuestiones Generales, artículos 7 y 8 del Capítulo II de Aspectos Técnicos y en el artículo 9 del Capítulo III de Informaciones a los usuarios.

El artículo 7 estipula que "los proveedores de redes y servicios de telecomunicaciones que prestan el servicio de acceso a internet podrán implementar medidas de gestión de tráfico que sean razonables y no discriminatorias respecto de algún proveedor, servicio, contenido o protocolo específico".

Y, en cuanto a las prácticas de gestión de tráfico se establecen las siguientes opciones: 1. Reducir o mitigar los efectos de la congestión sobre la red., 2. Asegurar la seguridad e

integridad de las redes... 3. Asegurar la calidad del servicio a los usuarios., 4. Priorizar tipos o clases genéricas de tráfico en función de los requisitos de calidad de servicio (QoS) propias de dicho tráfico, tales como latencia y retardo de los mismos y 5. Proporcionar servicios o capacidades de acuerdo con la elección de los usuarios, que atiendan los requisitos técnicos, estándares o mejores prácticas adoptadas por iniciativas de gobernanza de Internet u organizaciones de estandarización.

El artículo 8 por su parte dispone con relación a la priorización de tráfico que los proveedores "no pueden llevar al cabo conductas de priorización, degradación o bloqueo que contraríen lo previsto en la presente resolución"; no obstante, el numeral 3.4 del artículo 3 en esta resolución señala que: "los proveedores de redes y servicios de telecomunicaciones que prestan el servicio de acceso a Internet podrán hacer ofertas según las necesidades de los segmentos de mercado o de sus usuarios de acuerdo con sus perfiles de uso y consumo, lo cual no se entenderá como discriminación".

El artículo 56 de la Ley 1450 permite a los proveedores la creación de planes específicos para segmentos de mercado, sin que se haya establecido que ello signifique discriminación. Con ello, el artículo 9 de la resolución sostiene que:

(…) En todo caso, los proveedores de redes y servicios de telecomunicaciones deberán siempre poner a disposición de sus usuarios, una alternativa o plan tarifario que no contemple limitación alguna respecto de los servicios, contenidos o aplicaciones a los cuales puede acceder el usuario. En esta medida, dicha alternativa deberá ofrecer condiciones equivalentes en todos los demás aspectos al plan con limitaciones respecto del tipo de contenidos, aplicaciones o servicios a los cuales puede acceder el usuario.

2.3.3 Brasil (América Latina)

De manera general, se puede indicar que en Brasil la neutralidad de la red se encuentra amparada en la Ley Marco Civil de la Internet, más específicamente en su artículo 9 que será detallado más adelante; según el estudio de la Neutralidad de red en América Latina (Latina & Intervozes, 2017), hasta el año 2017 se habrían tramitado en el parlamento brasileño más de cincuenta Proyectos de Ley, de los cuales muchos de ellos podrían haber afectado la libertad de expresión en la red, privacidad y fortalecido mecanismos de

bloqueo yendo en contra de los preceptos de lo que plantea el principio de la neutralidad de la red.

Estadísticas en síntesis

De acuerdo al portal de estadísticas Statista, el número de usuarios de Internet en Brasil que cuenta con una población aproximada de 209.288.278 hasta el año 2017, entre los años 2013 a 2018 ha aumentado de 99,2 millones a 125,9 millones de internautas, y se prevé que al 2019 se llegará a 128,5 millones. (Statista, 2018)

A continuación, en la tabla siguiente se muestran algunas estadísticas relacionadas con el acceso a Internet:

Tabla 5: Situación del acceso a Internet – Estadísticas Brasil al 2016

Ítem	Cantidad
Abonados banda ancha fija c/100 habitantes	11,7%
Abonados a Internet Fija	26.752.564
Abonados a banda ancha móvil c/100 habitantes	51.6%
Banda ancha considerando una velocidad igual o mayor que 256 kbit/s	

Fuente: (Knoema, 2018)

En lo que se refiere a las empresas que ofrecen el acceso a Internet a través de conexiones fijas, en base a las estadísticas de la Agencia Nacional de Telecomunicaciones (ANATEL) se tiene los siguientes datos por cantidad de accesos al mes de marzo de 2017: Telecom Américas (31,57%), Telefónica (27,595), Oi (23,62%) y demás operadores (17,22%); adicionalmente, en Brasil de manera similar a otros países en el mundo es el equipo más utilizado para acceder a Internet, es decir, alrededor de 98 millones de brasileños que tienen de 10 años para adelante son usuarios de Internet a través de este medio, lo cual correspondería al 56% de la población.

Adicionalmente, el servicio de conexión móvil es ofrecido por empresas privadas, siendo liderado por Vivo (30,2%), Tim (26%), Claro (24,7%) y Oi (13,3%), con más del 98% de accesos (Latina & Intervozes, 2017).

Regulación de la neutralidad de la red

Brasil incorpora el principio de la neutralidad de la red recientemente en abril del año 2014 a través de la expedición del denominado Marco Civil de Internet (MCI), ley 12.695 (Anexo 9) que regula los aspectos técnicos y civiles de la red de Internet; brevemente es de señalar que el origen de esta propuesta data del año 2009, año en el cual se lanzó en este país un proceso de consulta sobre la forma de crear un marco regulatorio de Internet y para el cual habría participado gran parte de la sociedad civil, con ello y hasta su aprobación se generaron un total de siete audiencias públicas y varios seminarios en varias regiones del país (Carboni & Labate, 2018).

Dentro del Marco Civil de Internet, el artículo 9 del Capítulo III y Sección I (De la Neutralidad de la Red), establece que: "El responsable por la transmisión, conmutación o enrutamiento tiene el deber de tratar de forma isonómica cualquier paquete de datos, sin distinción por contenido, origen y destino, servicio, terminal o aplicación"; se prevé dos posibilidades de rompimiento de este principio: (1) por requisitos técnicos indispensables para la prestación adecuada de los servicios y aplicaciones; y (2) priorización de servicios de emergencia.

Constituye de igual manera obligación de la operadora de informar "previamente de modo transparente, de forma clara y suficientemente descriptiva a sus usuarios sobre las prácticas de gestión y mitigación de tráfico adoptadas, incluso las vinculadas a la seguridad de la red".

Posteriormente a la entrada en vigencia del MCI, se publica el Decreto Presidencial N° 8.771/2016 que reglamenta el Marco y señala e sus artículos 3 al 9 que el carácter excepcional de discriminación de tráfico que "solamente podrán resultar de requisitos técnicos indispensables a la prestación adecuada de servicios y aplicaciones o de la priorización de servicios de emergencia"; de ello, el Decreto describe a los requisitos técnicos indispensables, como: "I - tratamiento de cuestiones de seguridad de redes, tales como restricción al envío de mensajes en masa (spam) y control de ataques de negación de servicio; y II - tratamiento de situaciones excepcionales de congestionamiento de redes, tales como rutas alternativas en casos de interrupciones de la ruta principal y en situaciones de emergencia."

Se permite además la gestión de la red “con el objetivo de preservar sus estabilidad, seguridad y funcionalidad”.

Por su parte, el artículo 7 del Decreto establece los lineamientos de la relación con el usuario final para garantizar el principio de transparencia previsto en el MCI, señalando así que los contratos de prestación de servicios y los sitios web deben informar de manera clara las eventuales prácticas de degradación o discriminación de tráfico, motivaciones y efectos; en el MCI, los servicios de emergencia que pueden beneficiarse de una priorización de tráfico son: (I) comunicaciones destinadas a los prestadores de los servicios de emergencia, o comunicación entre ellos, como está previsto en la reglamentación de la Agencia Nacional de Telecomunicaciones - Anatel; o (II) - comunicaciones necesarias para informar la población en situaciones de riesgo de desastre, de emergencia o de estado de calamidad pública.

Finalmente, el Decreto buscó establecer reglas entre el responsable de transmisión, conmutación y enrutamiento y el proveedor de aplicaciones en Internet, indicando que las relaciones entre ellos no pueden comprometer “el carácter público e irrestricto del acceso a la Internet”, “priorizar paquetes de datos en razón de arreglos comerciales” y el hecho de privilegiar aplicaciones propias del operador. (Latina & Intervozes, 2017)

2.3.4 Perú (América Latina)

La evolución de la regulación en el Perú tuvo sus inicios a finales del año 1999, cuando Telefónica habría denunciado ante el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) supuestos actos de competencia desleal que habría adoptado la Red Científica Peruana (RCP) al comercializar un dispositivo (Aplio) que permitía a los clientes de Telefónica que se encontraban suscritos al servicio de acceso a Internet de la RCP realizar llamadas de larga distancia internacional (LDI) a través de Internet sin que la RCP cuente con la concesión respectiva para ello; al final, la denuncia fue desestimada por cuanto se consideró por parte del Cuerpo Colegiado Ordinario de OSIPTEL que los usuarios de Telefónica tienen la libertad para determinar la forma de su uso con Internet.

En función de lo ocurrido, la decisión tomada por la OSIPTEL permitió hacer factible el desarrollar normativa para el manejo de las conexiones a Internet (Rodríguez, Neutralidad de Red en Perú: Una Retrospectiva, 2017).

Estadísticas en síntesis

El Reporte Digital 2018 (Global Digital, 2018) señala que a inicios del año 2018 el total de la población en Perú es de 32,36 millones de personas, de las cuales 22 millones han utilizado Internet, lo cual significa una penetración del servicio del 68%, un 10% más que en enero del año 2017.

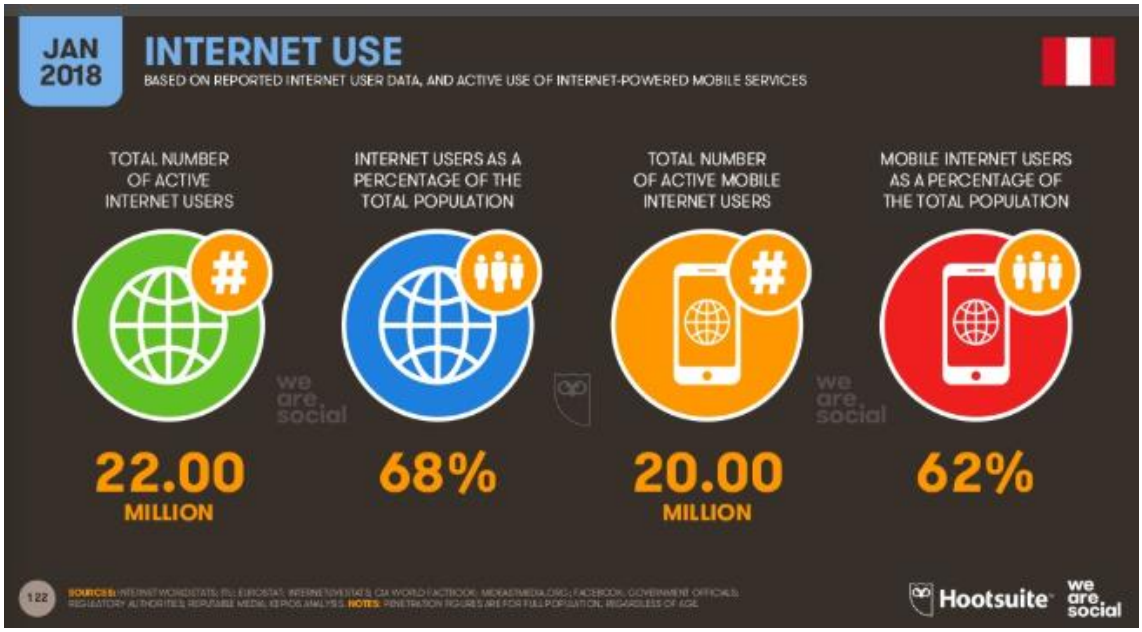

Figura 11: Estadísticas de uso de Internet en Perú

Fuente: (Global Digital, 2018)

De acuerdo al Instituto Nacional de Estadística e Informática (INEI) se determina que el 48,7% de la población con una edad igual o mayor a 6 años tiene acceso a Internet; según el lugar de residencia, en el área urbana, el 58,2% de la población usa Internet y en el área rural el 15,4% y en cuanto del acceso a Internet por tecnología, se concluye que del total de la población, el 32% los hace desde el teléfono celular, 11,5% desde su hogar y el porcentaje restante desde otros lugares (Gestión, 2018).

Adicionalmente, el mercado de la banda ancha fija, se encuentra distribuido de la siguiente manera:

Operador	Propietario	Tecnologia	% de mercado
Claro	América Móvil	HFC	20,4
Entel	Entel Chile	Inalambrica	0,4
Telefónica	Telefónica	xDSL / HFC	76,9
Otros	N/A	N/A	2,3

Figura 12: Perú - Operadoras de Banda Ancha

Fuente: (TeleSemana, Panorama de mercado, 2018)

Regulación de la neutralidad de la red

El Reglamento de Neutralidad de la Red de Perú, emitido en el año 2016 y que entró en vigencia a partir del 01 de enero de 2017 (Anexo 10), establece como objetivos, el establecimiento de disposiciones necesarias para asegurar el cumplimiento de las disposiciones establecidas dentro de la normativa que promueve la banda ancha, así como los principios y medidas que se deben adoptar para garantizar el principio de la neutralidad de la red.

El Reglamento se aplica para todos los proveedores del servicio de acceso a Internet y su alcance es para la prestación o producto disponible en Internet; se enfoca en cuatro principios principales que son: el de libre uso, de precaución, de equidad y el de transparencia; las medidas que son permitidas en relación al principio de neutralidad de la red son aquellas se encuentran debidamente autorizadas en el Reglamento, se trata de una situación de emergencia o de una medida implementada por mandato judicial.

Los tipos de medidas autorizadas se relacionan con: 1) la gestión de Direcciones IP, 2) duración de la sesión dinámica en la red, 3) almacenamiento temporal de contenidos, 4) filtro y bloqueo de servicios y/o aplicaciones a solicitud del abonado, 5) filtro y bloqueo de servicios y/o aplicaciones en cumplimiento de obligaciones contractuales con el Estado o con motivo de norma específica y 6) otras medidas siempre que no contravengan

el principio de la neutralidad de la red; de ellas, se describe las consideraciones para su implementación.

Dentro de las medidas que se encuentran prohibidas de ser implementadas están la gestión arbitraria de tráfico, el filtro y/o bloqueo arbitrario de servicios y/o aplicaciones legales y la diferenciación arbitraria en la oferta comercial de productos de acceso a Internet.

Finalmente, este reglamento establece de manera detallada el régimen de infracciones y sanciones aplicable a la falta de cumplimiento de las obligaciones establecidas en este reglamento.

2.3.5 Argentina (América Latina)

En Argentina no se ha promulgado una ley o reglamento específico relacionado con la neutralidad de la red; no obstante, en este país existe la Ley N° 27.078 de Argentina Digital que surgió como reemplazo de la Ley de Telecomunicaciones que estuvo vigente hasta ese entonces.

Estadísticas en síntesis

El Reporte Digital 2018 (Global Digital, 2018) indica que a inicios del año 2018 el total de la población en Argentina es de 44,48 millones de personas, de las cuales 34,79 millones han utilizado Internet, lo cual significa una penetración del servicio del 78%.

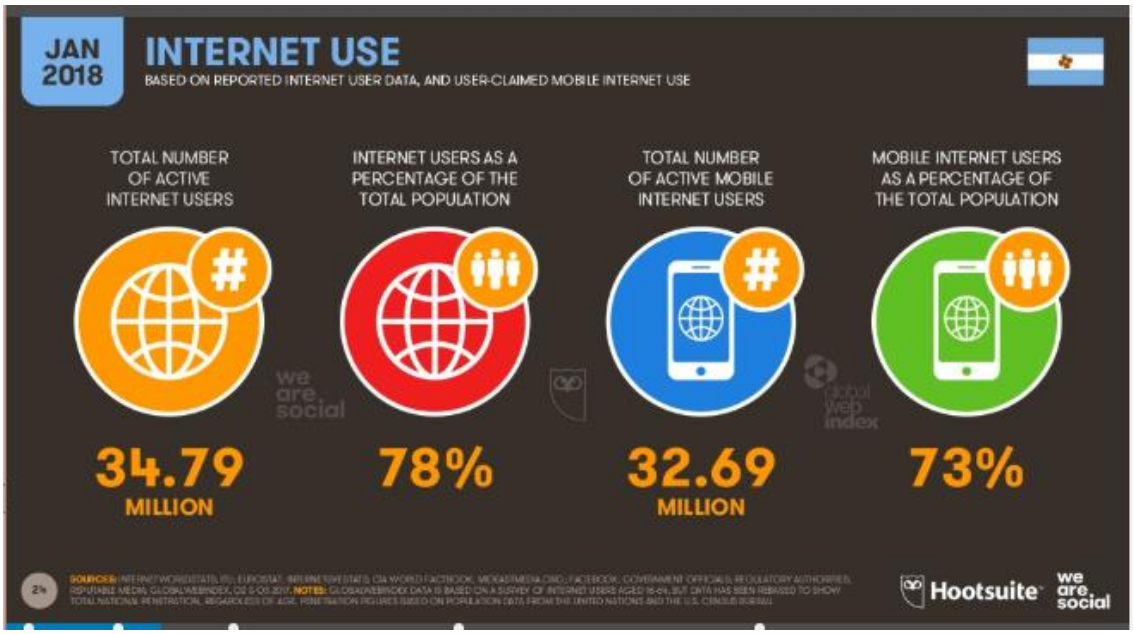

Figura 13: Estadísticas de uso de Internet en Argentina

Fuente: (Global Digital, 2018)

El mercado de la banda ancha fija, se encuentra distribuido de la siguiente manera:

Operador	Propietario	Tecnología	Participación de mercado
Cablevisión	Grupo Clarin	HFC	30,3
Telefónica	Telefónica	xDSL	25,7
Telecom	Telecom	xDSL	24,1
Otros			19,9

Figura 14: Argentina - Operadoras de Banda Ancha

Fuente: (TeleSemana, Panorama de mercado, 2018)

Regulación de la neutralidad de la red

La Ley N° 27.078 Argentina Digital promulgada el 18 de diciembre de 2014 (Anexo 11) establece dentro de su objetivo el desarrollo de las tecnologías de la información y las comunicaciones y las telecomunicaciones estableciendo y garantizando la completa neutralidad de las redes. Dentro de esta misma Ley, los artículos 56 y 57 hablan específicamente acerca del principio de neutralidad de la red.

El artículo 56 respecto a la neutralidad de la red señala que: “Se garantiza a cada usuario el derecho a acceder, utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, servicio o protocolo a través de Internet sin ningún tipo de restricción, discriminación, distinción, bloqueo, interferencia, entorpecimiento o degradación.”

Mientras que el artículo 57 describe las prohibiciones para los prestadores de servicios TIC de la siguiente manera:

a) Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o expresa solicitud del usuario.

b) Fijar el precio de acceso a Internet en virtud de los contenidos, servicios, protocolos o aplicaciones que vayan a ser utilizados u ofrecidos a través de los respectivos contratos.

c) Limitar arbitrariamente el derecho de un usuario a utilizar cualquier hardware o software para acceder a Internet, siempre que los mismos no dañen o perjudiquen la red.

2.3.6 México (Norte América)

En México se trata el principio de la neutralidad de la red en la Ley Federal de Telecomunicaciones y Radiodifusión de México que se encuentra vigente desde el 13 de agosto de 2014, misma Ley que tienen por objetivo el regular la prestación de los servicios de telecomunicaciones, los derechos de los usuarios y ejercicio de varios artículos de la Constitución Política de los Estados Unidos Mexicanos (Mexicanos, 2014).

Estadísticas en síntesis

El Reporte Digital 2018 (Global Digital, 2018) indica que a inicios del año 2018 el total de la población en México es de 130 millones de personas, de las cuales 85 millones son usuarios de Internet, lo cual significa una penetración del servicio del 78%.

Figura 15: Estadísticas de uso de Internet en México

Fuente: (Global Digital, 2018)

El mercado de la banda ancha fija, se encuentra distribuido de la siguiente manera:

Operador	Propietario	Tecnología	% de mercado
Axtel	Axtel	FTTx / Inalámbrica	2,6
Grupo Televisa	Televisa	Cable Modem	21,5
Maxcom	Maxcom	xDSL	0,8
Megacable	Megacable	Cable Modem	13,3
Otros	Otros	N/A	0,8
Telmex	America Móvil	xDSL	57,5
Total Play	Grupo Salinas	FTTH	3,5

Figura 16: México - Operadoras de Banda Ancha

Fuente: (TeleSemana, Panorama de mercado, 2018)

Regulación de la neutralidad de la red

El principio de la neutralidad de la red en la Ley Federal de Telecomunicaciones y Radiodifusión de México (Anexo 12) establece con relación al principio de la neutralidad

de la red, dos artículos específicos, el 145 y 146 del Capítulo VI, mismos que a continuación se describen:

> 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.

2.3.7 Estados Unidos (Norte América)

Para el caso de los Estados Unidos, se hace referencia a los acontecimientos de los últimos años en torno a la neutralidad de la red; de esta forma es importante señalar que en febrero del año 2015, bajo el mandato del Presidente Barack Obama, la Comisión Federal de Comunicaciones (FCC) adoptó reglas para la protección de un Internet abierto; no obstante, a finales del año 2017, las medidas del año 2015 fueron votadas como

derogadas, de tal manera que el 11 de junio del 2018, la FCC permitió la entrada en vigencia de esta decisión (Oliver & Peña, 2018).

Estadísticas en síntesis

El Reporte Digital 2018 (Global Digital, 2018) indica que a inicios del año 2018 el total de la población en Estados Unidos es de 325,6 millones de personas, de las cuales 286,9 millones son usuarios de Internet, lo cual significa una penetración del servicio del 88%, sin que haya sufrido cambio desde enero del año 2017.

Figura 17: Estadísticas de uso de Internet en México

Fuente: (Global Digital, 2018)

En cuanto a la provisión de acceso al servicio de Internet, en Estados Unidos existen muchos proveedores de Internet entre los cuales, los usuarios pueden elegir y su disponibilidad varía de acuerdo a las ciudades, códigos postales e incluso por calles. Entre los principales proveedores se encuentran los descritos en la tabla 6.

Tabla 6: Lista de varios proveedores de Internet – Estados Unidos

Proveedor	
AT&T	Frontier Communications
Comcast	Megapath
Time Warner Cable	Charter
CenturyLink	Verizon FiOS
Verizon	Cox Comunications
Windstream	Optimum
WOW!	Mediacom

Fuente: (HSI, 2018)

Regulación de la neutralidad de la red

En febrero del año 2015, la FCC que es una comisión independiente en los Estados Unidos y que se encarga de regular la industria de las telecomunicaciones en este país decide votar a favor de que Internet sea clasificado como un "bien público" ya que hasta esa fecha, este servicio era considerado como un servicio de información y por lo tanto no era factible para el regulador exigir a las compañías tratar con principio de igualdad a las conexiones realizadas por los usuarios. (Pereda, 2015).

Con base en esta decisión se establecieron un conjunto de reglas clave para una Orden de Internet abierta (Anexo 13), tanto en la banda ancha fija como para la móvil; las tres primeras reglas que prohíben prácticas dañinas para una Internet abierta, son: (FCC, 2015):

a) Sin bloqueo: los proveedores de banda ancha no pueden bloquear el acceso a contenido legal, aplicaciones, servicios, o dispositivos no dañinos;

b) Sin limitación: los proveedores de banda ancha no pueden perjudicar o degradar el tráfico legal de Internet, bases de contenidos, aplicaciones, servicios o en dispositivos no dañinos;

c) Sin prioridad de pago: los proveedores de banda ancha no pueden favorecer el tráfico legal en Internet, se prohíbe las "vías rápidas"; a través de esta regla se prohíbe a su vez a los ISP dar prioridad a los contenidos y servicios de sus afiliados.

La Orden establece además que los ISP no pueden "interferir injustificadamente ni perjudicar injustificadamente" la capacidad de los consumidores para seleccionar, acceder y utilizar el contenido, las aplicaciones, servicios o dispositivos legales de su elección; también, la FCC adquiere la autoridad necesaria para abordar prácticas cuestionables, caso por caso que se identifique contrario a estas reglas.

En cuanto a aspectos de transparencia, la Orden exige que los ISP divulguen de manera exacta y de manera consistente las ofertas brindadas por ellos, en cuanto a tarifas, promociones, recargos y topes de datos, información de pérdida de paquetes de datos como medida de rendimiento de la red y notificación de prácticas de gestión de la red.

No obstante la regulación promovida en el año 2015 por el expresidente Barack Obama, recientemente, el 11 de junio de 2018, la FCC realizó un fallo que finaliza con las reglas establecidas para una red abierta; es decir, la nueva regulación permite a los prestadores del servicio de acceso a Intente bajo respaldo legal, ralentizar y bloquear páginas de Internet en función de los pagos realizados por los usuarios o empresas (France, 2018).

De acuerdo a (France, 2018), entre los argumentos para dejar de lado las reglas de neutralidad de la red, según el Director de la FCC, Ajit Pai, estarían los hechos que los usuarios deben compartir los costos de mantener con los proveedores la costosa infraestructura de la red, así como que se garantizaría con esta desregulación, el desarrollo del sector.

Al momento, fiscales de varios estados de este país han interpuesto una demanda contra la FCC por la emisión de la nueva orden en contra de la neutralidad de la red y conforme lo ha señalado el "The New York Times", 29 estados habrían presentado proyectos de ley para que el principio de la neutralidad de la red se mantenga en sus fronteras (Oliver & Peña, 2018).

2.3.8 Unión Europea

La Unión Europea (UE) apoya las normativas sobre la neutralidad de la red; de esta manera, en el año 2014, el Parlamento Europeo vota de forma favorable por este principio y en agosto del año 2016 el Organismo de Reguladores Europeos de Comunicaciones Electrónicas (BEREC) aprobó una serie de normas para aplicar de manera armonizada de la neutralidad de la red por parte de sus 28 Estados miembros.

Estadísticas en síntesis

De acuerdo al sitio web del mercado único digital, el uso de Internet tiene mayor actividad en los estados de Dinamarca, Suecia y los Países Bajos, mientras por el contrario, es menor en Rumania, Italia y Bulgaria.

En cuanto al uso de Internet, las actividades en línea se componen de: lectura de noticias (72%), realizar llamadas de video o audio (46%), uso de redes sociales (65%), compras en línea (68%) y uso de banca en línea (61%); de igual manera, la banda ancha fija se encuentra disponible para el 98% de europeos y un alto porcentaje de hogares están cubiertos por banda ancha rápida con al menos 30 Mbps (Comisión Europea, 2018)

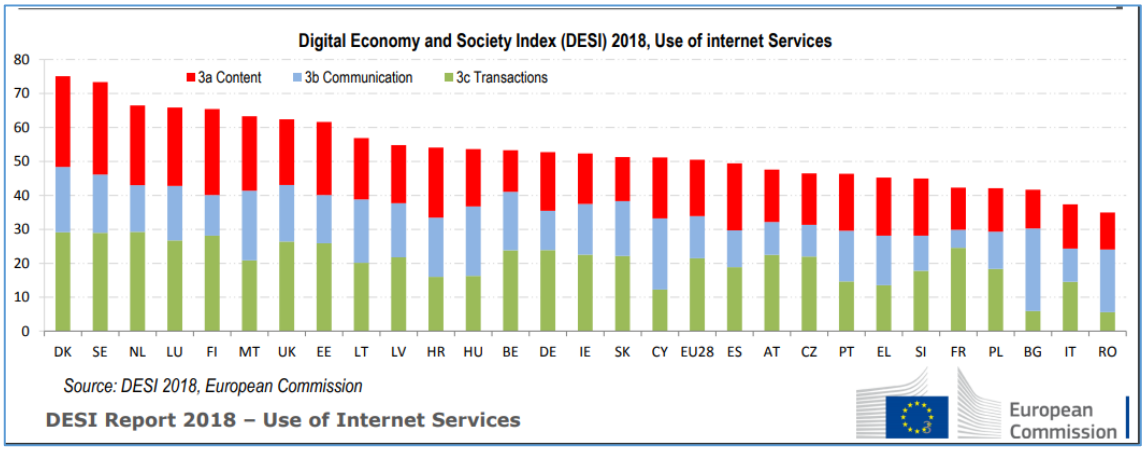

Figura 18: Uso del Servicio de Internet en Europa

Fuente: (Comisión Europea, 2018)

Regulación de la neutralidad de la red

Las directrices establecidas en agosto del año 2016 por parte del BEREC "Directrices Del ORECE Sobre La Implementación Por Los Reguladores Nacionales De Las Normas Europeas De Neutralidad De La Red" (BEREC, 2016), se encuentran enfocadas a los siguientes aspectos descritos en forma breve sobre la neutralidad de la red (Anexo 14):

- Acceso a contenido: Los usuarios finales tienen el derecho a acceder y distribuir información y contenido, usar y proporcionar aplicaciones y servicios, y utilizar el equipo de terminal de su elección, independientemente de la ubicación del usuario final o del proveedor o la ubicación, origen o destino de la información, contenido, aplicación o servicio, a través de su servicio de acceso a internet.

  Los proveedores de comunicaciones electrónicas al público, incluidos los ISP son libres de ofrecer servicios distintos de los de acceso a Internet cuando la optimización sea necesaria para cumplir con aplicaciones o servicios para niveles de calidad específicos.

- Acuerdos entre proveedores de acceso a Internet y usuarios de finales de empresas comerciales: los proveedores acceso a Internet deben prever en los acuerdos las condiciones técnicas, características de los servicios de acceso a Internet, como el precio, volúmenes de datos o velocidades mínimas y máximas y, cualquier práctica comercial llevada a cabo por el mismo.

  Adicionalmente, los ISP deben brindar información sobre las medidas de gestión de tráfico adoptadas y su impacto sobre la calidad de servicio, velocidad, limitación en volumen y datos personales de los usuarios; adicionalmente informar sobre recursos para resolver reclamos.

- Tratamiento del Tráfico: Los proveedores de servicios de acceso a Internet deben tratar todo el tráfico por igual, al proporcionar Internet servicios de acceso, sin discriminación, restricción o interferencia, y con independencia de remitente o receptor, el contenido accedido o distribuido, las aplicaciones o servicios utilizados o proporcionados, o el equipo terminal utilizado.

No se impide a los proveedores de acceso a Internet implementar medidas razonables de gestión de tráfico.

Para ser considerado como razonables, tales medidas deben ser transparentes, no discriminatorias y proporcionadas, y no pueden basarse en consideraciones comerciales, sino en una calidad técnica objetivamente diferente de requisitos de servicio de categorías específicas de tráfico.

Tales medidas no pueden controlar el contenido específico y no se podrán mantener por más tiempo del necesario y en particular no se permite el bloqueo, ralentización, alteración, restricción, interferencia, degradación o discriminación entre contenido específico, aplicaciones o servicios, o categorías específicas de los mismos.

Se exceptúa una gestión de tráfico solamente cuando sea necesario, considerando: a) cumplimiento de actos legislativos de la Unión, órdenes de tribunales o de autoridades públicas con poderes pertinentes, b) preservar la integridad y seguridad de la red, de los servicios prestados a través de esta red y de equipos terminales de los usuarios finales, c) evitar congestión inminente de la red y mitigar los efectos de excepcional o congestión temporal de la red.

- Supervisión: Las autoridades nacionales de la reglamentación de los Estados Miembros se encuentran facultadas para realizar la supervisión acerca del cumplimiento de los lineamientos establecidos en torno al acceso a Internet, promoviendo a su vez la disponibilidad continua y no discriminatoria; a su vez, las autoridades reguladoras pueden imponer requisitos sobre la prestación del servicio de Internet y deben publicar informes anuales sobre sus seguimientos y resultados, proporcionando los mismos a la Comisión y al BEREC.

  Los ISP, de igual manera, frente a las peticiones realizadas por las autoridades regulatorias, deben poner a disposición la información correspondiente a las obligaciones establecidas dentro de los plazos requeridos.

2.4 Posturas de organismos internacionales de telecomunicaciones

La neutralidad de la red, conforme se ha visto de los anteriores apartados tiene su propio papel protagónico en normativas de los diferentes países, ya sea de manera global o macro o a través de regulaciones expedidas de manera específica; de este modo, se describirá de manera breve y complementaria a continuación las posturas de la Unión Nacional de Telecomunicaciones (UIT), Asociación GSM (GSMA) y la Asociación Interamericana de Empresas de Telecomunicaciones (ASIET), con relación a este principio.

2.4.1 Unión Internacional de Telecomunicaciones (UIT)

Los temas relacionados con las tecnologías de la información y comunicación a nivel mundial se encuentran reguladas por la UIT, organismo de la Organización de las Naciones Unidas (ONU) y que fue fundada en el año 1865.

Con relación a Internet y sus características para ser neutral, la recomendación UIT-T X.700 describe cinco (5) áreas de gestión de un sistema real abierto: a) gestión de fallos, b) gestión de contabilidad que conlleva a la facturación por servicios personalizados prestados por los ISP, c) gestión de configuración desde elementos individuales de la red hasta la red de manera global, d) gestión de calidad de funcionamiento para mantener niveles de servicios pactados con los usuarios y e) gestión de seguridad que involucra mecanismos de seguridad, distribución de información relativa a seguridad y sucesos relacionados con la seguridad.

Según el Manual de regulación sobre la calidad de servicio publicado en el año 2017 por parte de la UIT (UIT, 2017), se señala que los enfoques regulatorios en torno a la calidad de servicio sobre la red y por tanto sobre la neutralidad de la red deben “tener mucho cuidado para lograr un equilibrio adecuado, evitando daños sin también prevenir beneficios”; de esta manera, concluye que para efectos de generar regulación es necesario resolver adecuadamente cualquier inquietud que permita evaluar medidas para hacer cumplir la neutralidad de la red.

2.4.2 Asociación GSM (GSMA)

La GSMA, organización de operadores móviles y compañías relacionadas a nivel mundial, en su Manual de políticas públicas de telecomunicaciones móviles (GSMA, 2018) indica que en razón de los 17 Objetivos de Desarrollo Sostenible (ODS) adoptados unánimemente por los líderes del mundo en septiembre del año 2015 durante Agenda de la ONU, se ha revisad las contribuciones que se pueden realizar particularmente para ODS 3: Salud y bienestar, 9: Industria, innovación e infraestructura, 11: Ciudades y comunicaciones sostenibles, y 13: Acción por el clima.

En cuanto a la neutralidad de la red, la mencionada Asociación sostiene que "Para satisfacer las diversas necesidades de los consumidores, los operadores de redes móviles necesitan contar con la capacidad de contar con la capacidad de gestionar de forma activa el tráfico de red"; adicionalmente, señala que es importante que Internet continúe siendo una red abierta y funcional para lo cual, los operadores deben contar con la flexibilidad necesaria para diferenciar entre distintos tipos de tráfico. De esta manera, la gestión de tráfico, considerada como una herramienta eficaz y necesaria en distintas circunstancias operativas y comerciales pueden ser de los siguientes tipos: a) por integridad de la red, b) para protección infantil, c) debido a servicios activados por la suscripción, d) por llamadas de emergencia ye) por requisitos de prestación.

2.4.3 Asociación Interamericana de Empresas de Telecomunicaciones (ASIET)

La ASIET nació en 1982 con el nombre de AHCIET y se encuentra conformada por empresas públicas y privadas del sector de las telecomunicaciones que operan en el continente americano, quienes a su vez participan en debates sobre políticas públicas en la región y en foros de alto nivel. (ASIET, 2018)

Según Pablo Bello, Director Ejecutivo de la ASIET es necesario comprender el ecosistema digital para debatir sobre la neutralidad de la red; además es imprescindible preservar una red Internet abierta a la innovación para estimular las inversiones y la competencia, tanto en las redes y servicios, como en los contenidos y aplicaciones.

Entre los aspectos que la ASIET considera necesarias para proteger una libertad efectiva de Internet están: a) se debe resguardar la competencia a lo largo de todos los segmentos que integran en ecosistema digital, b) fortalecer la capacidad y libertad de elección de los consumidores, c) favorecer la inversión y el emprendimiento para abordar el desafío de cerrar la brecha digital. (ASIET, 2018).

2.5 Representación comparativa

Después de haber realizado la descripción del tratamiento del principio de la neutralidad de la red en diferentes países y regiones del mundo, a continuación se presentará cuadros comparativos sobre las realidades experimentadas en torno al acceso a Internet y regulación sobre neutralidad de la red.

2.5.1 Características de mercado de acceso a Internet en los países estudiados

Tabla 7: Usuarios de internet (millones)

País /Región	Usuarios de Internet (millones)
Chile (América Latina)	14,11
Ecuador (América Latina)	13,47
Colombia (América Latina)	31
Brasil (América Latina)	139,1
Perú (América Latina)	22
Argentina (América Latina)	34,79
México (Norte América)	85
Estados Unidos (Norte América)	286,9
Unión Europea	704,84

Fuente: (Digital Report; Exito Exportador, 2018)

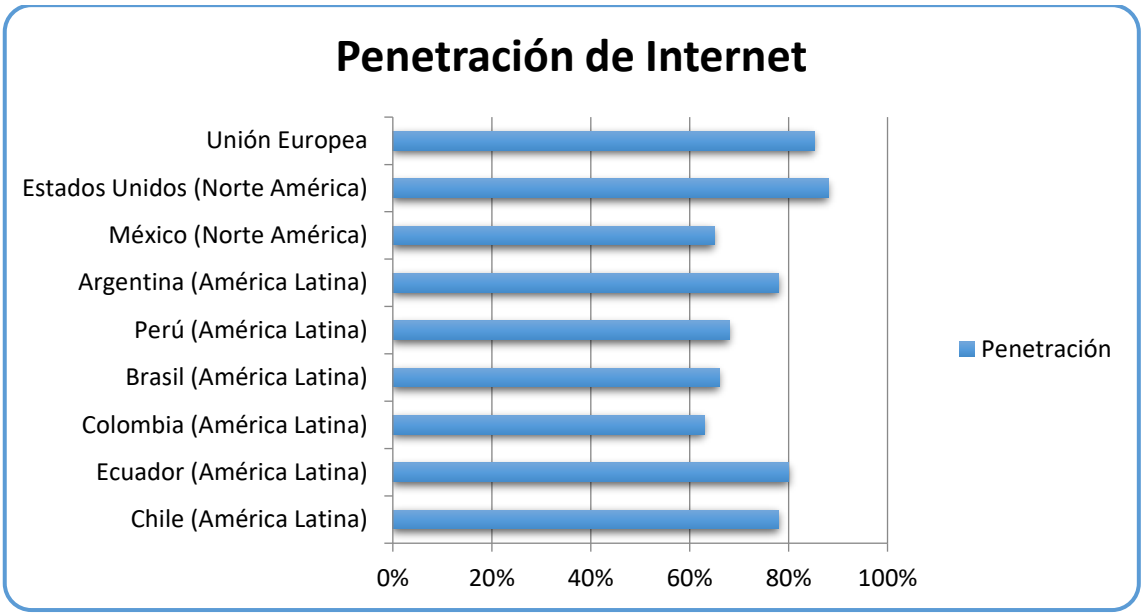

Tabla 8: Penetración de Internet en los Países y Regiones estudiadas

Fuente: (Digital Report; Exito Exportador, 2018)

2.5.2 Comparación de etapa de reglamentación de neutralidad de la red en los diferentes países

En función del detalle de las distintas normativas que han sido expedidas en los diferentes países, se describe a continuación el cuadro comparativo de los aspectos que se han considerado relevantes frente a la neutralidad de la red.

Tabla 9: Situación de la normativa relacionada con neutralidad de la red

	Normativa vigente	Año	Regulador	Etapa de normativa	Transparencia	Bloqueo	Gestión de Tráfico	Contenido
Ecuador (América Latina)	Ley Orgánica de Telecomunicaciones (LOT) y Reglamento General a la LOT	2015	Agencia de Regulación y Controlde las Telecomunicaciones (ARCOTEL)	Inicial: No se establece normativa específica o lineamientos// se describe de manera general en LOT	A favor/ de manera general	En contra/ de manera general	Abierto / establecido de manera general	A favor / de manera general
Chile (América Latina)	Ley 20.453/2010 y Resolución 40/2014	2010// 2014	Subsecretaría de Telecomunicaciones de Chile (SUBTEL)	Avanzado: Existe reglamentación Específica e imposición de sanciones	A favor	En contra	Abierto / se establecen requisitos	A favor
Colombia (América Latina)	Ley 1450 del año 2011 (Artículo 56) // Resolución 3502	2011	Comisión de Regulación de Comunicaciones (CRC)	Intermedio: Reglamentación del artículo 56 de la Ley	A favor	En contra	En contra/ de manera general	A favor
Brasil (América Latina)	Ley 12.965/2014 (Marco Civil de la Internet) //Decreto Presidencial 8.771/2016	2014// 2016	Agencia Nacional de Telecomuniccaiones (ANATEL)	Intermedia: Establece reglas generales relacionadas al tema en la Ley	A favor	En contra	En contra/ de manera general	A favor
Perú (América Latina)	Reglamento de Neutralidad de la Red de Perú de 01/01/2017	2017	Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL)	Avanzado: Existe reglamentación Específica e imposición de sanciones	A favor	En contra	Abierto / se establecen requisitos	A favor
Argentina (América Latina)	Ley N° 27.078 de Argentina Digital	2014	Ente Nacional de Comunicaciones (ENACOM)	Inicial: No se establece normativa específica o lineamientos	A favor/ de manera general	En contra/ de manera general	En contra/ de manera general	A favor / de manera general
México (Norte América)	Ley Federal de Telecomunicaciones y Radiodifusión (LFTR)	2014	Instituto Federal de Telecomunicaciones (IFT)	Inicial: No se establece normativa específica o lineamientos	A favor/ de manera general	En contra/ de manera general	En contra/ de manera general	A favor / de manera general
Estados Unidos (Norte América)	Comisión Federal de Comuniccaiones (FCC) // 2018 nuevos lineamientos	2018	Comisión Federal de Comuniccaiones (FCC)	Actualmente en tratamiento por desacuerdo de varios Estados ante la derogació de las directrices del año 2015	En conflicto actualmente/ Senado de EEUU ha requerido retomar lineamientos de 2015			
Unión Europea	Directrices del ORECE Sobre La Implementación Por Los Reguladores Nacionales De Las Normas Europeas De Neutralidad De La Red // agosto 2016	2016	Corresponde a regulador de cada miembro de la Unión Europea	Avanzado: Existe reglamentación Específica e imposición de sanciones	A favor	En contra	Abierto / se establecen requisitos	A favor

Fuente: Elaboración propia en función del contenido de este documento.

2.5.3 Reflexiones sobre el análisis comparativo y resultados obtenidos

Conforme se ha evidenciado de revisión realizada, la neutralidad de la red es un tema del cual se han desarrollado amplias discusiones en los países y regiones del mundo, y de tal manera, se desprende que en algunos de ellos se ha perfeccionado normativa específica, mientras que en otros existen alusiones de este principio enfocados de manera más general.

En el caso particular del Ecuador, se observa que el principio de la neutralidad de la red se encuentra garantizado según se establece dentro de la LOT, sin perjuicio de lo cual, se puede decir que de acuerdo a la regulación que existe en otros lugares del mundo como países cercanos como Chile y Perú, así como de la Unión Europea, tiene todavía un largo camino que recorrer.

Por otra parte, es importante que frente a este principio de neutralidad de la red se pueda evaluar los acontecimientos suscitados en los últimos meses en una potencia mundial, como lo es Estados Unidos dado que el no continuar con los lineamientos establecidos en el año 2015 para garantizar la neutralidad de la red, podría generar efectos no deseados en otros lugares del mundo; esto se puede explicar por aspectos como que las conexiones que salen de los países se relacionan con los servidores en EE.UU., pudiendo las grandes empresas dictar sus propias reglas de juego para el acceso a Internet.

Hemos observado que la Unión Europea ha dictaminado reglas para garantizar el cumplimiento de la neutralidad de la red en todos sus 28 países miembros; esto conlleva a que cada una de las legislaciones nacionales adapten sus propias normativas garantizando el principio de la neutralidad de la red.

En cuanto a las principales aristas de tratamiento de la neutralidad de la red, se ha observado que gran parte de las discusiones se han enfocado a la posibilidad de gestión del tráfico y en lo que se considera una gestión razonable, reconociendo que los prestadores del servicio de acceso a Internet podrían requerir adaptar algunas prácticas, de carácter técnico, para garantizar el uso eficiente de las redes y a su vez, proveer a los usuarios una mejor calidad de servicio.

Adicionalmente, en relación al tratamiento de acceso a contenidos, transparencia y bloqueo de tráfico se observa que en general existen consenso en las posturas de las diferentes normativas; sin embargo, particularmente en relación al contenido, se debe tener presente que de acuerdo a puntualizaciones realizadas desde el inicio de este capítulo, el acceso a los contenidos puede estar supeditado a las realidades propias de cada uno de los países, ya sea por cultura, política o directrices gestionadas por los propios Gobiernos.

3 PROPUESTA DE LINEAMIENTOS PARA LA REGULACIÓN EN ECUADOR SOBRE NEUTRALIDAD DE LA RED BASADO EN LAS PRÁCTICAS EFECTUADAS EN LOS PAÍSES REVISADOS.

Una vez que se ha realizado una breve revisión de cómo diferentes países de América y la Comunidad Europea tratan en sus respectivas legislaciones el principio de la neutralidad de la red, a continuación se presentará la propuesta de un manual que contendrá las consideraciones básicas futuras que se han derivado de los desarrollos previos, rescatando además las mejores prácticas observadas que a criterio propio debieran ser tomadas en cuenta, al momento de determinar una normativa específica sobre neutralidad de la red.

De igual manera, se realizará un conjunto de recomendaciones generales para los diferentes intervinientes en la cadena que conforman el ecosistema relacionado con la neutralidad de la red, además de proponer un plan de mejora continua, en el caso de que se establezca regulación específica sobre neutralidad de la red en Ecuador.

3.1 Análisis causa - efecto sobre la aplicación de normativa específica de neutralidad de red en el Ecuador

El análisis causa – efecto que se presenta a continuación permite obtener la representación de las posibles causas para el efecto de la falta de normativa o lineamientos específicos sobre la neutralidad de la red en el Ecuador.

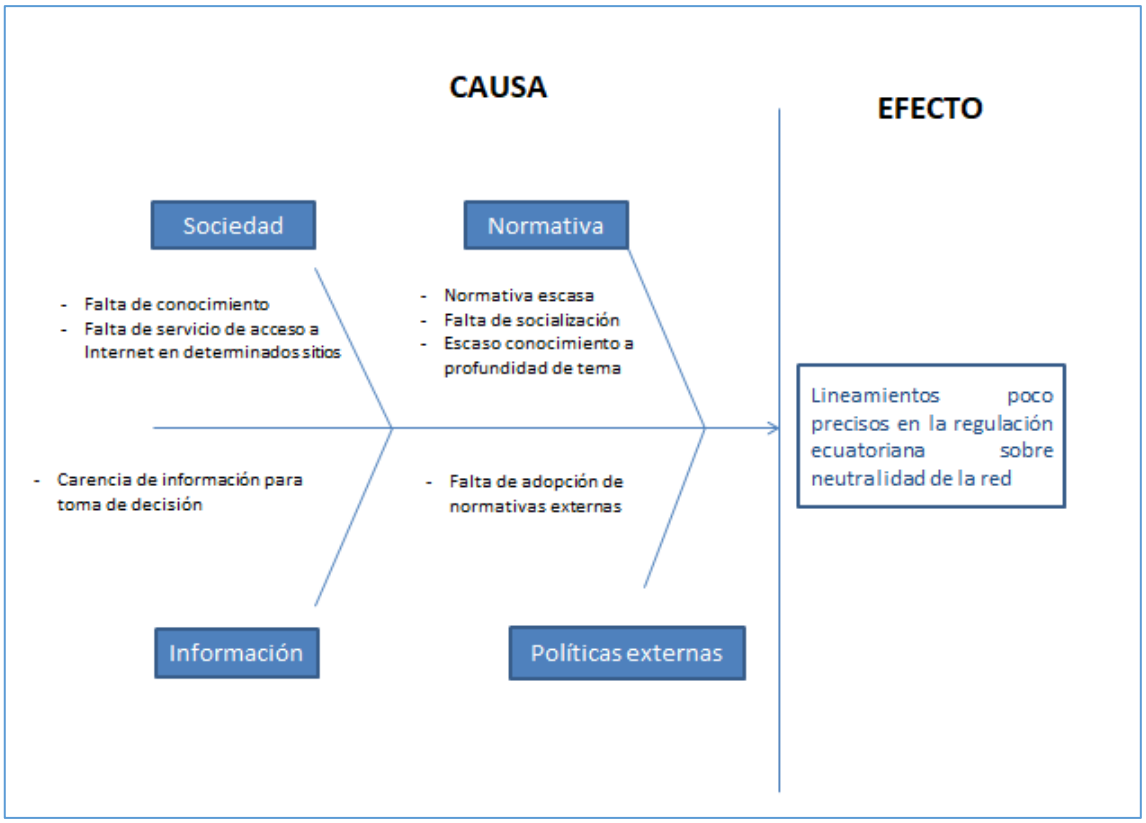

Figura 19: Diagrama de causa – efecto respecto a los lineamientos poco precisos sobre la neutralidad de la red en el Ecuador

Seguidamente se describe brevemente cada una de las causas descritas que originan como efecto los "lineamientos poco precisos en la regulación ecuatoriana sobre la neutralidad de la red"

- **Sociedad**

  Causa 1.- Falta de conocimiento. La sociedad ecuatoriana en los actuales momentos usa el Internet para actividades que se podrían considerar rutinarias frente al uso que se da al mismo en otros sitios del mundo; es decir son altos los porcentajes de uso en cuanto a búsqueda de información y comunicación se refiere, más que en ámbitos de frecuencia de compra de productos o servicios por ejemplo. De esta manera, se concluye el concepto de neutralidad de la red no se encuentra en el Ecuador ampliamente difundido y por consecuencia, entendido.

  Causa 2.- Falta de servicio de Internet en determinados sitios. De acuerdo al INEC, para el año 2017, los hogares en área urbana con acceso a Internet a nivel nacional

bordea el 46%, mientras en el área rural se tiene que apenas el 16.6% de los hogares tiene acceso a Internet; de este modo se evidencia que el entendimiento de la neutralidad de la red en la sociedad se encontrará por ahora rezagada en función de entre otros aspectos analizados, a la expansión y acceso al Internet en los hogares del Ecuador. (INEC, 2018)

- **Normativa**

Causa 3.- Normativa escasa. Conforme se ha descrito durante el desarrollo de este trabajo, no existe en Ecuador actualmente una normativa específica sobre la neutralidad de la red.

Causa 4.- Falta de socialización. Conforme las generalidades existentes en las normativas ecuatorianas sobre la neutralidad de la red, se desprende la falta de socialización a manera de detalle lo que comprende este principio, por parte de las autoridades en el sector y las empresas.

Causa 5.- Escaso conocimiento a profundidad del tema. El principio de la neutralidad de la red, como se ha observado, se compone de varios aspectos importantes; de esta forma, se evidencia por el contenido escaso de la regulación ecuatoriana en torno a su aplicación, que la sociedad en general carece de un conocimiento profundo acerca de este principio y su correcta aplicación.

- **Información**

Causa 6.- Carencia de Información para toma de decisión. Si bien se ha mostrado como en otros lugares del mundo se ha tratado de manera profunda la neutralidad de la red, no se evidencia que exista una variedad de análisis sobre el impacto de la neutralidad de la red en el Ecuador, lo que implica que bajo este enfoque, la falta de información incide en una toma de decisión para establecer lineamientos a mayor detalle sobre este principio en el país.

- **Políticas externas**

  Causa 7.- Falta de adopción de normativas externas. Una vez que se ha descrito la normativa externa mundial que existe en torno a la neutralidad de la red, se concluye que para una mejor comprensión de lo que significa este principio, podría ser iniciativa del regulador el análisis, adopción y difusión de reglas generales en referencia a este concepto, cuestión que a la presente fecha no se realiza.

3.2 Entrevista realizada sobre la neutralidad de la red en el Ecuador con el Ing. Francisco Balarezo

Continuando con las actividades tendientes al objetivo de propuesta sobre el tema planteado en el presente trabajo, se describe a continuación un breve resumen sobre la entrevista realizada al Ing. Francisco Balarezo Pozo, quien es actualmente Gerente General de Netlife en Ecuador, así como Director Ejecutivo de la Asociación de Empresas Proveedoras de Servicios de Internet, Valor Agregado, Portadores y Tecnologías de la Información (AEPROVI).

Para el desarrollo de la entrevista se ha partido considerando la siguiente hipótesis: La neutralidad de la red debe tener lineamientos normativos en el Ecuador

3.2.1 Desarrollo de la entrevista

A continuación se presenta a manera de resumen las respuestas brindadas a las preguntas realizadas durante la entrevista y los datos generales de la misma:

Lugar: La entrevista fue llevada a cabo día martes 13 de noviembre de 2018 en las instalaciones de Netlife en Quito, ubicadas en la calle Núñez de Vela E3-13 y Av. Atahualpa.

Persona entrevistada: Ing. Francisco Balarezo, Gerente General de Netlife en Ecuador y Director Ejecutivo de la AEPROVI.

Realización de entrevista: La entrevista inició a las 08h30 y tuvo una duración de 42 minutos y 59 segundos. Se adjunta en el Anexo 15, la descripción de la entrevista y el audio realizado como parte del presente trabajo. Como puntos clave que se trataron en la mencionada entrevista, se encuentran los siguientes:

- Explicación sobre el significado de la neutralidad de la red.
- Punto de vista de los proveedores de Internet acerca de la neutralidad de la red y su necesidad o no de contar con lineamientos para este principio.
- La neutralidad de la red con relación al contenido y piratería.
- Aplicación de la transparencia de información en el Ecuador sobre el servicio de Acceso a Internet.
- La neutralidad de la red y las aplicaciones en este servicio.
- Lineamientos para aplicación de la neutralidad de la red, considerando las normativas internacionales.
- Aspectos complementarios.

3.3 Propuesta de diseño: formulación de Lineamientos para una regulación de la neutralidad de la red en el Ecuador bajo las mejores prácticas revisadas

En función de los insumos obtenidos en el transcurso del desarrollo de este trabajo, en adelante se desarrolla una propuesta de lineamientos para el tratamiento de la neutralidad de la red que podría generarse en el futuro en Ecuador dentro de la agenda de normativas que se encuentren previstas por parte del regulador, como aporte referencial y en base a lo observado como prácticas externas llevadas a cabo por otros países.

Para la presentación de esta propuesta se parte del hecho que en la LOT se consagra el objetivo de garantizar la neutralidad de la red.

3.3.1 Objetivos

- Describir lineamientos básicos sobre neutralidad de la red, con la finalidad de garantizar un trato igualitario y no discriminatorio del tráfico en el servicio de Acceso a Internet y permitiendo su continuo funcionamiento.

- Describir medidas permitidas, no permitidas sobre la aplicación de este principio para los diferentes actores relacionados en el ecosistema de Internet.

3.3.2 Alcance.- Aplicable para:

- Los operadores de servicios de telecomunicaciones.
- Proveedores de Acceso a Internet.
- Proveedores de aplicaciones, contenidos y servicios en Internet.
- Usuarios del servicio de acceso a Internet.

3.3.3 Marco conceptual

- Gestión de tráfico: Acciones por las cuales se analiza, administra y/o gestiona los paquetes o flujo de paquetes de datos y que en cuanto a neutralidad de la red son las medidas que tienen la potencialidad de generar bloqueo, discriminación, restricción o degradación de cualquier tipo de tráfico en la red de Internet.

- Internet: Sistema mundial de redes de datos interconectadas entre sí a través del uso del protocolo IP y que permite a los usuarios conectados, conectarse entre sí para acceso y compartición de información.

- Información legal en Internet: Toda aquella información que es permitida según las normativas ecuatorianas y que no se encuentran en contra de la moral y buenas costumbres.

- Usuarios del servicio de acceso a Internet: Persona natural o jurídica que hace uso de los servicios de telecomunicaciones, en este caso el de Acceso a Internet, bajo cualquier modalidad.

- Servicio de Acceso a Internet (SAI): Servicio que permite la provisión del acceso a la red mundial Internet, por medio de plataformas y redes de acceso implementadas para tal fin (ARCOTEL, 2016).

- Proveedores del Servicio de Acceso a Internet (ISP): Persona natural o jurídica que preste servicios de acceso a Internet y por tanto, conectividad entre los usuarios o las redes de Internet e Internet con independencia de la tecnología de red y el equipo terminal utilizado por los usuarios finales, y que, además dispone del título habilitante dispuesto en la normativa regulatoria vigente para la prestación de sus servicios.

- Proveedores de aplicaciones, contenidos y servicios en Internet: Persona natural o jurídica que pone a disposición de los usuarios de forma gratuita o con tarifas determinadas aplicaciones, servicios o contenidos soportados en el Acceso a Internet.

- Neutralidad de la red: Principio por el cual, el tráfico de la red de Internet debe ser tratado con igualdad, sin discriminación, restricción o interferencia de manera independiente de su remitente, destinatario, contenido, favoreciendo la libertad y elección de los usuarios frente a la información disponible en esta red.

3.3.4 Lineamientos sobre Proveedores de Acceso a Internet (ISP)

Calidad del servicio

- Indicadores de calidad: Obligación de medición y cumplimiento de los indicadores de calidad que sean determinados por el organismo de regulación y control de las telecomunicaciones. Las mediciones de los indicadores de calidad deben involucrar, velocidades de transmisión, niveles de calidad ofrecido a los usuarios, tiempos de restablecimiento de servicio en caso de pérdida del mismo. Las mediciones realizadas deben contar con sus respectivos respaldos y estarán debidamente documentados.

Transparencia

- Publicación de Información: Obligación de mantener debidamente publicada y actualizada en su página web, la información en forma clara de las características sobre los servicios de acceso a Internet que son ofertados a los usuarios, conteniendo aspectos como:

  a) Características comerciales del o de los planes ofertados a los usuarios.

  b) Velocidades de subida y bajada ofertadas.

  c) Compartición del enlace expresada como 1: xx, entendiéndose éste como el resultado de la división entre la suma de las velocidades contratadas de todos los usuarios y la velocidad propia del enlace.

  d) Indicadores de calidad.

  e) Tiempo de restablecimiento del servicio en caso de pérdida del mismo.

  f) En caso de que existan, la descripción detallada y comprensible de medidas de gestión de tráfico y administración de la red, incluyendo: características, aplicaciones, descripción de afectación, periodos de tiempo en las cuales se

gestionará el tráfico. Para este propósito poder emplear la explicación de casos prácticos, por gráficos de ser el caso.

- Formalización de oferta de servicios: Obligación de los ISP para poner en conocimiento del organismo de regulación y control las ofertas comerciales en torno al servicio de acceso a Internet.

  Debe existir la libertad de celebrar acuerdos entre el ISP y los usuarios finales relacionados con condiciones técnicas y comerciales (precio, volúmenes de datos, compartición de enlace, velocidad, cobertura y otras características) para la prestación del servicio de acceso a Internet, sin que esto menoscabe o limite el derecho de los usuarios del acceso a Internet.

- Atención a requerimientos de los usuarios: Se debe prever la entrega a los usuarios, bajo pedido de los mismos, de la información de los servicios ofertados y contratados.

- Atención a requerimientos del organismo regulador: De conformidad a lo establecido en la LOT, corresponderá a los ISP, facilitar la entrega de información que el organismo regulador, con la finalidad de verificar la correcta aplicación de los indicadores de calidad, transparencia de información que se brinda a los usuarios.

Gestión de tráfico

- Sobre la información de medidas sobre la neutralidad de la red:

  a) Los ISP no pueden de manera arbitraria, bloquear, interferir, discriminar, entorpecer o restringir, el derecho de los usuarios al uso, envío, recepción, a la oferta, de cualquier contenido, aplicación o servicio que sea legal a través de Internet.

  b) No pueden los ISP prohibir cualquier tipo de actividad legal que se realice sobre Internet, para lo cual es necesario ofrecer a los usuarios un servicio de acceso a Internet que garantice esta condición.

c) Los ISP pueden tomar medidas para gestionar el tráfico en Internet y administración de la red, siempre que dichas medidas no sean tomadas con objeto de realizar acciones en contra de las pautas indicadas como prohibiciones.

   En el caso de la toma de aplicación de medidas de gestión de tráfico y/o administración de la red por parte del ISP, es obligación del ISP informar de manera oportuna a los usuarios sobre la medida adoptada de manera clara, señalando además los aspectos de tiempo de permanencia de dicha medida.

d) No pueden los ISP prohibir cualquier tipo de actividad legal que se realice sobre Internet, para lo cual es necesario ofrecer a los usuarios un servicio de acceso a Internet que garantice esta condición.

- Prácticas sobre gestión de tráfico relativa a neutralidad de la red:

a) A petición expresa del usuario y debidamente respaldada, los ISP se encuentran facultados a bloquear los contenidos, aplicaciones o cualquier servicio que se brinde por la red, de acuerdo a lo solicitado.

b) El bloqueo o restricción realizada como consecuencia de la petición del usuario, no debe afectar arbitrariamente a los proveedores de contenidos, aplicaciones y servicios que se encuentran en Internet.

c) A favor de los usuarios, los ISP tendrán a su disponibilidad servicios de control para el bloqueo de contenidos que atenten en contra de la ley, moral y buenas costumbres, con sus debidas instrucciones de uso.

d) En cuanto a contenidos direccionados a público adulto, los ISP deberán establecer las validaciones necesarias para la aceptación de acceso a dicho contenido por parte de los usuarios.

e) De acuerdo a las directrices establecidas en el LOT, los ISP tendrán la responsabilidad de gestionar las acciones respectivas, con la finalidad de

asegurar la protección de sus redes a través de uso de las herramientas tecnológicas legales disponibles.

f) Conforme lo establecido en la LOT, corresponde a los ISP establecer los mecanismos necesarios para asegurar la protección de la privacidad de los usuarios.

g) Los ISP puede implementar una medida relativa a neutralidad de la red cuando sea calificada como una medida aceptada por el regulador o dispuesta a nivel judicial, así como se trate de una situación de emergencia relacionada con este principio.

h) La gestión de tráfico relativa a neutralidad de la red no será considerada medida arbitraria cuando se genere para preservar la seguridad e integridad de la red (bloqueo de fuentes de ataques, uso de software malicioso, virus, bloqueo de puertos que constituyen amenazas a la red, etc.) así como prevenir efectos de congestión severa de la red o situaciones de emergencia o casos de fuerza mayor de acuerdo a las definiciones efectuadas en torno a los lineamientos generales y únicamente de manera temporal hasta superar el evento.

   En caso que los eventos sucedidos con los ISP sea recurrentes y larga duración, se debe evaluar la expansión de la capacidad de la red.

i) Se puede gestionar el tráfico por servicios, contenidos y/o aplicaciones con el carácter estrictamente temporal y excepcional, con la finalidad de garantizar la continuidad del servicio evitando congestiones severas en la red, o acciones ilegales, como piratería u otras que se identifiquen y que sean debidamente comprobadas.

- Medidas sobre neutralidad de la red sin autorización del regulador:

a) Bloqueo de contenido, direcciones IP, puertos de Internet, aplicaciones y/o servicios en Internet que hayan sido solicitados expresamente por el usuario.

b) Gestión sobre las direcciones IP que identifican a los usuarios y almacenamiento de contenidos por tiempo o capacidad, siempre que no se afecte el normal uso del servicio de acceso a Internet.

c) Bloqueos y restricciones dispuestas por autoridad competente, para cuyo caso deben existir los justificativos respectivos.

- Medidas sobre neutralidad de la red en situaciones de fuerza mayor o emergencia:

a) Una situación de emergencia constituye el o los eventos ocurridos que ponen en serio riesgo el normal funcionamiento del servicio de Acceso a Internet, afectando la disponibilidad de la información, contenido, aplicaciones o servicios dentro de éste; las situaciones de fuerza mayor son de acuerdo a lo establecido en el ordenamiento jurídico vigente.

b) Ante dichas situaciones que deben encontrarse debidamente documentadas, los proveedores del servicio de acceso a Internet pueden adoptar acciones temporales y/o de gestión de tráfico para protección de las redes ante acciones maliciosas o que pongan en peligro el servicio de acceso a Internet.

c) La información que respalda las acciones realizadas deben ser informadas al organismo de regulación, conforme los plazos establecidos para el efecto.

d) El prestador de servicios de telecomunicaciones que se vea afectado por una situación de emergencia relacionada con la neutralidad de la red pero que dependa a su vez del control de la red de otro prestador de servicio de acceso a Internet, deberá solicitar a éste tome las medidas correspondientes de acuerdo a los eventos debidamente justificados.

Contenidos, aplicaciones y servicios sobre Internet

- Se consideran prácticas restrictivas en Internet:

  a) Toda acción arbitraria que pretenda bloquear, obstaculizar, interferir, entorpecer, ralentizar y/o restringir el derecho del o los usuarios para el uso, envío, recepción u oferta de cualquier contenido, aplicación, o servicio legal sobre Internet.

  b) Toda acción arbitraria descrita en el literal a) con relación a cualquier actividad o uso que sea legal sobre Internet.

  c) Las acciones que se deriven de la gestión de tráfico o administración de la red que afecten a los niveles de servicio contratados por el o los usuarios.

  d) Toda acción que de forma arbitraria priorice o discrimine entre proveedores de contenido, proveedores de aplicaciones y/o usuarios.

  e) Toda acción de restricción para los usuarios relacionada al acceso de información relativa a los servicios ofrecidos o contratados.

  f) Toda acción que impida o restrinja a los usuarios a la utilización de equipos, aparatos o dispositivos en la red que sean legales, homologados y que no sean perjudiciales a la red o a la calidad del servicio.

3.3.5 Lineamientos sobre proveedores de contenido, servicios y aplicaciones en Internet

- Contenidos y aplicaciones lícitos: Todo contenido y aplicación en Internet que sea lícitamente permitido es objeto de uso en libertad por parte de los usuarios.

- Equidad: Cualquier protocolo, tráfico, contenido, aplicación brindado por un ISP a través de sus redes tiene por ser tratado de manera equitativa, salvo exista casos de excepción determinados de manera expresa y bajo justificativos sustentados de entidad competente.

- Optimización: Los proveedores de contenido, servicios y aplicaciones en Internet tienen la libertar de realizar optimización sobre ellos cuando se considere objetivamente necesaria para cumplir con niveles específicos de calidad frente a prestaciones de similares características, con la provisión de una capacidad suficiente.

- Distribución: Para la distribución de los servicios, aplicaciones o contenidos de Internet, los proveedores deben disponer de los acuerdos y permisos que les faculten para tal fin.

- Acuerdos con proveedores de Acceso a Internet: Las condiciones técnicas, características de los servicios de acceso a Internet y prácticas comerciales de los ISP no deben limitar los derechos de acceso y distribución de información y contenido, así como el uso y proporción de aplicaciones y servicios de los usuarios por elección, protegiendo de esta forma el acceso abierto a Internet.

3.3.6 Lineamientos sobre Usuarios

- Acceso y distribución de información: Derecho al acceso, uso y distribución de información y contenido; a la proporción de aplicaciones y servicios a través de su servicio de Acceso a Internet, dentro del marco legal relacionado con la legalidad de los contenidos, aplicaciones o servicios que se encuentren o sean establecidos en el Ecuador.

- Uso de dispositivos en la red: Los usuarios tienen derecho al uso de cualquier clase de equipo o dispositivo en la red siempre y cuando sean legales, debidamente homologados y no causen daño o inseguridad a las redes.

- Presentación de reclamos: Los usuarios tienen el derecho de presentar sus reclamos hacia los prestadores del servicio de acceso a Internet y a recibir respuesta de los mismos en los plazos máximos establecidos en la normativa regulatoria vigente, esto es, hasta 15 días hábiles.

La presentación y gestión de los reclamos debe efectuarse a través de los medios que se establezcan para el efecto por parte del ISP e inclusive por mecanismos señalados por el organismo de regulación y control de las telecomunicaciones; en todos los casos, el usuario debe poder disponer del identificativo de su queja para los seguimientos que considere pertinentes.

- Oferta de servicios a terceros: Se enmarca como práctica prohibida el hecho que los usuarios que han contratado el servicio de acceso a Internet para disponer de contenidos, ofrezcan el servicio a terceros sin contar con las debidas autorizaciones de prestación de servicios de telecomunicaciones.

- Servicios de control de información en Internet: Los usuarios tienen el derecho de contar con servicios de control ofertados por los ISP, para el control de contenidos en Internet que atenten en contra de la Ley, moral, buenas costumbres. Estos servicios deben ser debidamente explicados por el ISP.

- Datos personales: Los usuarios tienen el derecho de que se garantice la protección de sus datos personales, la libertad de expresión e información, protección como consumidor.

- Información de los servicios contratados: Sin perjuicio de la obligación de los ISP para brindar información clara y detallada sobre los servicios ofertados y contratados por los usuarios, corresponde a los usuarios mantenerse debidamente informados sobre las características de los servicios contratados y que se encuentren publicados por el ISP en su página web, o, se encuentre a su disposición por otros medios que disponga el ISP.

3.3.7 Lineamientos hacia la entidad reguladora

- Lineamientos sobre neutralidad de la red: Emisión de lineamientos para protección del principio de neutralidad de la red, siguiendo el mecanismo dispuesto en la LOT, es decir:

a) Elaboración del proyecto de lineamientos que debe ser puesto a disposición de revisión del público en general, con la finalidad de recibir los aportes necesarios.

b) Realización de los talleres conjuntos de trabajo entre el regulador y el sector de empresas que brindan el servicio de acceso a Internet, los usuarios y demás interesados.

c) Emisión de lineamientos sobre la neutralidad de la red para el cumplimiento de todos los actores que forman parte de este ecosistema.

d) Determinar causales básicas y sus características, de lo que pueden constituir situaciones de emergencia o de fuerza mayor en contra de la neutralidad de la red, en función de las cuales, los operadores del servicio de acceso a Internet puedan tomar acciones de control.

- Protección de datos: El regulador debe actuar de tal manera que garantice la protección de los datos personales de los usuarios en el uso del servicio de acceso a Internet.

- Potestad sancionadora: El organismo de regulación y control de las telecomunicaciones tiene la facultad de sancionar las infracciones cometidas en contra de garantizar la neutralidad de la red; no obstante para ello, es necesario que se observen los debidos procesos establecidos en el ordenamiento jurídico vigente.

- Difusión de los lineamientos sobre la neutralidad de la red: Generar en conjunto con los operadores de servicios de telecomunicaciones de Acceso a Internet, proveedores de aplicaciones, contenidos y servicios en Internet una adecuada difusión de los lineamientos sobre neutralidad de la red.

3.4 Plan de acción de mejora continua

A continuación se propone un plan de acción básico y sencillo suponiendo que dentro de la normativa ecuatoriana se evalúe incluir lineamientos enfocados a definir de manera más detallada sobre el principio de la neutralidad de la red; de esta manera, el plan de

acción que se describe se define en base al ciclo de mejora continua o círculo de Deming, también denominado Ciclo PDCA o PHVA, de las siglas “Plan, Do, Check, Act” (Planificar, Hacer, Verificar y Actuar).

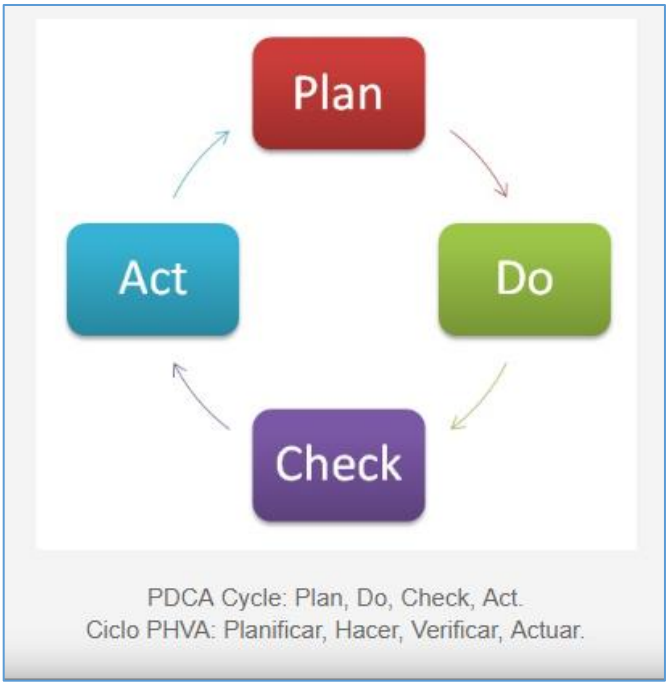

Figura 20: Ciclo PHVA: Planificar, Hacer, Verificar, Actuar

Fuente: (Bernal, 2018)

3.4.1 Planificar (Plan)

Dentro de la planificación, será necesario que las entidades gubernamentales del sector de telecomunicaciones establezcan a través de los procesos definidos en la LOT, las directrices o lineamientos sobre la aplicación de la neutralidad de la red en el Ecuador; para ello, se debe adecuar de la mejor manera, la comunicación con todos los actores del ecosistema que forman parte de Internet, la determinación de las directrices propiamente dichas y las acciones que en lo posterior se deriven de la aplicación de la regulación sobre este principio.

3.4.2 Hacer (Do)

Esta parte del ciclo constituye el hecho de llevar a cabo lo planificado que, en relación a los lineamientos de neutralidad de la red, es la emisión de los lineamientos o directrices

sobre este principio a través de un reglamento o norma técnica, con la finalidad que en adelante sea cumplida por los diferentes actores en Internet.

3.4.3 Controlar o verificar (Check)

Una vez ejecutadas las acciones descritas, será necesario que tanto el regulador como los usuarios, proveedores del servicio de acceso a Internet, proveedores de contenidos, aplicaciones y servicios en esta red revisen la ejecución de lo planeado en torno a las directrices establecidas en referencia a la neutralidad de la red, a través de procesos de valoración de impacto y evaluaciones de resultados obtenidos por la aplicación de los lineamientos.

Esto permitirá desarrollar un historial y una serie de documentación que permita mejorar los procedimientos adoptados.

3.4.4 Actuar (Act)

Con base en la referencia de la evaluación de aplicación de lineamientos sobre neutralidad de la red se podrá evaluar la forma de mejora que se pueda llevar a cabo, como por ejemplo: refuerzo de educación sobre el uso de Internet, implementar mecanismos adicionales de extensión de uso de Internet, incentivando a los usuarios, empresas, prestadores del servicio de acceso a Internet y mejorando los procesos de verificación y seguimiento positivos del organismo regulador a través de evaluaciones proactivas y disminuyendo en lo posible aspectos de carácter sancionatorio.

4 CONCLUSIONES Y RECOMENDACIONES

Con la finalización del presente trabajo, a continuación se presentan las siguientes conclusiones y recomendaciones

4.1 Conclusiones

La red Internet ha tenido un desarrollo evolutivo extraordinario desde su aparición y ha sido un importante motor de innovación en donde se alberga una enorme cantidad de información que crece de manera diaria y que se encuentra a disposición de las personas alrededor del mundo.

Se ha evidenciado que el desarrollo del acceso a Internet alrededor del mundo tiene aún camino por recorrer, sin embargo el uso del acceso a contenidos, aplicaciones, información o servicios contenidos se ha visto incrementado de manera exponencial durante los últimos años, lo cual hace necesario que existan lineamientos para un uso adecuado de esta potente herramienta.

Internet es una red global y un ecosistema en el cual interactúan varios actores como son: la propia red global, proveedores de acceso a Internet, proveedores de contenidos, aplicaciones y servicios en Internet, usuarios, Gobiernos y entidades reguladoras.

El principio de la neutralidad de la red ha sido un tema de debate a nivel mundial desde hace varios años y se ha constatado que existen varios lugares en el mundo en los cuales, los Gobiernos han optado por expedir directrices para el tratamiento dentro de sus naciones de este importante principio.

En base a lo revisado se puede concluir que el principio de la neutralidad de la red, de manera generalizada se refiere a un Internet libre y abierta a todos los usuarios que trata sin discriminación todo el tráfico que existe en Internet; no obstante es necesario también tomar acción sobre aspectos como perjuicios que pueden ocasionarse a la red, lo cual hace que existan excepciones para una gestión apropiada del tráfico que circula en esta red

global. Con base en las revisiones efectuadas, también es importante resaltar que la información en Internet tiene sus propias características de acuerdo a la clase de datos; es decir por ejemplo que, la información puramente de datos tiene características propias de uso de ancho de banda y velocidades que información de video, cuyas características tendrán por consecuencia características diferentes.

Durante el desarrollo de este trabajo, se ha constatado en base al análisis comparativo entre varios países que a pesar que existe la implementación de regulación sobre la neutralidad de la red en algunos de ellos, en una de las potencias mundiales como es los Estados Unidos de Norte América, durante el año 2018 se ha optado por deshacer los lineamientos que fueron generados en el año 2015, cuyas consecuencias deberán ser evaluadas por el impacto que puedan causar, en otras regiones del mundo.

Dentro del establecimiento de directrices sobre la neutralidad de la red, Chile ha sido el país pionero sobre el desarrollo de normativa expresa al respecto; de esta manera, ha sido un ejemplo referencial para el análisis y regulación de este principio en otros países del mundo.

En la realización de este trabajo se ha llegado a la conclusión de que para el tratamiento de la neutralidad de la red, principalmente deben observarse las aristas como: la gestión de tráfico, transparencia de la información, la provisión de contenidos, aplicaciones y servicios sobre Internet, calidad del servicio, bloqueo de información, lo cual a su vez tiene una incidencia directa sobre las cuestiones sociales, técnicas y de la propia comunicación.

En torno a la neutralidad de la red, se concluye con fundamento en el ejercicio comparativo efectuado que es adecuado que, a nivel normativa se puede establecer lineamientos que permitan una aplicación correcta de este principio por parte de todos quienes intervienen en la prestación del servicio de acceso a Internet; de tal modo que, se ha planteado estos lineamientos a fin de ser considerados como reglas claras para la gestión de tráfico, transparencia, manejo adecuado en torno a los contenidos y aplicaciones que podrían efectuar los prestadores del servicio de acceso a Internet en el país y el manejo de la información bajo un marco general de legalidad en favor de los usuarios del servicio de acceso a Internet.

4.2 Recomendaciones

Una vez que se ha planteado de manera referencial un conjunto de lineamientos normativos en torno a la neutralidad de la red que pueden ser observados en el futuro, se ha podido evidenciar la importancia que tiene el papel que desempeña cada uno de los componentes del ecosistema de Internet; de esta forma, surgen algunas recomendaciones generales que podrían tomarse en cuenta, como:

- Acerca de los lineamientos: Como se ha visto en el transcurso del desarrollo de este trabajo, será indispensable que los lineamientos que en referencia a la neutralidad de la red se desarrollen en el país, sean inclusivos y claros para todos los actores que intervienen en el ecosistema de Internet, además que los mismos sean definidos de manera independiente a la LOT

- Desarrollo de las redes: Las políticas gubernamentales del país deben incentivar el desarrollo de las redes de los servicios de telecomunicaciones, al caso referido en este caso el de Internet, con la finalidad de que en el Ecuador, las zonas remotas y rurales puedan contar con el acceso a la información que se encuentra en esta red global.

- Privacidad de datos y seguridades de la red: En el uso de Internet, debe garantizarse la protección de la privacidad de los datos de los usuarios; de igual manera, los controles de la seguridad en la misma deben ser de acuerdo a la naturaleza de las amenazas, buscando la protección de prestadores del servicio de acceso a Internet y los usuarios.

- Innovación: Cualquier persona natural o jurídica puede introducir aplicaciones, contenidos y servicios en la red de Internet, de tal modo de enriquecer la información que se encuentra en dicha red; es preponderante de igual manera la innovación al respecto a través de estándares abiertos.

- Contenidos, aplicaciones y servicios en Internet: En el contexto de lo tratado, no se ha pretendido o se pretende listar lineamientos sobre regulación de la información u opinión que se emitan en Internet por cuanto no se ha implementado normativa

específica al respecto; no obstante, las medidas que dentro del país se establezcan en cuanto a la neutralidad de la red deben ser positivas para procurar la diversidad de contenidos en la red, de manera plural y diverso, dentro de límites legales y reconociendo el valor del conocimiento que sea intercambiado. Se debe de igual manera, educar a los usuarios de diversas maneras (centros educativos, a través de las operadoras de servicios de telecomunicaciones, programas gubernamentales), sobre la naturaleza de Internet, sus peligros, ventajas, desventajas; de esta forma, los usuarios tendrán la información necesaria sobre la elección de las comunicaciones en la red.

Se recomienda que cualquier iniciativa en el Ecuador que apunte a establecer lineamientos o reglas específicas para la neutralidad de la red, se generen en base a la participación pública de todos los actores que forman parte del ecosistema de Internet y salvaguardando los derechos de los usuarios consagrados en la Constitución de la República y ordenamiento jurídico vigente.

Se recomienda que a través de las políticas gubernamentales, se incentive la expansión del acceso a Internet en todas las regiones del país y en particular en aquellas zonas en las cuales hace falta dicho acceso, a través de alianzas con empresas privadas y públicas y a través de incentivos para ello, favoreciendo de esta forma el conocimiento y el acceso a la información para beneficio de la sociedad en general.

Se recomienda que en cuanto a aspectos de carácter técnico, la normativa prevea la existencia de una calidad de servicio mínima para asegurar el envío y recepción de información de manera aceptable y adecuada, en función de análisis pormenorizados no solo de las prácticas adoptadas en diferentes países sino analizando de manera objetiva la realidad del desarrollo del servicio en el país.

Se recomienda la adopción de lineamientos claros y adecuadamente bien definidos en torno a la neutralidad de la red que permita un apropiado acceso a la información de Internet por parte de los usuarios, así como una adecuada gestión de tráfico tomando en cuenta los aspectos de riesgo de la red, mal o ilegal uso de Internet, calidad del servicio, congestión de la red y situaciones de emergencia.

Se recomienda que los proveedores de acceso a Internet actúen con transparencia frente a los usuarios, informando de manera clara y detallada acerca de las ofertas comerciales que son ofertadas y contratadas, los aspectos tarifarios y aspectos de gestión de la red que podrían eventualmente presentarse; además que los mismos, proporcionen a los usuarios conexiones sin ninguna clase de restricción, bloqueo, ralentización de cualquier información, contenido, aplicación y/o servicio en Internet.

Finalmente, se recomienda mantener a la red de Internet como una red abierta y como un medio de comunicación libre en donde se respete los derechos de los usuarios y el derecho al acceso a información que contribuye sin duda al progreso de la sociedad y de todos los países alrededor del mundo.

REFERENCIAS

1. Comisión Europea. (10 de noviembre de 2018). *Mercado Único Digital*. Obtenido de Mercado Único Digital: https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-2018-report

2. ARCOTEL. (6 de mayo de 2016). Reglamento para la prestación de servicios de telecomunicaciones y de audio y video por suscripción. Quito, Pichincha, Ecuador.

3. ARCOTEL. (2017). BOLETÍN ESTADÍSTICO. *BOLETÍN ESTADÍSTICO*, 20.

4. Asamblea Nacional. (2008). *Constitución de la República del Ecuador.*

5. ASIET. (10 de noviembre de 2018). *Asociación Interamericana de Empresas de Telecomunicaciones*. Obtenido de Asociación Interamericana de Empresas de Telecomunicaciones: https://asiet.lat/sobre-asiet/

6. BEREC. (2016). *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.*

7. Bernal, J. J. (18 de noviembre de 2018). *Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua*. Obtenido de Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua: https://www.pdcahome.com/5202/ciclo-pdca/

8. BIWEBZONE. (2018). *¿Cuál es el origen de Internet?* Obtenido de ¿Cuál es el origen de Internet?: http://www.biwebzone.com/FrontPageLex/1GENINICIOMFBWZCRRJ.php?IdPort=2810809917

9. Carboni, O. V., & Labate, C. (2018). América Latina por una red neutral: el principio de neutralidad in Chile y Brasil. *Famencos*, 12 - 15/21.

10. CEPAL. (2018). *La nueva revolución digital. De la Internet del consumo a la Internet de la producción.* Santiago de Chile: CEPAL.

11. CIDH. (2013). Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. En CIDH, *Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión* (pág. 30).

12. CIDH, C. I. (22 de noviembre de 1969). *Convención Americana sobre Derechos Humanos*. Obtenido de Convención Americana sobre Derechos Humanos: https://www.cidh.oas.org/Basicos/Spanish/Basicos2.htm

13. CIDH, C. I. (2014). *Declaración conjunta sobre universalidad y el derecho a la libertad de expresión*. Obtenido de Declaración conjunta sobre universalidad y el derecho a la libertad de expresión: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=945&lID=2

14. Comisión Presidencial, C. d. (2011). *Pacto Internacional de Derechos Civiles y Políticos.* Obtenido de Pacto Internacional de Derechos Civiles y Políticos: http://www.copredeh.gob.gt/

15. DATATECA. (2018). *Elementos de conexión a Internet*. Obtenido de http://datateca.unad.edu.co/contenidos/MDL000/ContenidoTelematica/elementos_de_conexin_a_internet.html

16. Departamento de Justicia de EE.UU. (2 de noviembre de 2002). *Juicio Final_ US. v. Microsoft Corporation*. Obtenido de Juicio Final_ US. v. Microsoft Corporation: https://www.justice.gov/atr/case-document/final-judgment-133

17. Digital Report; Exito Exportador. (noviembre de 2018). *Digital Report; Exito Exportador*. Obtenido de Digital Report; Exito Exportador: https://digitalreport.wearesocial.com/;http://www.exitoexportador.com/stats2.htm

18. Espinoza, P. F., & González, M. E. (2015). La neutralidad en la red y los fundamentos de su aplicación como principio general en el derecho. *La neutralidad en la red y los fundamentos de su aplicación como principio general en el derecho*. Santiago de Chile, Chile.

19. Estrada Garavilla, M. (octubre de 2018). *Delitos informáticos.* Obtenido de Université de Fribourg: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

20. FCC. (26 de febrero de 2015). FCC adopta reglas sólidas y sostnibles para proteger el Internet abierto. *FCC adopta reglas sólidas y sostnibles para proteger el Internet abierto*. Washingtong, Washingtong, Estados Unidos: FCC.

21. France, 2. (12 de junio de 2018). *Estados Unidos: llegó el fin de la neutralidad de la red.* Obtenido de Estados Unidos: llegó el fin de la neutralidad de la red: https://www.france24.com/es/20180612-estados-unidos-fin-neutralidad-internet

22. Fundación Telefónica. (2011). *Neutralidad de red:Aportaciones al debate.* Madrid: Ariel S.A.

23. Gestión. (30 de octubre de 2018). *Gestión*. Obtenido de Gestión: https://gestion.pe/tecnologia/dia-internet-datos-ciberespacio-peru-233846

24. Global Digital. (2018). *Informe Digital 2018.*

25. GSMA. (2018). *Manual de políticas públicas de telecomunicaciones móviles_una guía de temas clave.* Niall Magennis.

26. Guerrero, N. L., & Chávez, L. A. (1 de noviembre de 2015). Neutralidad de la red, perspectiva desde el ámbito regulatorio de las telecomunicaciones. *Neutralidad de la red, perspectiva desde el ámbito regulatorio de las telecomunicaciones*. México, México.

27. HSI. (2018). *Lista de proveedores de Internet en Estados Unidos*. Obtenido de Lista de proveedores de Internet en Estados Unidos: https://www.highspeedinternet.com/es/companias-de-internet

28. Huichalaf, P. (2015). *La Neutralidad de la Red: El Caso Chileno*. Obtenido de La Neutralidad de la Red: El Caso Chileno: http://www.regulatel.org/wordpress/wp-content/uploads/2015/07/4.Neutralidad_de_la_red_version%20final.pdf

29. INEC. (2018). *Tecnologías de la Información y Comunicación.* Quito.

30. José Luis González San Juan. (15 de septiembre de 2016). Neutralidad de red en Internet. *Neutralidad de red en Internet*. Salamanca, España, España: Ibersid.

31. Knoema. (2018). *Atral mundial de datos_Brasil_Temas_Telecomunicaciones_Servicios de Telecomunicaciones*. Obtenido de Atral mundial de datos_Brasil_Temas_Telecomunicaciones_Servicios de Telecomunicaciones: https://knoema.es/

32. Latina, D. D., & Intervozes. (2017). *Neutralidad de red en América Latina.* Sao Paulo: Hiperativa Comunicación.

33. Marsden, C. T. (2012). Neutralidad de la Red: Historia, regulación y futuro. *IDP*, 2-20.

34. Mexicanos, C. G. (13 de agosto de 2014). Ley Federal de Telecomunicaciones y Radiodifusión. *Ley Federal de Telecomunicaciones y Radiodifusión*. México, México, México.

35. MINTEL. (2016). *Plan Nacional de Telecomunicaciones y Tecnologías de la Información.* Quito.

36. MINTIC. (2018). Boletín trimestral de las TIC_Cifras Primer Trimestre de 2018. *Boletín trimestral de las TIC_Cifras Primer Trimestre de 2018*, 7-8/52.

37. Naciones Unidas. (2015). *Declaración Universal de los Derechos Humanos.*

38. Oliver, E., & Peña, M. (octubre de 2018). *Todo lo que debes saber sobre la ley de Neutralidad de la red*. Obtenido de Todo lo que debes saber sobre la ley de Neutralidad de la red: https://es.digitaltrends.com/computadoras/todo-sobre-la-ley-de-neutralidad-de-la-red/

39. ONTSI. (2017). *Estudio de uso y actitudes de consumo de contenidos digitales.* Quito: iclaves.

40. Pereda, C. (26 de febrero de 2015). *EE UU blinda la neutralidad en la Red*. Obtenido de EE UU blinda la neutralidad en la Red: https://elpais.com/tecnologia/2015/02/26/actualidad/1424974386_348813.html

41. REGULATEL. (2015). *Grupo de Trabajo- Neutralidad de la Red y Gobernanza de Internet.* Chile.

42. Reicher, A. (enero de 2011). *Redefiniendo la Neutralidad de la Red luego de Comcast v. FCC*. Obtenido de Redefiniendo la Neutralidad de la Red luego de Comcast v. FCC: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1888&context=btlj

43. Reuters. (7 de abril de 2010). *La FCC no puede impedir que una operadora sancione a usuarios de P2P en EEUU*. Recuperado el 21 de octubre de 2018, de La FCC no puede impedir que una operadora sancione a usuarios de P2P en EEUU: https://www.elmundo.es/elmundo/2010/04/07/navegante/1270625650.html

44. Rezende-Mediatelecom, J. (30 de enero de 2018). *El sector de telecomunicaciones y el mundo de Internet (Análisis).* Obtenido de https://www.arenapublica.com/articulo/2018/01/30/9346/internet-telecomunicaciones-regulacion-infraestructura-mundo-digital-legislar-politica-analisis

45. Rodríguez, M. M. (21 de abril de 2017). Neutralidad de Red en Perú: Una Retrospectiva. *Derecho & Sociedad N° 49 / pp 203 - 219*, 203 - 219.

46. Ruiz Gómez, L. M. (2014). *Análisis de la competencia y neutralidad de red.* ICE.

47. Society, I. (marzo de 2017). Perspectivas de Internet Society (ISOC) sobre el bloqueo de contenido en Internet:Visión General. *Perspectivas de Internet Society (ISOC) sobre el bloqueo de contenido en Internet:Visión General*. Ginebra, Suiza, Suiza: Internet Society.

48. Statista. (2018). *Número de usuarios de Internet en Brasil entre 2013 y 2019 (en millones)*. Obtenido de Número de usuarios de Internet en Brasil entre 2013 y 2019 (en millones): https://es.statista.com/estadisticas/598921/brasil-numero-de-usuarios-de-internet--2019/#0

49. Subsecretaria de Telecomunicaciones - SUBTEL. (15 de diciembre de 2010). Decreto 368. *Reglamento que regula las características y condiciones de la neutralidad de la red en el servicio de acceso a internet*. Chile.

50. Subsecretaría de Telecomunicaciones - SUBTEL. (18 de agosto de 2010). Ley 20453. Chile.

51. SUPERTEL. (2017). *Compendio histórico de las telecomunicaciones en Ecuador*. Quito: SUPERTEL.

52. TeleSemana. (octubre de 2018). *Panorama de mercado.* Obtenido de Panorama de mercado : https://www.telesemana.com/panorama-de-mercado

53. ThingLink. (2018). *Cambio 16*. Obtenido de Cambio 16: https://www.cambio16.com/mundo/censura-en-internet-2018/

54. UEES, U. E. (2017). *Antecedentes y situación del e-commerce en Ecuador*. Quito: UEES.

55. UIT. (2017). *Manual de Regulación sobre calidad de servicio* .

56. Universidad de Chile. (1996). *Evolución de internet.* Obtenido de Evolución de internet: http://www.periodismo.uchile.cl/talleres/internet/evoluciondeinternet.pdf

57. Wikypedia. (5 de septiembre de 2016). *Ley de neutralidad en la red (Chile)*. Obtenido de Ley de neutralidad en la red (Chile): https://es.wikipedia.org/wiki/Ley_de_neutralidad_en_la_red_(Chile)#cite_note-4

58. Wu, T. (2 de febrero de 2015). *http://timwu.org/*. Obtenido de http://timwu.org/: http://timwu.org/

ANEXOS

Anexo 1: Componentes Cadena Valor

Hardware: Se refiere a los elementos físicos que permiten al usuario el recibir y enviar información, mismos que son, en primer lugar, el computador personal (PC), la portátil o Tablet, además de los teléfonos móviles o los propios televisores que dispongan de un teclado.

Luego, un módem, cuya finalidad es ser el medio de entendimiento entre las series análogas que transportan las líneas telefónicas y las señales digitales que son transportadas por los computadores.

Se sigue con la conexión, que es el mecanismo de enlace que existe entre el computador y la red de Internet, lo cual permitirá el acceso a la información que se encuentra en ella.

Software: En cuanto a software, se requiere básicamente de un sistema operativo que controla la computadora y gestiona los archivos, desenvolvimiento del hardware y pérdida de datos; un navegador, que es la interfaz que permite a los usuarios acceder a los diferentes sitios de Internet.

Protocolo TCP/IP: Son normas que se emplean en la comunicación por Internet y describe un conjunto de guías generales de operación que permite a los equipos poder comunicarse en una red, proporcionando conectividad de extremo a extremo y especificando como los datos deben ser tratados en su generación, dirección, transmisión, enrutamiento y recepción por parte de los destinatarios.

Con ello, el Proveedor de Servicios de Internet puede asignar a cada computador conectado a Internet una dirección (IP), con lo que puede efectuar comunicación con otras.

Proveedor de servicios de Internet (ISP): Son aquellas empresas que se encargan de proveer el acceso a esta inmensa red; funciona en base a proporcionarse al usuario un número telefónico (que será llamado por el módem). Con el establecimiento de la conexión, el usuario puede acceder al uso de Internet.

Proveedores de contenidos (ICPs), aplicaciones (IAPs) y/o servicios en Internet: Son aquellas empresas que brindan sus servicios (por ejemplo, espacio en la nube), contenido (dueños de sitios web) y aplicaciones (Gmail, Outlook) a través de las redes de Internet que han sido construidas por parte de los ISP's.

Usuario: Es toda aquella persona natural o jurídica que hace uso de los servicios de telecomunicaciones, en este caso del servicio de acceso a Internet. En la sociedad en general, como usuarios de Internet se encuentran los usuarios finales, empresas en general (Grandes empresas, PYMES, micro empresas) las instituciones de distinta índole.

Gobierno: Son los encargados de generar las políticas en cuanto a las prestación de los diferentes servicios en el país, en este caso el de telecomunicaciones de acceso a Internet.

Fuente: (DATATECA, 2018)

Anexo 2: Proveedores de Acceso a Internet_países

País	Proveedores
El Salvador	Claro, Digicel, ESAMSAT,[2] IBW, Movistar, Tigo, IBW, Japi.
España	Movistar España, Vodafone España, Orange España, Yoigo, R, Euskaltel, Telecable, Adamo Telecom, entre otras.
Chile	Bynarya, Claro Chile, Julero CMET, Entel Chile, GTD Manquehue, Movistar Chile, Netsouth, Nextel Chile, Optic Wisp, Steel, Telefónica del Sur, VTR, entre otras.
Argentina	8Bits servicios de Internet, Cotelcam (Tigre, Bs. As.), Cablenet (Galvez, Sta Fe.), Arnet (Telecom Argentina), DIRECTV / Cablevisión / Fibertel (Grupo Clarín), Gigared, Optical ISP, Anylink (Anylink Argentina SA), Mundo Satelital, Sion, Skymax, TELEINTER S.R.L y SkyServ, entre otras.
Colombia	Claro Colombia, Colombia Mas TV, DirectTV, ETB, UNE, Telefónica, TIGO, Red Uno S.A, Movistar Colombia.
Venezuela	CANTV, Inter (Venezuela), Movilnet filial de CANTV, Movistar Venezuela, Digitel y Totalcom Venezuela.
México	GDLIcanet, Gemtel, Kiwi Networks, Totalplay Telecomunicaciones, Telnor, Axtel, Izzi Telecom (Cablemas, Cablevision, Cablecom), Megacable, Prodigy Internet de Telmex, EnlaceTPE (Totalplay Empresarial), Star Go
Panamá	Claro, Cable and Wireless Panamá, Cable Onda, Digicel, Movistar, Telecarrier, entre muchos otros más.
Estados Unidos	Comcast, Time Warner Cable, AT&T, Cox Communications, Charter Communications, Google Fiber, Verizon entre muchos otros más.
Perú	Americatel, Claro (Perú), Movistar del Perú, Entel, Optical Networks, Telmex, ColinaNet, MegaCableNet, Inventa Telecomunicaciones, WIN , iWAY telecom sac.
Guatemala	Claro, Movistar, Tigo, Intertelco, IBW.
Costa Rica	Claro, Instituto Costarricense de Electricidad (ICE), Movistar, Tigo.
Ecuador	Telconet, CNT E.P.COMPU DIGIT@LL, MaxFib, SITERTL, Claro, Grupo TV Cable, Igotel, Puntonet, Clicknet , Turbonet, PROANET ROCAFUERTE, SilviaNET entre muchos otros más.
Paraguay	Claro, Personal, Tigo, Vox (Paraguay), entre muchos otros más.
Uruguay	Antel (empresa estatal, principal proveedor de servicios de Internet y telecomunicaciones), TCCvivo, Claro, Dedicado, Movistar, entre otras.
Bolivia	AXS Bolivia, Cotas Bolivia, Entel, Tigo y Viva Bolivia.
República Dominicana	Claro, Altice y Viva.

Fuente: (Wikypedia, 2016)

Anexo 3: Descripción de contenido en Internet

Contenido audiovisuales: información con enfoque a la televisión.

Sector de la música: desarrollo de los servicios de ***streaming***, radio en línea.

Videojuegos: obras audiovisuales con recursos gráficos, sonoros, audiovisuales o literarios.

Juegos en línea: videojuegos jugados a través de Internet por una o varias personas.

Libros digitales: información provista por fuentes oficiales y editores que puede ser adquirida mediante pago o no pago por los lectores.

Prensa digital: realizada por editores de periódicos para acceso a noticias.

Contenidos generados por usuarios: que son abordados desde diferentes perspectivas de mercado, implicando aspectos de propiedad intelectual.

Redes sociales: son un contenido en sí mismas y son actualmente uno de los principales accesos al resto de contenidos digitales.

Contenidos digitales para la educación: de acuerdo a tendencias del mercado y desarrolladas para aplicación en la enseñanza.

Aplicaciones móviles: que se desarrollan de acuerdo a las tendencias del mercado de consumo de los usuarios y sus necesidades.

Fuente: (ONTSI, 2017)

Anexo 4: Instituciones relacionadas con temas de Internet

ICANN: En español Corporación de Internet para la Asignación de Nombres y Números, creada en 1998 y se encarga de la preservación de la estabilidad operacional de Internet; responsable de asignar espacio de direcciones numéricas de IP, identificadores de protocolos y administración del sistema de servidores raíz.

W3C: Consocio Mundial de la Web, creada en 1994 y se encarga de producir recomendaciones para Internet.

ISOC: Sociedad de Internet, creada en 1991 no gubernamental y sin ánimo de lucro, se encarga de manera exclusiva al desarrollo mundial de Internet como un centro de coordinación global en el desarrollo de protocolos y estándares compatibles.

IETF: Fuerza de Labor de Ingeniería de Internet creada en EE.UU. en 1986 como una organización internacional sin fines de lucro con el objetivo de normalización y estandarización para la mejora de Internet.

Otras Instituciones: Foro de Gobernanza de Internet (IGF); la Cumbre Mundial de la Sociedad de Internet (WSIS), la Organización Internacional para la estandarización (ISO), etc.

Fuente: (Guerrero & Chávez, 2015)

Anexo 5: Factores - Impacto en la sociedad por el uso de Internet

Aspectos positivos:

- Información inmediata: Se encuentra información de fuentes de una forma directa, lo que permite a los usuarios de mayor información y de modo ágil: noticias de distinta índole, compras, entretenimiento, aplicaciones, etc.

- Beneficios en la educación: Con el apoyo de las nuevas tecnologías, se facilita a las personas el acceso a la educación de manera remota y el acceso a la información que existe en Internet, lo cual puede permitir el desarrollo del intelecto y capacitaciones en zonas alejadas de aquellas que son céntricas.

- Beneficios en el área de la salud: Con el acceso a la información que se encuentra en Internet, se promueve la circulación de datos sobre el cuidado de la salud, información sobre sitios de atención en salud, tele salud para acceso en zonas remotas.

- Beneficios en empleo: Sin duda el acceso a la información que existe en Internet aporta para facilitar cualquier trabajo, además de beneficiar la práctica del trabajo a distancia que además ahorra en desplazamientos que pudieran ser considerados innecesarios.

- Innovación: Permite sin lugar a dudas el desarrollo de nuevas ideas por parte de los usuarios en general, que luego pueden ser puestas a disposición de todas las personas a través de Internet, apoyando el desarrollo de la sociedad y emprendimientos en general.

Aspectos negativos:

- Brecha digital: No obstante que en los últimos años el acceso a Internet ha sido muy importante en los diferentes países, aún queda mucho por hacer para que dicho acceso se extienda hacia más lugares en el mundo; responsabilidad que corresponde a los diferentes Gobiernos y las políticas que decidan adoptar.

- Piratería: Es conocida comúnmente como aquella reproducción no autorizada de obras por parte de terceros. En el Ecuador, la Ley de Propiedad intelectual penaliza a través de su artículo 325 la piratería y establece acción de prisión y multa para quienes violen los derechos de autor o derechos conexos.

Fraudes informáticos:

Existe un conjunto de delitos informáticos que se encuentran reconocidos por la Organización de las Naciones Unidas (ONU) y son (Estrada Garavilla, 2018):

- Fraudes cometidos mediante manipulación de computadoras: Comprende: manipulación de los datos de entrada; manipulación de programas; manipulación de datos de salida; fraude efectuado por manipulación informática.

- Falsificaciones informáticas: Comprende: falsificaciones como objeto; falsificaciones como instrumentos.

- Daños o modificaciones de programas o datos computarizados: Comprende: sabotaje informático (virus, gusanos, bomba lógica o cronológica); acceso no autorizado a servicios y sistemas informáticos (piratas informáticos o hackers); reproducción no autorizada de programas informáticos de protección legal.

- Delitos contra propios sistemas: Comprende: acceso no autorizado; destrucción de datos; infracción de copyright de base de datos; interceptación de correo electrónico; estafas electrónicas; transferencia de fondos.

- Delitos soportados en Internet: Comprende: espionaje; terrorismo; narcotráfico; tráfico de armas; proselitismo de sectas; propaganda de grupos extremistas; extorsión; ciberpiratería; ciberviolencia; ciberabuso.

A. Fraudes cometidos mediante manipulación de computadoras. a) Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede

realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos. b) La manipulación de programas: es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. c) Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito. d) Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica del salchichón en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. B. Falsificaciones informáticas. a) Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada. b) Como instrumentos: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos. C. Daños o modificaciones de programas o datos computarizados. a) Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son: i) Virus: es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede

ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya. ii) Gusanos: se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus. Por ejemplo, un programa gusano que eventualmente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita. iii) Bomba lógica o cronológica: exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su "detonación" puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba. b) Acceso no autorizado a servicios y sistemas informáticos: se produce por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático. i) Piratas informáticos o hackers: el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema. c) Reproducción no autorizada de programas informáticos de protección legal: ésta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido

a que el bien jurídico a tutelar es la propiedad intelectual. Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son: a) Acceso no autorizado: uso ilegitimo de contraseñas y la entrada de un sistema informático sin la autorización del propietario. b) Destrucción de datos: los daños causados en la red mediante la introducción de virus, bombas lógicas, etc. c) Infracción al copyright de bases de datos: uso no autorizado de información almacenada en una base de datos. d) Interceptación de correo electrónico: lectura de un mensaje electrónico ajeno. e) Estafas electrónicas: a través de compras realizadas haciendo uso de la red. f) Transferencias de fondos: engaños en la realización de actividades bancarias electrónicas. Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos: a) Espionaje: acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos. b) Terrorismo: mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. c) Narcotráfico: transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas. d) Otros delitos: las mismas ventajas que encuentran en el Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o viceversa.

Fuente: (Estrada Garavilla, 2018)

Anexo 6: Principio de NR Chile

Tipo Norma	:Ley 20453
Fecha Publicación	:26-08-2010
Fecha Promulgación	:18-08-2010
Organismo	:MINISTERIO DE TRANSPORTES Y TELECOMUNICACIONES; SUBSECRETARÍA DE TELECOMUNICACIONES
Título	:CONSAGRA EL PRINCIPIO DE NEUTRALIDAD EN LA RED PARA LOS CONSUMIDORES Y USUARIOS DE INTERNET
Tipo Versión	:Única De : 26-08-2010
Inicio Vigencia	:26-08-2010
Id Norma	:1016570
URL	:https://www.leychile.cl/N?i=1016570&f=2010-08-26&p=

LEY NÚM. 20.453

CONSAGRA EL PRINCIPIO DE NEUTRALIDAD EN LA RED PARA LOS CONSUMIDORES Y USUARIOS DE INTERNET

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente proyecto de ley, iniciado en Moción de los Diputados señores Gonzalo Arenas Hodar; Marcelo Díaz Díaz; Enrique Estay Peñaloza; Alejandro García-Huidobro Sanfuentes; Patricio Hales Dib; Javier Hernández Hernández; Tucapel Jiménez Fuentes; José Antonio Kast Rist; Carlos Recondo Lavanderos, y Felipe Ward Edwards.

Proyecto de ley:

"Artículo único.- Agréganse los siguientes artículos 24 H, 24 I y 24 J en la Ley N° 18.168, General de Telecomunicaciones:

"Artículo 24 H.- Las concesionarias de servicio público de telecomunicaciones que presten servicio a los proveedores de acceso a Internet y también estos últimos; entendiéndose por tales, toda persona natural o jurídica que preste servicios comerciales de conectividad entre los usuarios o sus redes e Internet:

a) No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red. En este sentido, deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad al proveedor de acceso a Internet, según corresponda, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de éstos, habida cuenta de las distintas configuraciones de la conexión a Internet según el contrato vigente con los usuarios.

Con todo, los concesionarios de servicio público de telecomunicaciones y los proveedores de acceso a Internet podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red, en el exclusivo ámbito de la actividad que les ha sido autorizada, siempre que ello no tenga por objeto realizar acciones que afecten o puedan afectar la libre competencia. Los concesionarios y los proveedores procurarán preservar la privacidad de los usuarios, la protección contra virus y la seguridad de la red. Asimismo, podrán bloquear el acceso a determinados contenidos, aplicaciones o servicios, sólo a pedido expreso del usuario, y a sus expensas. En ningún caso, este bloqueo podrá afectar de manera arbitraria a los proveedores de servicios y aplicaciones que se prestan en Internet.

b) No podrán limitar el derecho de un usuario a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y que los mismos no dañen o perjudiquen la red o la calidad del servicio.

c) Deberán ofrecer, a expensas de los usuarios que lo soliciten, servicios de controles parentales para contenidos que atenten contra la ley, la moral o las buenas costumbres, siempre y cuando el usuario reciba información por adelantado y de manera clara y precisa respecto del alcance de tales servicios.

d) Deberán publicar en su sitio web, toda la información relativa a las

características del acceso a Internet ofrecido, su velocidad, calidad del enlace, diferenciando entre las conexiones nacionales e internacionales, así como la naturaleza y garantías del servicio.

El usuario podrá solicitar al concesionario o al proveedor, según lo estime, que le entregue dicha información a su costo, por escrito y dentro de un plazo de 30 días contado desde la solicitud.

Artículo 24 I.- Para la protección de los derechos de los usuarios de Internet, el Ministerio, por medio de la Subsecretaria, sancionará las infracciones a las obligaciones legales o reglamentarias asociadas a la implementación, operación y funcionamiento de la neutralidad de red que impidan, dificulten o de cualquier forma amenacen su desarrollo o el legítimo ejercicio de los derechos que de ella derivan, en que incurran tanto los concesionarios de servicio público de telecomunicaciones que presten servicio a proveedores de acceso a Internet como también éstos últimos, de conformidad a lo dispuesto en el procedimiento contemplado en el artículo 28 bis de la Ley N° 18.168, General de Telecomunicaciones.

Articulo 24 J.- Un reglamento establecerá las condiciones mínimas que deberán cumplir los prestadores de servicio de acceso a Internet en cuanto a la obligatoriedad de mantener publicada y actualizada en su sitio web información relativa al nivel del servicio contratado, que incorpore criterios de direccionamiento, velocidades de acceso disponibles, nivel de agregación o sobreventa del enlace, disponibilidad del enlace en tiempo, y tiempos de reposición de servicio, uso de herramientas de administración o gestión de tráfico, así como también aquellos elementos propios del tipo de servicio ofrecido y que correspondan a estándares de calidad internacionales de aplicación general. Asimismo, dicho reglamento establecerá las acciones que serán consideradas prácticas restrictivas a la libertad de utilización de los contenidos, aplicaciones o servicios que se presten a través de Internet, acorde a lo estipulado en el artículo 24 H.".

Artículo transitorio.- El reglamento a que hace referencia el artículo 24 J se publicará dentro de los 90 días siguientes a la publicación de la presente ley.".

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 18 de agosto de 2010.- SEBASTIÁN PIÑERA ECHENIQUE, Presidente de la República.- Felipe Morandé Lavín, Ministro de Transportes y Telecomunicaciones.
Lo que transcribo para su conocimiento.- Saluda atentamente a Ud., Jorge Molina Osorio, Subsecretario de Telecomunicaciones Subrogante.

Anexo 7: Reglamento NR Chile

Tipo Norma	:Decreto 368
Fecha Publicación	:18-03-2011
Fecha Promulgación	:15-12-2010
Organismo	:MINISTERIO DE TRANSPORTES Y TELECOMUNICACIONES; SUBSECRETARÍA DE TELECOMUNICACIONES
Título	:REGLAMENTO QUE REGULA LAS CARACTERÍSTICAS Y CONDICIONES DE LA NEUTRALIDAD DE LA RED EN EL SERVICIO DE ACCESO A INTERNET
Tipo Versión	:Única De : 18-03-2011
Inicio Vigencia	:18-03-2011
Id Norma	:1023845
URL	:https://www.leychile.cl/N?i=1023845&f=2011-03-18&p=

REGLAMENTO QUE REGULA LAS CARACTERÍSTICAS Y CONDICIONES DE LA NEUTRALIDAD DE LA RED EN EL SERVICIO DE ACCESO A INTERNET

Santiago, 15 de diciembre de 2010.- Con esta fecha se ha decretado lo que sigue:
Núm. 368.- Vistos:

a) Lo dispuesto en los artículos 24°, 32° N° 6 y 35° de la Constitución Política de la República;
b) La ley N° 18.168, General de Telecomunicaciones, en adelante la ley;
c) El decreto ley N° 1.762, de 1977, que creó la Subsecretaría de Telecomunicaciones, en adelante también la Subsecretaría;
d) La Ley N° 19.628, Sobre Protección de la Vida Privada;
e) El decreto supremo N° 533, de 2000, y sus modificaciones, del Ministerio de Transportes y Tecomunicaciones que fijó el texto refundido del Reglamento de Tramitación y Resolución de Reclamos de Servicios de Telecomunicaciones, en adelante Reglamento de Reclamos;
f) La resolución exenta N° 698 de 2000, de la Subsecretaría, que fija indicadores de calidad de los enlaces de conexión para cursar el tráfico nacional de Internet y sistema de publicidad de los mismos;
g) La resolución exenta N° 669 de 2001, de la Subsecretaría, y sus modificaciones, que fija indicadores de calidad del servicio de acceso a Internet y publicidad de los mismos;
h) La resolución exenta N° 159 de 2006, de la Subsecretaría, que creó el Sistema de Transferencia de Información.
i) La resolución N° 1.600, de 2008, de la Contraloría General de la República, que Fija Normas sobre Exención del Trámite de Toma de Razón, y

Considerando:

a) Que, de conformidad a lo previsto en el artículo 6° de la ley, corresponde al Ministerio de Transportes y Telecomunicaciones, a través de la Subsecretaría, la aplicación y control de aquella y sus reglamentos;
b) Que, de acuerdo al inciso segundo del artículo 7° de la ley, le corresponde, asimismo, controlar y supervigilar el funcionamiento de los servicios públicos de telecomunicaciones y la protección de los derechos de los usuarios, sin perjuicio de las acciones judiciales y administrativas a que estos últimos tengan derecho;
c) Que, de acuerdo a los artículos 24°H, 24°I y 24°J de la Ley, la Subsecretaría debe velar para que los servicios, aplicaciones y contenidos de Internet sean ofrecidos sin discriminación, a la vez que el acceso por parte de los usuarios a ellos sea permitido sin restricciones arbitrarias por parte de los concesionarios o ISP.
d) Que, en concordancia con lo dispuesto en la letra b) del artículo 3° del decreto ley N° 211, la provisión del servicio de acceso a Internet se debe brindar en un régimen de libre competencia, evitando las prácticas restrictivas ilegítimas, de abuso de posición dominante o de competencia desleal, promoviendo la eficiencia y la accesibilidad del servicio.
e) Que, la tecnología inalámbrica está sujeta a fenómenos de naturaleza probabilística como la propagación de señales radioeléctricas y los niveles de tráfico instantáneo a nivel de acceso en recursos compartidos. Este hecho ha sido recogido para los servicios de voz, donde se establece un tratamiento diferenciado en la normativa de calidad de servicio para las redes fijas o locales y las móviles, basándose en el hecho que no es posible garantizar este último servicio en forma permanente, ya que la propagación de la señal y la cantidad variable de usuarios que acceden al servicio en dicha zona hace necesario que los análisis deban ser realizados en base a modelos de comportamiento probabilístico;

f) Que, a fin de poder controlar y supervigilar el efectivo cumplimiento de las obligaciones a que hace referencia la ley, es necesario establecer el procedimiento y la metodología de obtención de indicadores técnicos de calidad y tiempo de reposición de servicio de acceso a Internet de acuerdo a estándares de calidad internacionales de aplicación general como los establecidos en el Instituto Europeo de Normas de Telecomunicaciones, Organización de Estandarización de la Industria de las Telecomunicaciones, en sus Recomendaciones ETSI EG 202, 057-4 V1.2.1 (2008-07) y ETSI EG 202 057-1 V1.2.1 (2005-10);
g) Que, asimismo, para el cumplimiento de los anteriores objetivos, este Ministerio y su Subsecretaría de Telecomunicaciones están facultados para requerir información cierta respecto de los servicios de telecomunicaciones y el desempeño de los proveedores de éstos, de modo de generar estadísticas que ayuden a la toma de decisiones, en la tarea de aplicar y supervisar el cumplimiento de la normativa de telecomunicaciones y, en especial, de este reglamento;
h) Que, por su parte, conforme a lo establecido en los artículos 37° de la ley y 6°, letra k), del decreto ley N° 1.762 de la letra c) de los Vistos, los prestadores de servicios de telecomunicaciones están obligados a proporcionar los antecedentes e informes que, en uso de sus facultades, sean requeridos por la Subsecretaría;
i) Que, por último, el artículo 24° J de la ley, encomienda a la potestad reglamentaria la regulación, de un lado, de las condiciones mínimas que deberán cumplir los prestadores de servicios de acceso a internet en cuanto a la obligatoriedad de mantener publicada y actualizada en su sitio web la información relativa a los servicios ofrecidos y, de otro, las acciones que serán consideradas prácticas restrictivas a la libertad de utilización de los contenidos, aplicaciones o servicios que se presten a través de Internet, y en uso de mis atribuciones legales, dicto el siguiente,

Decreto:

Apruébase el siguiente Reglamento que dispone el artículo 24° J de la ley N° 18.168, que regula el Principio de Neutralidad de la Red para los Consumidores y Usuarios de Internet.

Título I.- Del Ámbito de Aplicación

Artículo 1°. De acuerdo a lo dispuesto en los artículos 24° H, 24° I y 24° J de la ley N° 18.168, el presente Reglamento regula el ejercicio de los derechos y obligaciones que derivan de la misma respecto al principio de neutralidad en la red, sin perjuicio de aquellas materias cuya regulación corresponda a otros cuerpos reglamentarios, según el caso.

Título II.- De las Definiciones

Artículo 2°. Sin perjuicio de las definiciones ya contempladas en la normativa de telecomunicaciones vigente, para los efectos de este reglamento se entenderá por:

a) Servicio de acceso a Internet: Servicio que permite a los usuarios acceder al contenido, información, aplicaciones u otros servicios ofrecidos por Internet;
b) ISP: Las concesionarias de servicio público de telecomunicaciones que presten servicio a los proveedores de acceso a Internet y también estos últimos, entendiéndose por tales a toda persona natural o jurídica que preste servicios comerciales de conectividad entre los usuarios o sus redes e Internet;
c) Proveedor de aplicación: Persona natural o jurídica que pone a disposición de los usuarios contenidos y/o aplicaciones en Internet a través de medios propios o de terceros;
d) Usuario: Persona natural o jurídica que goza o hace uso del servicio de acceso a Internet, en cualquier modalidad;
e) STI: Sistema de Transferencia de Información creado por la resolución exenta 159/2006 de la Subsecretaría de Telecomunicaciones;
f) PIT: Corresponde, para los efectos de la medición de los indicadores de calidad a que se refiere esta norma, al punto de intercambio de tráfico nacional de Internet, que cumple la función de agrupar e intercambiar el tráfico de dos o más ISP.
Título III.- De los Derechos y Obligaciones de los ISP y de los Usuarios

Artículo 3°. Los ISP deberán medir trimestralmente los indicadores técnicos de calidad de servicio, de acuerdo a la metodología definida en el numeral 5 de la Recomendación ETSI EG 202 057-4 V1.2.1 (2008-07) y sus anexos pertinentes.
El cálculo de los indicadores se basará en muestras estadísticamente representativas de todo el país donde los ISP presten sus servicios de acceso a Internet y se medirán separadamente según tecnología, velocidad de transmisión y nivel de calidad ofrecido, identificando dónde se ha(n) realizado la(s) medición(es).

Artículo 4°. Los ISP deberán medir, trimestralmente, el tiempo de reposición de servicio de acceso a Internet, de acuerdo a la metodología definida en el numeral 5.5 de la Recomendación ETSI EG 202 057-1 V1.2.1 (2005-10).
Para estos efectos, se entenderá por tiempo de reposición de servicio a aquel período comprendido entre el instante en que se reporta una falla de servicio por parte de cualquier usuario y el instante en que se restablece dicho servicio.

Artículo 5°. Los ISP deberán mantener publicada y actualizada la información relativa a las características de los servicios de acceso a Internet ofrecidos o contratados, según sea el caso, su velocidad, calidad del enlace, naturaleza y garantías del servicio. Dicha obligación se cumplirá mediante la publicación y difusión de la referida información en un sitio web especialmente acondicionado para estos efectos por cada ISP, el que deberá contar con un enlace destacado desde su sitio web principal.
La información que los ISP estarán obligados a proporcionar a los usuarios deberá estar redactada en idioma español y emplear definiciones conceptuales expresadas en un lenguaje técnico simple, de manera tal que permita su fácil comprensión por parte de los usuarios, pudiendo contener gráficos que permitan fácilmente a los usuarios realizar comparaciones visuales. La información suministrada deberá cumplir con criterios de inteligibilidad, homogeneidad, integridad y claridad.
En particular, los ISP deberán poner a disposición de los usuarios, al menos, la siguiente información actualizada para cada plan y/o servicio que comercialicen:

a) Características comerciales del plan o servicio ofertado y el nivel de los mismos, lo que deberá establecerse expresamente en el contrato respectivo, indicando al menos la velocidad publicitada de subida y bajada, límite de descarga y garantías del servicio.
b) Tasa de agregación o de sobreventa utilizada, expresada como 1:XX, entendiéndose como el cociente entre la suma de las velocidades contratadas de todos los usuarios conectados a un ISP y la velocidad del enlace con su respectivo PIT.
c) Indicadores técnicos de calidad de servicio, de acuerdo lo establecido en el artículo 3°, los que deberán informarse en los siguientes términos:
   1. Tiempo de acceso de usuario (login): Percentil 80 y 95 de los tiempos de login, ordenados de menor a mayor.
   2. Velocidad de transmisión de datos conseguida: Máxima, mínima, valor promedio y desviación estándar, separado para subida y bajada.
   3. Proporción de transmisiones de datos fallidas: Porcentaje de transmisiones de datos fallidas.
   4. Proporción de accesos de usuario con éxito: Porcentaje de conexiones exitosas.
   5. Retardo: Promedio y desviación estándar, medido en milisegundos.

d) Tiempo de reposición del servicio que, de acuerdo lo establecido en el artículo 4°, deberá considerar las siguientes medidas:
   1. Percentil 80 y 95 del tiempo de reposición de las fallas válidas, ordenado de menor a mayor.
   2. El porcentaje de las fallas reparadas en el tiempo objetivo que defina el propio ISP.

e) Calidad y disponibilidad del enlace, diferenciando entre las conexiones nacionales e internacionales, de acuerdo a lo establecido en la resolución exenta N° 698 de 2000 de la Subsecretaría de Telecomunicaciones.
f) Medidas de gestión de tráfico y administración de red. En caso que existan las mencionadas medidas, deberán especificarse sus características y sus eventuales efectos en el servicio prestado a los usuarios. Esto incluirá los tipos de aplicaciones, servicios y protocolos que se vean afectados, así como también

información sobre los períodos de alta demanda o de mayor carga. El ISP deberá indicar si las políticas de administración de tráfico son horarias, semanales y si es para tráficos nacionales y/o internacionales.

Asimismo, los usuarios podrán solicitar a los ISP que les entreguen por escrito, dentro del plazo de 30 días contados desde la solicitud a que hace referencia el inciso final del artículo 24° H de la Ley, toda la información relativa a las características de los planes y servicios que éstos ofrecen. Dicha información deberá contener, a lo menos, los elementos a que se hace referencia en los literales anteriores.

Artículo 6°. La Subsecretaría podrá solicitar a los ISP, a través del STI, toda la información necesaria para verificar la veracidad de los indicadores señalados en el artículo 5° y comparar sus niveles entre los distintos ISP.

Asimismo, tanto los sistemas de medición como las mediciones que deban implementar los ISP para los fines que establece este reglamento, deberán estar debidamente documentados, con el objeto de permitir su posterior fiscalización por parte de la Subsecretaría de Telecomunicaciones. Para estos fines, la Subsecretaría aprobará los protocolos de las mediciones descritas en los artículos precedentes.

Por su parte, los ISP deberán comunicar a la Subsecretaría, para su aprobación, sus protocolos de medición, debiendo informar con, a lo menos, dos meses de antelación a su entrada en vigencia, cualquier modificación a dicho protocolo.

Los ISP deberán prestar todas las facilidades técnicas que permitan a la Subsecretaría de Telecomunicaciones efectuar las mediciones que sean pertinentes en sus redes, en el ejercicio de las facultades fiscalizadoras que tiene legalmente encomendadas.

Lo dispuesto en el presente reglamento, lo es sin perjuicio de las demás facultades que competen a la Subsecretaría de conformidad a la ley.

Artículo 7°. Los ISP no podrán, arbitrariamente, bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de ésta. En este sentido, los ISP deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad al proveedor de acceso a Internet, según corresponda, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de éstos, habida cuenta de las distintas configuraciones de las conexiones a Internet, las que varían según el tipo de contrato vigente con cada usuario.

No obstante lo dispuesto en el inciso precedente, los ISP podrán tomar las medidas o ejecutar las acciones necesarias para llevar a cabo la gestión de tráfico y administración de red, en el exclusivo ámbito de la actividad que les ha sido autorizada, siempre que ello no tenga por objeto realizar acciones que afecten o puedan afectar la libre competencia.

En el caso que los ISP tomen medidas o ejecuten acciones de gestión de tráfico y/o administración de red, ello deberá ser informado a los usuarios a través de una publicación clara e inteligible de acuerdo a los términos indicados en el artículo 5°.

Artículo 8°. Se considerarán como prácticas restrictivas a la libertad de utilización de los contenidos, aplicaciones o servicios que se presten a través de Internet, las siguientes:

1) Toda aquella acción que, arbitrariamente, tienda a bloquear, interferir, entorpecer, restringir y/o de cualquier forma obstaculizar el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red, en especial, aquellas medidas de gestión de tráfico o administración de red que, en aquel carácter, afecten a los niveles de servicio contratados por el respectivo usuario.

2) Toda aquella acción que, arbitrariamente, tienda a priorizar o discriminar entre proveedores de contenidos, aplicaciones y/o usuarios. En todo caso, siempre se entenderá como arbitraria la acción de priorización o discriminación que afecte a proveedores de contenidos, aplicaciones y/o usuarios respecto de otros de similar naturaleza.

3) Toda aquella acción que impida o restrinja el derecho de los usuarios a acceder a la información veraz y actualizada relativa a las características de los servicios de acceso a Internet ofrecidos o contratados, según sea el caso, a que se

refiere el artículo 5° del presente reglamento.
4) Toda aquella acción que impida, restrinja o limite el derecho de los usuarios a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y no dañen o perjudiquen la red o la calidad del servicio prestado a terceros.

Artículo 9°. Asimismo, los ISP podrán bloquear contenidos, aplicaciones o servicios a petición expresa del usuario, sin que aquel pueda extenderse arbitrariamente a otros contenidos, aplicaciones o servicios distintos de los solicitados por el usuario. En ningún caso, este bloqueo podrá afectar de manera arbitraria a los proveedores de servicios y a las aplicaciones que se encuentran en Internet. Los ISP deberán tener disponible, para los usuarios que lo soliciten, un servicio de control parental que bloquee contenidos que atenten contra la ley, la moral o las buenas costumbres.
Los ISP deberán publicar de manera clara las características operativas de este servicio y las instrucciones para que el usuario pueda operar las aplicaciones necesarias para el correcto funcionamiento del mencionado servicio.

Artículo 10°. Los ISP procurarán preservar la privacidad de los usuarios, la protección contra virus y la seguridad de la red, utilizando para ello las herramientas tecnológicas disponibles.

Artículo 11°. Los usuarios tendrán derecho a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y que los mismos no dañen o perjudiquen la seguridad de la red o la calidad del servicio prestado a terceros.

Artículo 12°. Sin perjuicio de las materias cuya regulación corresponda a otros organismos y de las facultades que asisten al Ministerio de Transportes y Telecomunicaciones y la Subsecretaría en virtud de lo dispuesto en el artículo 36° de la ley, los usuarios y proveedores de aplicaciones podrán reclamar, de acuerdo al procedimiento establecido en el artículo 28° Bis de la Ley y su Reglamento sobre Tramitación y Resolución de Reclamos de Servicios de Telecomunicaciones, respecto de los servicios prestados por los ISP y sus eventuales incumplimientos a las obligaciones legales y/o reglamentarias asociadas a la implementación, operación y funcionamiento de la neutralidad de red que impidan, dificulten o de cualquier forma amenacen su desarrollo o el legítimo ejercicio de los derechos que de ella derivan.

Disposición Final

Artículo único. Déjese sin efecto la resolución exenta N° 669, de 2001 de la letra g) de los Vistos.

Artículos Transitorios

Artículo Primero. Los ISP tendrán un plazo de 120 días para implementar la plataforma de información y transparencia de servicio de acceso de Internet, de acuerdo a lo establecido en el artículo 5°.

Artículo Segundo. Los ISP dispondrán de un plazo de hasta 60 días, contados desde la entrada en vigencia del presente Reglamento, para remitir a la Subsecretaría los protocolos de medición que contendrán los detalles de los equipos utilizados, así como la programación y las condiciones en que se efectúen las mediciones.

Anótese, regístrese, tómese razón, comuníquese y publíquese en el Diario Oficial. SEBASTIÁN PIÑERA ECHENIQUE, Presidente de la República.- Felipe Morandé Lavín, Ministro de Transportes y Telecomunicaciones.

Lo que transcribo para su conocimiento.- Saluda atentamente a Ud., Jorge Atton Palma, Subsecretario de Telecomunicaciones.

Anexo 8: Plan Nacional Desarrollo Colombia

ARTÍCULO 56. *NEUTRALIDAD EN INTERNET.* Los prestadores del servicio de Internet:

1. Sin perjuicio de lo establecido en la Ley 1336 de 2006 <sic, 2009>, no podrán bloquear, interferir, discriminar, ni restringir el derecho de cualquier usuario de Internet, para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio lícito a través de Internet. En este sentido, deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de estos. Los prestadores del servicio de Internet podrán hacer ofertas según las necesidades de los segmentos de mercado o de sus usuarios de acuerdo con sus perfiles de uso y consumo, lo cual no se entenderá como discriminación.

2. No podrán limitar el derecho de un usuario a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales y que los mismos no dañen o perjudiquen la red o la calidad del servicio.

3. Ofrecerán a los usuarios servicios de controles parentales para contenidos que atenten contra la ley, dando al usuario información por adelantado de manera clara y precisa respecto del alcance de tales servicios.

4. Publicarán en un sitio web, toda la información relativa a las características del acceso a Internet ofrecido, su velocidad, calidad del servicio, diferenciando entre las conexiones nacionales e internacionales, así como la naturaleza y garantías del servicio.

5. Implementarán mecanismos para preservar la privacidad de los usuarios, contra virus y la seguridad de la red.

6. Bloquearán el acceso a determinados contenidos, aplicaciones o servicios, sólo a pedido expreso del usuario.

PARÁGRAFO. La Comisión de Regulación de Comunicaciones regulará los términos y Condiciones de aplicación de lo establecido en este artículo. La regulación inicial deberá ser expedida dentro de los seis meses siguientes a la entrada en vigencia de la presente ley.

Anexo 9: Marco Civil Brasileño Internet

LEY Nº 12.965, DE 23 DE ABRIL DE 2014[20]

(Marco Civil de Internet)

Establece los principios, garantías, derechos y obligaciones para el uso de Internet en Brasil.

La presidente de la República
Sépase que el Congreso Nacional decreta y yo sanciono la siguiente ley:

CAPÍTULO I
DISPOSICIONES PRELIMINARES

Artículo 1º Esta ley establece los principios, garantías, derechos y obligaciones para el uso de Internet en Brasil y determina directrices para la actuación de la Unión, de los estados, del Distrito Federal y de los municipios en este sentido.

Artículo 2º La disciplina de la utilización de Internet en Brasil se basa en el respeto a la libertad de expresión, así como:
I – el reconocimiento de la escala mundial de la red;
II – los derechos humanos, el desarrollo de la personalidad y el ejercicio de la ciudadanía en los medios digitales;
III – la pluralidad y la diversidad;
IV – la apertura y la colaboración;
V – la libre empresa, la libre competencia y protección del consumidor; y
VI – la finalidad social de la red.

Artículo 3º La disciplina de la utilización de Internet en Brasil cuenta con los siguientes principios:
I – garantía de la libertad de expresión, la comunicación y la manifestación del pensamiento, según la Constitución Federal;
II – protección de la privacidad;
III – protección de los datos personales, en forma de la ley;

20 Publicada en el *Diário Oficial da União*, Sección 1, de 24 de abril de 2014, p. 1.

IV – preservación de la garantía de neutralidad de la red;
V – preservación de la estabilidad, seguridad y funcionalidad de la red, por medio de medidas técnicas compatibles con los patrones internacionales y por el estímulo al uso de buenas prácticas;
VI – fijar responsabilidad a las partes de acuerdo con sus actividades, en los términos de la ley;
VII – preservación de la naturaleza participativa de la red;
VIII – libertad de los modelos de negocio promovidos a través de Internet, siempre que no interfieran con los demás principios establecidos en esta ley.
Párrafo único. Los principios expresados en esta ley no excluyen otros previstos en el ordenamiento jurídico nacional relacionados con el tema, o en los tratados internacionales en los que participe la República Federal de Brasil.

Artículo 4º La disciplina del uso de Internet en Brasil tiene como objetivo la promoción de los siguientes:
I – el derecho de acceso a Internet de todos;
II – el acceso a la información, al conocimiento y a la participación en la vida cultural y la conducción de asuntos públicos;
III – la innovación y fomentar una difusión amplia de nuevas tecnologías y modelos de uso y acceso; y
IV – la adherencia a los padrones tecnológicos abiertos que permitan la comunicación, accesibilidad y la interoperabilidad entre aplicaciones y bases de datos.

Artículo 5º A efectos de esta ley se entiende:
I – Internet: el sistema constituido por un conjunto de protocolos lógicos, estructurados a escala mundial para el uso público y sin restricciones, con la finalidad de posibilitar la comunicación de datos entre terminales por medio de diferentes redes;
II – terminal: la computadora o cualquier dispositivo que se conecte a Internet;
III – dirección de protocolo de Internet (dirección IP): código atribuido a un terminal de una red para permitir su identificación, definido según parámetros internacionales;
IV – administrador de sistema autónomo: persona física o jurídica que administra bloques de direcciones IP específicas y el respectivo sistema autónomo de enrutamiento, debidamente registrada en el ente nacional responsable del registro y distribución de direcciones IP geográficamente relacionadas con el país;

V – conexión a Internet: habilitación de un terminal para envío o recepción de paquetes de datos por Internet, mediante la atribución o autenticación de una dirección IP;
VI – registro de conexión: conjunto de informaciones referentes a datos y hora de inicio y término de una conexión a Internet, su duración y la dirección IP utilizada por el terminal para el envío y recepción de paquetes de datos;
VII – aplicaciones de Internet: conjunto de funcionalidades que pueden ser usadas por medio de un terminal conectado a Internet; y
VIII – registros de acceso a aplicaciones de Internet: conjunto de informaciones referentes a fecha y hora de uso de una determinada aplicación de Internet a partir de una determinada dirección IP.

Artículo 6º En la interpretación de esta ley se tendrán en cuenta, más allá de los fundamentos, principios y objetivos, la naturaleza de Internet, sus usos y costumbres particulares y su importancia para la promoción del desarrollo humano, económico, social y cultural.

CAPÍTULO II
DE LOS DERECHOS Y GARANTÍAS DE LOS USUARIOS

Artículo 7º El acceso a Internet es esencial para el ejercicio de la ciudadanía y para los usuarios están garantizados los siguientes derechos:
I – la inviolabilidad de la intimidad y de la vida privada, asegurando su protección y la indemnización por el daño material o moral resultante de su violación;
II – la inviolabilidad y secreto del flujo de las comunicaciones por Internet, salvo por orden judicial, de acuerdo con la ley;
III – la inviolabilidad y el secreto de sus comunicaciones privadas almacenadas, salvo por orden judicial;
IV – la no suspensión de la conexión a Internet, salvo por deuda contraída directamente por su utilización;
V – el mantenimiento de la calidad de la conexión a Internet contratada;
VI – informaciones claras y completas en los contratos de prestación de servicios, detallando el régimen de protección de los registros de conexión y de los registros de acceso a aplicaciones en Internet, así como de las prácticas de gestión de la red que puedan afectar a su calidad; y
VII – la imposibilidad de suministrar a terceros sus datos personales, incluyendo registros de conexión y de acceso a aplicaciones en Internet, salvo

mediante consentimiento libre, expreso e informado o en circunstancias establecidas por la ley;
VIII – información clara y completa sobre la recogida, uso, almacenamiento, tratamiento y protección de sus datos personales, que sólo podrán ser utilizados para finalidades que:

a) justifiquen su recolección;
b) no estén prohibidas por ley; y
c) queden especificadas en los contratos de prestación de servicios o en los términos de uso de las aplicaciones de Internet;

IX – consentimiento expreso sobre la recogida, uso, almacenamiento y tratamiento de datos personales, que deberá presentarse de forma destacada de las demás cláusulas contractuales;
X – la eliminación definitiva de los datos personales que se hayan proporcionado a determinada aplicación de Internet, a solicitud suya, al término de la relación entre las partes, salvo en los casos de custodia obligatoria de registros previstas en esta ley;
XI – la publicación y claridad de las eventuales políticas de uso por parte de los proveedores de conexión a Internet y de las aplicaciones de Internet;
XII – la accesibilidad, teniendo en cuenta las características físico-motoras, perceptivas, sensoriales, intelectuales y mentales del usuario, en los términos definidos por la ley; y
XIII – aplicación de las normas de protección y defensa del consumidor en las relaciones de consumo realizadas en Internet.

Artículo 8º La garantía del derecho a la privacidad y a la libertad de expresión en las comunicaciones es condición para el pleno ejercicio del derecho de acceso a Internet.
Párrafo único. Son nulas de pleno derecho las cláusulas contractuales que violen lo dispuesto anteriormente, tales como las que:
I – impliquen ofensa a la inviolabilidad y al secreto de las comunicaciones privadas a través de Internet; o
II – en la contratación, no ofrezcan al contratante la adhesión al foro brasileño para la solución de conflictos derivados de servicios prestados en Brasil.

CAPÍTULO III
DE LA PROVISIÓN DE CONEXIÓN Y DE APLICACIONES DE INTERNET

Sección I
De la Neutralidad de la Red

Artículo 9º El responsable de la transmisión, conmutación o ruteo tiene el deber de tratar de forma igual cualquier paquete de datos, sin distinción por contenido, origen y destino, servicio, terminal o aplicación.

§ 1º La discriminación o degradación del tráfico será reglamentada en los términos de las atribuciones privativas del Presidente de la República previstas en el inciso IV del artículo 84 de la Constitución Federal, para la ejecución fiel de esta ley, consultados el Comité Gestor de Internet y la Agencia Nacional de Telecomunicaciones y solamente podrá ser resultado de:

I – requisitos técnicos indispensables para la prestación adecuada de los servicios y aplicaciones; y

II – priorización de los servicios de emergencia.

§ 2º En el caso de discriminación o degradación del tráfico prevista en el § 1º, el responsable mencionado en el artículo debe:

I – abstenerse de causar daño a los usuarios, de acuerdo con lo dispuesto en el artículo 927 de la Ley nº 10.406, de 10 de enero de 2002 (Código Civil);

II – actuar con proporcionalidad, transparencia e igualdad;

III – informar previamente de modo transparente, claro y suficientemente descriptivo a sus usuarios sobre las prácticas de gestión y reducción del tráfico adoptadas, inclusive las relacionadas con la seguridad de la red; y

IV – ofrecer servicios en condiciones comerciales no discriminatorias y abstenerse de practicar conductas anticompetitivas.

§ 3º En el suministro de la conexión a Internet, de pago o gratuita, así como en la transmisión, conmutación o enrutamiento, está prohibido bloquear, monitorear, filtrar o analizar el contenido de los paquetes de datos, respetando lo dispuesto en este artículo.

Sección II
De la Protección a los Registros, Datos Personales y Comunicaciones Privadas

Artículo 10. La custodia y entrega de los registros de conexión y de acceso a aplicaciones de Internet de que trata esta ley, así como de los datos personales

y del contenido de las comunicaciones privadas, deben atender a la preservación de la intimidad, de la vida privada, de la honra y de la imagen de las partes directa o indirectamente involucradas.
§ 1º El proveedor responsable de la custodia solamente será obligado a entregar los registros mencionados en el artículo, de forma autónoma o asociados a datos personales u otras informaciones que puedan contribuir a la identificación del usuario o del terminal, mediante orden judicial, tal como queda dispuesto en la Sección IV de este Capítulo, respetando lo dispuesto en el artículo 7º.
§ 2º El contenido de las comunicaciones privadas solamente podrá ser entregado mediante orden judicial, en los casos y en la forma que establece la ley, respetando lo dispuesto en los párrafos II y III del artículo 7º.
§ 3º Lo dispuesto en este artículo no impide el acceso, por parte de las autoridades administrativas que detenten competencia legal para su solicitud, a los datos de registro que contengan información personal, filiación y dirección, de acuerdo con la ley.
§ 4º Las medidas y procedimientos de seguridad y secreto deben ser informados por el responsable de la provisión de servicios de forma clara y atenerse a patrones definidos en reglamento, respetando su derecho de confidencialidad en lo que respecta a secretos empresariales.

Artículo 11. En cualquier operación de recolección, almacenamiento, protección o tratamiento de registros, datos personales o de comunicaciones por proveedores de conexión y de aplicaciones de Internet en las que por lo menos uno de estos actos ocurra en territorio nacional, deberá ser obligatoriamente respetada la legislación brasileña, los derechos a la privacidad y a la protección de los datos personales y al secreto de las comunicaciones privadas y de los registros.
§ 1º Lo dispuesto en el artículo se aplica a los datos recolectados en territorio nacional y al contenido de las comunicaciones en las cuales por lo menos uno de los terminales está localizado en Brasil.
§ 2º Lo dispuesto en este artículo se aplica también aunque las actividades sean llevadas a cabo por personas jurídicas domiciliadas en el exterior, siempre que oferten servicios al público brasileño o que al menos una integrante del mismo grupo económico posea un establecimiento en Brasil.
§ 3º Los proveedores de conexión y de aplicaciones de internet deberán presentar, en línea con la reglamentación, información que permita la verificación del cumplimiento de la legislación brasileña en lo referente a la

recolección, protección, almacenamiento o tratamiento de datos, así como en lo que respecta a la privacidad y al secreto de las comunicaciones.
§ 4º Un decreto reglamentará el procedimiento de determinación de infracciones a lo dispuesto en este artículo.

Artículo 12. Sin perjuicio de las demás sanciones civiles, criminales o administrativas, las infracciones a las normas previstas en los artículos 10 y 11 quedan sujetas, según el caso, a las siguientes sanciones, aplicadas de forma individual o acumulativa:
I – advertencia, con indicación de plazo para la adopción de medidas correctivas;
II – multa de hasta el 10% (diez por ciento) de lo facturado por el grupo económico en Brasil en su último ejercicio, excluidos los impuestos, considerando la condición económica del infractor y el principio de proporcionalidad entre la gravedad de la falta y la gravedad de la sanción;
III – suspensión temporal de las actividades que involucren los actos previstos en el artículo 11; o
IV – prohibición de ejercicio de las actividades que involucren los actos previstos en el artículo 11.
Párrafo único. Cuando se trate de una empresa extranjera, responde solidariamente del pago de la multa de que trata este artículo su filial, sucursal, oficina o establecimiento situado en el país.

Subsección I
De la Custodia de Registros de Conexión

Artículo 13. En la provisión de conexión a Internet, cabe al administrador del sistema autónomo respectivo el deber de mantener los registros de conexión, bajo secreto, en un ambiente controlado y seguro, durante el plazo de un año, según el reglamento.
§ 1º La responsabilidad de mantener los registros de conexión no puede ser transferida a terceros.
§ 2º La autoridad policial o administrativa o el Ministerio Público podrá requerir cautelarmente que los registros de conexión sean guardados durante un plazo superior al previsto en este artículo.
§ 3º En la hipótesis del § 2º, la autoridad solicitante tendrá el plazo de sesenta días, contados a partir de la solicitud, para ingresar, con el pedido de autorización judicial, a los registros previstos en este artículo.

§ 4º El proveedor responsable de la custodia de los registros deberá mantener el secreto en relación a la solicitud prevista en el § 2º, que perderá su eficacia en caso de que el pedido de autorización judicial no sea aceptado o no haya sido ejecutado en el plazo previsto en el § 3º.
§ 5º En cualquier caso, la disponibilidad al requirente de los registros de los que trata este artículo deberá ser precedida de una autorización judicial, conforme a lo dispuesto en la Sección IV de este capítulo.
§ 6º En la aplicación de sanciones por el incumplimiento de lo dispuesto en este artículo, serán considerados la naturaleza, la gravedad de la infracción y los daños resultantes de ella, eventual beneficio para el infractor, las circunstancias agravantes, los antecedentes del infractor y la reincidencia.

Subsección II
De la Custodia de Registros de Acceso a Aplicaciones de Internet en la Provisión de Conexión

Artículo 14. En la provisión de conexión, onerosa o gratuita, está prohibido almacenar registros de acceso a aplicaciones de Internet.

Subsección III
De la Custodia de Registros de Acceso a Aplicaciones de Internet en la Provisión de Aplicaciones

Artículo 15. El proveedor de aplicaciones de Internet constituido en forma de persona jurídica, que ejerza esa actividad en forma organizada, profesionalmente y con fines económicos, deberá mantener los respectivos registros de acceso a aplicaciones de Internet, en secreto, en ambiente controlado y de seguridad, por el plazo de seis meses, en los términos del reglamento.
§ 1º Orden judicial podrá obligar, por tiempo determinado, a los proveedores de aplicaciones de Internet, que no estén sujetos a lo dispuesto en el artículo a guardar registros de acceso a aplicaciones de Internet, si se tratan de registros relativos a hechos específicos en un tiempo determinado.
§ 2º La autoridad policial o administrativa o el Ministerio Público podrán solicitar cautelarmente a cualquier proveedor de aplicaciones de Internet que los registros de acceso a aplicaciones de Internet sean guardados, incluso por plazo superior al previsto en el artículo, observando lo dispuesto en los §§ 3º y 4º del artículo 13.

§ 3º En cualquier caso, la disponibilidad al requirente, de los registros de los que trata este artículo, deberá ser precedida de autorización judicial, conforme lo dispuesto en la Sección IV de este Capítulo.
§ 4º En la aplicación de sanciones por el incumplimiento de lo dispuesto en este artículo, serán considerados la naturaleza y gravedad de la infracción, los daños resultantes de ella, el eventual beneficio para el infractor, las circunstancias agravantes, los antecedentes del infractor y la reincidencia.

Artículo 16. En la provisión de conexión, onerosa o gratuita, está prohibida la custodia:
I – de los registros de acceso a otras aplicaciones de Internet sin que el titular de los datos haya consentido previamente, respetando lo dispuesto en el artículo 7º; o
II – de datos personales que sean excesivos en relación a la finalidad para la cual fue dado el consentimiento por su titular.

Artículo 17. Excepto en los casos previstos en esta ley, la opción de no guardar los registros de acceso a aplicaciones de Internet no implica responsabilidad sobre los datos que surgieran del uso de esos servicios por terceros.

Sección III
De la Responsabilidad por Daños que Surgieran del Contenido Generado por Terceros

Artículo 18. El proveedor de conexión a Internet no será responsabilizado civilmente por daños surgidos por contenido generado por terceros.

Artículo 19. Con el objetivo de asegurar la libertad de expresión e impedir la censura, el proveedor de aplicaciones de Internet solamente podrá ser responsabilizado por daños que surjan del contenido generado por terceros si, después de una orden judicial específica, no toma las previsiones para, en el ámbito de los límites técnicos de su servicio y dentro del plazo asignado, tornar indisponible el contenido especificado como infractor, exceptuando las disposiciones legales que se opongan.
§ 1º La orden judicial de que trata este artículo deberá contener, bajo pena de nulidad, identificación clara y específica del contenido especificado como infractor, que permita la localización inequívoca del material.
§ 2º La aplicación de lo dispuesto en este artículo para infracciones a derechos de autor y a derechos conexos depende de la previsión legal específica, que

deberá respetar la libertad de expresión y las demás garantías previstas en el artículo 5 de la Constitución Federal.
§ 3º Las causas judiciales que traten sobre el resarcimiento por daños surgidos de contenidos disponibles en Internet relacionados a la honra, la reputación y a derechos de personalidad, así como sobre la indisponibilidad de esos contenidos por proveedores de aplicaciones de Internet, podrán ser presentadas mediante los juzgados especiales.
§ 4º El juez, incluso en el procedimiento previsto en el § 3º, podrá anticipar, total o parcialmente, los efectos de la tutela pretendida en el pedido inicial, existiendo la prueba inequívoca del hecho y considerando el interés de la colectividad en la disponibilidad del contenido en Internet, estando presentes requisitos de verosimilitud de la alegación del autor y de temor fundado de daño irreparable o de difícil reparación.

Artículo 20. Siempre que tenga informaciones de contacto del usuario directamente responsable por el contenido al que se refiere el artículo 19, corresponderá al proveedor de aplicaciones de Internet comunicarle los motivos e informaciones relativos a la indisponibilidad de contenido, con informaciones que permitan la contradicción y amplia defensa en juicio, salvo expresa previsión legal o salvo expresa determinación judicial fundamentada en contra.
Párrafo único. Cuando sea solicitado por el usuario que hizo disponible el contenido que ha sido hecho indisponible, el proveedor de aplicaciones de Internet que ejerza esa actividad de forma organizada, profesionalmente y con fines económicos, sustituirá el contenido indisponible, por la motivación o por la orden judicial que fundamenta la indisponibilidad.

Artículo 21. El proveedor de aplicaciones de Internet que haga disponible contenido generado por terceros será responsabilizado subsidiariamente por la violación de la intimidad resultado de la divulgación, sin autorización de sus participantes, de imágenes, de videos y de otros materiales que contengan escenas de desnudos o de actos sexuales de carácter privado cuando, posterior al recibimiento de la notificación por el participante o su representante legal, dejar de promover, de forma diligente, en el ámbito y en los límites técnicos de su servicio, la indisponibilidad de ese contenido.
Párrafo único. La notificación prevista en el artículo deberá contener, bajo pena de nulidad, elementos que permitan la identificación específica del material apuntado como violador de la intimidad del participante y la verificación de la legitimidad para presentación del pedido.

Sección IV
De la Solicitud Judicial de Registros

Artículo 22. La parte interesada podrá, con el propósito de formar conjunto probatorio en proceso judicial civil o penal, en carácter incidental o autónomo, requerir al juez que ordene al responsable por la guarda u otorgamiento de registros de conexión o de registros de acceso a aplicaciones de Internet.
Párrafo único. Sin perjuicio de los demás requisitos legales, el requerimiento deberá contener, bajo pena de inadmisibilidad:
I – fundados indicios del acontecimiento del ilícito;
II – justificación motivada de la utilidad de los registros solicitados para fines de investigación o instrucción probatoria; y
III – período al cual se refieren los registros.

Artículo 23. Cabe al juez tomar las providencias necesarias a la garantía del sigilo de las informaciones recibidas y a la preservación de la intimidad, de la vida privada, de la honra y de la imagen del usuario, pudiendo determinar secreto de justicia, inclusive en cuanto a los pedidos de custodia de registro.

CAPÍTULO IV
DEL EJERCÍCIO DEL PODER PÚBLICO

Artículo 24. Constituyen directrices para la actuación de la Unión, de los estados, del Distrito Federal y de los municipios en el desarrollo de Internet en Brasil:
I – establecimiento de mecanismos de administración participativa, transparente, colaborativa y democrática, con participación del gobierno, del sector empresarial, de la sociedad civil y de la comunidad académica;
II – promoción de la racionalización de la gestión, la expansión y el uso de Internet, con la participación del Comité Gestor de Internet en Brasil;
III – promoción de la racionalización y la interoperabilidad tecnológica de los servicios de gobierno electrónico, entre los diferentes poderes y niveles de la federación, para permitir el intercambio de información y la rapidez de los procedimientos;
IV – promoción de la interoperabilidad entre los diversos sistemas y terminales, incluso entre los diferentes niveles federativos y diferentes sectores de la sociedad;
V – adopción preferencial de tecnologías, estándares y formatos abiertos y libres;

VI – publicidad y difusión de los datos y la información pública, de forma abierta y estructurada;
VII – optimización de la infraestructura de las redes y el fomento de la creación de centros de almacenamiento, gestión y difusión de datos en el país, promoviendo la excelencia técnica, la innovación y la difusión de las aplicaciones de Internet, sin perjuicio de la apertura, de la neutralidad y de la naturaleza participativa;
VIII – desarrollo de acciones y programas de capacitación para el uso de Internet;
IX – promoción de la cultura y de la ciudadanía; y
X – prestación de servicios públicos de atención al ciudadano de forma integral, eficiente, simple y por múltiples vías de acceso, inclusive a distancia.

Artículo 25. Las aplicaciones de Internet de los entes del Poder Público deben buscar:
I – compatibilidad de los servicios de gobierno electrónico con diferentes terminales, sistemas operativos y aplicaciones de acceso;
II – accesibilidad a todos los interesados, independientemente de sus capacidades físico-motoras, perceptivas, sensoriales, intelectuales, mentales, culturales y sociales, salvaguardando los aspectos confidenciales y restricciones administrativas y legales;
III – compatibilidad tanto con la lectura humana como con el tratamiento automatizado de la información;
IV – facilidad de uso de los servicios de gobierno electrónico; y
V – fortalecimiento de la participación social en las políticas públicas.

Artículo 26. El cumplimiento de la obligación constitucional del Estado en la provisión de la educación, en todos los niveles de enseñanza, incluida la capacitación, integrada con las otras prácticas educativas, para un uso seguro, consciente y responsable de Internet como herramienta para el ejercicio de la ciudadanía, la promoción de la cultura y el desarrollo tecnológico.

Artículo 27. Las iniciativas públicas que promueven la cultura digital y el uso de Internet como herramienta social deben:
I – promover la inclusión digital;
II – tratar de reducir las desigualdades, sobre todo entre las diferentes regiones del país, en el acceso a tecnologías de la información y comunicación y su uso; y
III – promover la producción y difusión de contenido nacional.

Artículo 28. El Estado debe, periódicamente, formular y fomentar estudios, así como fijar metas, estrategias, planes y programas relacionados al uso y desarrollo de Internet en el país.

CAPÍTULO V
DISPOSICIONES FINALES

Artículo 29. El usuario tendrá libre elección en el uso de programas de computadora en su terminal para facilitar el control parental de contenidos, según considere impropio para sus hijos menores, siempre y cuando cumplan con los principios de esta ley y de la Ley nº 8.069 de 13 de julio de 1990 (Estatuto del Niño e y del Adolescente).
Párrafo único. Corresponde al poder público, en conjunto con los proveedores de conexión y aplicaciones de Internet y la sociedad civil, promover la educación y proporcionar información sobre el uso de los programas de computadora definidos anteriormente, así como para la definición de buenas prácticas para la inclusión digital de niños y adolescentes.

Artículo 30. La defensa de los intereses y derechos establecidos en esta ley podrá ser ejercida individual o colectivamente, conforme a lo dispuesto por la ley.

Artículo 31. Hasta la entrada en vigencia de la ley específica prevista en el § 2º del artículo 19, la responsabilidad del proveedor de aplicaciones de Internet por daños y perjuicios resultantes por uso de contenido generado por terceros, en caso de infracción de derechos de autor o derechos conexos, se seguirán rigiendo por la legislación de derechos de autor en vigencia previo a la fecha de entrada en vigencia de la presente ley.

Artículo 32. Esta ley entrará en vigencia sesenta días después de la fecha de su publicación oficial.

Brasília, 23 de abril de 2014; 193º de la Independencia y 126º de la República.

DILMA ROUSSEFF
José Eduardo Cardozo
Miriam Belchior
Paulo Bernardo Silva
Clélio Campolina Diniz

Anexo 10: Reglamento NR Perú

REGLAMENTO DE NEUTRALIDAD DE RED

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1.- Objetivos

En el marco de lo dispuesto en la Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica, Ley N° 29904 y su Reglamento, aprobado mediante Decreto Supremo N° 014-2013-MTC, son objetivos del presente Reglamento:

1.1. Establecer las disposiciones necesarias para asegurar el cumplimiento de lo dispuesto en las normas antes citadas, referidas a la Neutralidad de Red.

1.2. Determinar los principios, las medidas permitidas, las medidas prohibidas y el régimen de infracciones y sanciones, entre otras, relativas a la Neutralidad de Red.

Artículo 2.- Alcance

2.1. El presente Reglamento es aplicable a los Operadores de Telecomunicaciones y Proveedores del Servicio de Acceso a Internet, que participan directa o indirectamente en la prestación del Servicio de Acceso a Internet, a quienes en adelante se les denomina, indistintamente, Operadores de Telecomunicaciones.

2.2. El alcance del presente Reglamento se extiende a cualquier prestación o producto comercial que ofrezca la conectividad para utilizar los recursos, totales o parciales, disponibles en el Internet, indistintamente de su denominación o estructura comercial. Entiéndase como recursos disponibles en Internet, a las diversas aplicaciones, servicios, protocolos, contenidos y/o tráfico disponibles en los nodos conectados al Internet.

Artículo 3.- Referencia reglamentaria

Cuando en el presente Reglamento se haga referencia a un título, capítulo, subcapítulo, artículo, numeral o literal o anexo, sin indicar la norma a la cual pertenece, se entiende referido al presente Reglamento.

Artículo 4.- Definiciones

Para efectos del presente Reglamento, las definiciones vinculadas a la Neutralidad de Red son las definidas en el Anexo I.

En ausencia de definición expresa, aplican las que se encuentran contenidas en la Normativa General Aplicable. Asimismo, se pueden utilizar supletoriamente y en orden prelatorio, las definiciones adoptadas por la UIT, IETF y ETSI.

Artículo 5.- Principios rectores de la Neutralidad de Red

Los principios, que permiten garantizar el pleno respeto por la Neutralidad de Red son los siguientes:

5.1. **Principio de libre uso**: Todo usuario tiene derecho a la libertad de uso y disfrute, a través del Servicio de Acceso a Internet, utilizando cualquier equipo o dispositivo terminal y dentro de lo lícitamente permitido, de cualquier tráfico, protocolo, servicio o aplicación.

5.2. **Principio de precaución:** Todo Operador de Telecomunicaciones, al implementar una medida relativa a la Neutralidad de Red, debe actuar asegurándose de adoptar las medidas necesarias para evitar que la intervención a su red genere daños o afectaciones al Servicio de Acceso a Internet.

5.3. **Principio de equidad**: Todo Operador de Telecomunicaciones mantiene un tratamiento equitativo para cualquier protocolo, tráfico, aplicación o servicio provisto por el Servicio de Acceso a Internet, brindado a través de su red, con el objetivo de garantizar una adecuada provisión del servicio, salvo en los casos determinados por norma expresa.

5.4. **Principio de transparencia**: Todo Operador de Telecomunicaciones debe hacer pública la información sobre las prácticas relacionadas a la Neutralidad de Red que implementa en su red.

Son complementarios a los principios antes indicados, aquellos establecidos en la Normativa General Aplicable.

TÍTULO II
MEDIDAS RELATIVAS A LA NEUTRALIDAD DE RED

Artículo 6.- Información provista por parte del Operador de Telecomunicaciones sobre las medidas relativas a la Neutralidad de Red

6.1. El Operador de Telecomunicaciones está obligado 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, con motivo de la provisión de sus servicios, calificadas expresamente como medidas autorizadas en el artículo 13.

Para dicho propósito, incluirá en la página principal de su sitio web, un link denominado "Neutralidad de Red" que dirija a una página web con información específica relacionada a las medidas relativas a la Neutralidad de Red implementadas. Esta información será publicada de acuerdo a los términos señalados del Anexo II.

6.2. La información publicada en el sitio web del Operador de Telecomunicaciones deberá ser completa y veraz, y encontrarse actualizada. Dichas actualizaciones serán comunicadas al OSIPTEL al menos un día hábil antes de ser publicadas en su sitio web. En la comunicación se debe especificar la fecha de actualización de las medidas.

Artículo 7.- Publicación de las medidas relativas a la Neutralidad de Red por parte del OSIPTEL

7.1. El OSIPTEL realiza con periodicidad trimestral, la publicación en su portal institucional de la información relativa a la Neutralidad de Red a la que se hace referencia en el numeral 6.1 del artículo 6.

7.2. Las resoluciones que emita el OSIPTEL, cuando hayan quedado firmes o se haya causado estado en el procedimiento administrativo, serán publicadas en su portal institucional.

Artículo 8.- Independencia respecto de las normas sobre derechos de los usuarios y de libre y leal competencia

8.1. Las medidas relativas a la Neutralidad de Red implementadas por el Operador de Telecomunicaciones deberán sujetarse a las normas sobre los derechos de los usuarios de los servicios públicos de telecomunicaciones, del consumidor y/o las normas de Libre y Leal Competencia.

8.2. Las infracciones por el incumplimiento del presente Reglamento son independientes respecto del resultado de la evaluación en torno a las normas sobre los derechos de los usuarios de los servicios públicos de telecomunicaciones, protección de los derechos de los consumidores y las normas de Libre y Leal Competencia establecidas en sus respectivos marcos normativos.

Artículo 9.- Precedente de observancia obligatoria

Las resoluciones de última instancia del OSIPTEL que al resolver casos particulares interpreten de modo expreso y con carácter general el sentido del presente Reglamento constituyen precedente de observancia obligatoria, debiendo declararse de manera expresa y ordenarse su publicación en el diario oficial El Peruano.

Artículo 10.-Cese temporal o definitivo de medidas relativas a la Neutralidad

El OSIPTEL puede ordenar el cese temporal o definitivo de cualquier medida implementada por el Operador de Telecomunicaciones, cuando se advierta que contraviene los principios y/o disposiciones del presente Reglamento, la Ley N° 29904 y/o su Reglamento.

La orden de cese será impuesta por la Gerencia General.

Artículo 11.-Impugnación de decisiones en materia de Neutralidad de Red.

La interposición de cualquier recurso administrativo contra la orden de cese dispuesto por el OSIPTEL, se tramita conforme a la Ley N° 27444, Ley del Procedimiento Administrativo General y sus modificatorias.

TÍTULO III
MEDIDAS PERMITIDAS RELATIVAS A LA NEUTRALIDAD DE RED

Artículo 12.-Tipos de medidas permitidas relativas a la neutralidad de red

El Operador de Telecomunicaciones podrá implementar una medida relativa a la Neutralidad de Red, cuando:

1. El presente Reglamento la califica expresamente como una medida autorizada relativa a la Neutralidad de Red.

2. Se trata de una medida ante situación de emergencia relativa a la Neutralidad de Red.

3. Se trata de una medida implementada por mandato judicial.

CAPÍTULO I
MEDIDAS AUTORIZADAS RELATIVAS A LA NEUTRALIDAD DE RED

Artículo 13.-Tipos de medidas autorizadas

El Operador de Telecomunicaciones puede implementar las siguientes medidas sin autorización previa del OSIPTEL:

1. Gestión de Direcciones IP.

2. Duración de la Sesión Dinámica en la Red.

3. Almacenamiento Temporal de Contenidos (CDN).

4. Filtro y/o Bloqueo de Servicios y/o Aplicaciones a solicitud del abonado.

5. Filtro y/o Bloqueo de Servicios y/o Aplicaciones en cumplimiento de obligaciones contractuales con el Estado o con motivo de una norma específica.

6. Otras medidas, siempre que no contravengan los principios rectores de la Neutralidad de Red.

SUB-CAPÍTULO I
DESCRIPCIÓN DE LAS MEDIDAS AUTORIZADAS

Artículo 14.-Gestión de Direcciones IP

Constituyen medidas de Gestión de Direcciones IP aquellas que permiten al Operador de Telecomunicaciones gestionar y/o administrar la asignación de las direcciones IP que identifican al usuario mientras accede a Internet, gestionar direcciones IP privadas o públicas, ya sean fijas o dinámicas; así como gestionar mecanismos de adopción de direcciones IPv6, entre otros. Todo ello, en concordancia con lo que se establezca específicamente en el contrato de abonado del Servicio de Acceso a Internet.

Artículo 15.-Duración de la Sesión Dinámica en la Red

Constituyen medidas de Duración de la Sesión Dinámica en la Red aquellas que permiten al Operador de Telecomunicaciones establecer un tiempo determinado para que la sesión del usuario en la red sea reiniciada, con el objetivo de gestionar los recursos disponibles en su red.

Artículo 16.-Almacenamiento Temporal de Contenidos (CDN)

Constituyen medidas de Almacenamiento Temporal de Contenidos (CDN) aquellas que permiten al Operador de Telecomunicaciones contratar los servicios o implementar una red informática que localiza determinados contenidos en un servidor espejo de almacenamiento, que permita establecer una menor distancia de red entre el usuario y el contenido.

Artículo 17.-Filtro y/o Bloqueo de Servicios y/o Aplicaciones a solicitud del abonado

Constituyen medidas de Filtro y/o Bloqueo de Servicios y/o Aplicaciones a solicitud del abonado aquellas que permiten al Operador de Telecomunicaciones bloquear puertas de entrada lógicas en el equipo terminal del usuario (puertos), desde y hacia Internet; bloquear nombres de dominio y/o direcciones IP; o, bloquear aplicaciones o servicios, siempre que haya sido solicitado expresamente por el abonado.

Artículo 18.-Filtro y/o Bloqueo de Servicios y/o Aplicaciones en cumplimiento de obligaciones contractuales con el Estado o con motivo de una norma específica

El Operador de Telecomunicaciones, en cumplimiento de las obligaciones contractuales que haya asumido con el Estado, o con motivo de una norma específica, siempre que estas sean expresas, está facultado para aplicar las medidas dirigidas a bloquear puertos desde y hacia Internet; bloquear nombres de dominio y/o direcciones IP; o bloquear aplicaciones y/o servicios.

SUB-CAPÍTULO II
CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE LAS MEDIDAS AUTORIZADAS

Artículo 19.-Consideraciones para la implementación de la Gestión de Direcciones IP

La implementación de medidas de Gestión de Direcciones IP no debe afectar o restringir la normal utilización del Servicio de Acceso a Internet por parte de los usuarios, incluyendo el uso de cualquier protocolo, tráfico, aplicación o servicio disponible en Internet, salvo que por causas debidamente justificadas, sea inevitable algún tipo de afectación particular, lo cual será registrado en los términos dispuestos en el Anexo II.

Artículo 20.-Consideraciones para la Duración de la Sesión Dinámica en la Red

La implementación de medidas de Duración de la Sesión Dinámica en la Red debe cumplir los siguientes requerimientos:

1. Se mantendrá la sesión del usuario siempre que se detecte transferencia de tráfico de datos.
2. El reinicio de la sesión del usuario se realiza cuando no exista transferencia de ningún tipo de tráfico de datos, dentro de un tiempo de inactividad en horas o minutos, el cual debe ser informado por la empresa según los términos del Anexo II.

3. El reinicio de la sesión se da de forma instantánea en un tiempo que sea imperceptible para el usuario.

Artículo 21.-Consideración para la implementación del Almacenamiento Temporal de Contenidos (CDN)

En caso el Operador de Telecomunicaciones implemente un CDN o contrate los servicios CDN de un tercero, esta implementación deberá cumplir con los principios establecidos en el presente Reglamento; asumiendo el Operador de Telecomunicaciones la responsabilidad administrativa por las vulneraciones a la Neutralidad de Red en la que incurra su proveedor de CDN.

CAPÍTULO II
MEDIDAS RELATIVAS A LA NEUTRALIDAD DE RED ADOPTADAS EN SITUACIÓN DE EMERGENCIA

Artículo 22.-Definición de situación de emergencia relativa a la Neutralidad de Red.

22.1. Evento que genera efectos adversos o potenciales efectos adversos a la Neutralidad de Red, afectando o pudiendo afectar la disponibilidad particular o total y/o el correcto funcionamiento esperado de servicios, aplicaciones, acceso a contenidos, protocolos o tráfico específicos disponibles a través del Servicio de Acceso al Internet.

22.2. Los eventos a que se hace referencia en el numeral anterior, pueden ser aquellos que: (i) atenten contra la seguridad e integridad de la red, y el medio difusor de la amenaza es el Internet, y/o (ii) atenten contra la disponibilidad del Servicio de Acceso a Internet, y/o (iii) atenten contra las funcionalidades y/o servicios disponibles a través del Servicio de Acceso a Internet.

22.3. La afectación indicada se puede originar por acciones de terceros, de fuerza mayor, o por acciones que adopta el Operador de Telecomunicaciones para evitar, neutralizar, eliminar y/o mitigar una situación de emergencia relativa a la neutralidad de red.

Artículo 23.-Medidas adoptadas ante una situación de emergencia relativa a la Neutralidad de Red

Las medidas adoptadas ante una situación de emergencia relativa a la Neutralidad de Red, son aquellas que realiza el Operador de Telecomunicaciones con el fin de evitar, neutralizar, eliminar y/o mitigar los efectos negativos producidos por una situación de emergencia.

Toda medida adoptada en situación de emergencia es de carácter temporal.

Artículo 24.-Aplicación de medidas adoptadas ante una situación de emergencia

24.1. El Operador de Telecomunicaciones puede implementar medidas ante situaciones de emergencia relativas a la Neutralidad de Red cuando las circunstancias así lo requieran. Dichas medidas estarán circunscritas a los Protocolos de Acción ante Situaciones de Emergencia.

24.2. Los Protocolos de Acción ante Situaciones de Emergencia son el conjunto de acciones predeterminadas por el Operador de Telecomunicaciones, que se ejecutan de forma preventiva y/o reactiva en sus redes y servicios, con la finalidad de evitar, mitigar o contrarrestar alguna situación de emergencia relativa a la Neutralidad de Red.

24.3. La implementación de los mencionados protocolos y sus actualizaciones son comunicados al OSIPTEL al menos un día hábil antes de entrar en vigor. En la comunicación se debe especificar la fecha de inicio de la vigencia de los protocolos.

24.4. Los tipos de medidas adoptadas ante situaciones de emergencia relativas a la Neutralidad de Red son:

(i) Protección de la red ante acciones maliciosas.

(ii) Gestión de tráfico ante situación de interrupción.

24.5. La medida adoptada ante situación de emergencia se mantendrá por el tiempo que dure el evento de emergencia. Finalizado el referido evento, el Operador de Telecomunicaciones procederá a levantar la medida, restituyendo la configuración del servicio al estado previo al evento de emergencia.

Artículo 25.-Protección de la red ante acciones maliciosas

Para efectos del presente Reglamento, son consideradas como acciones maliciosas:

1. Ataques de Denegación de Servicios (DoS).

2. Ataques Distribuidos de Denegación de Servicios (DDoS).

Artículo 26.-Gestión de tráfico ante situación de interrupción

26.1. En casos de interrupción de servicios portadores y uso de rutas alternas de respaldo que reducen drásticamente recursos como el ancho de banda disponible, el Operador de Telecomunicaciones podrá, excepcionalmente, implementar medidas

de gestión de tráfico del Servicio de Acceso a Internet, con el objetivo de no generar mayor afectación en los servicios provistos por su red.

26.2. En tal sentido, el Operador de Telecomunicaciones podrá priorizar entre clases de servicios, clases de aplicaciones, clases de protocolos y/o clases de tráficos, o en función al origen y destino de los mismos, con el fin de garantizar la continuidad de servicios o aplicaciones de mayor relevancia en situaciones de emergencia, de acuerdo al Protocolo de Acción ante Situaciones de Emergencia. En ningún caso, el Operador de Telecomunicaciones podrá priorizar, en función a un determinado servicio, aplicación, protocolo, tráfico y/o al origen y destino de los mismos dentro de las clases mencionadas, salvo disposición prevista en norma expresa en caso de desastres y/o situaciones de emergencia.

26.3. Según la normativa del sistema de comunicaciones en situaciones de emergencia, que corresponda, el Operador de Telecomunicaciones estará obligado a priorizar las comunicaciones de los grupos de respuesta y mitigación de los efectos causados por la emergencia.

26.4. El Operador de Telecomunicaciones es responsable por la gestión de tráfico realizada en su red, y los efectos que ello pueda generar a sus usuarios en la eventualidad de aplicar de manera indebida esta medida, o en caso de extenderla más allá de la duración del evento que origina la necesidad de esta gestión de tráfico.

Artículo 27.- Obligación de mantener registro de la información de implementación de medidas ante situaciones de emergencia

27.1. Las medidas de emergencia relativas a la Neutralidad de Red implementadas por el Operador de Telecomunicaciones, deberán ser registradas en los términos establecidos en el Anexo III. El OSIPTEL podrá solicitar dicha información cuando lo considere oportuno.

27.2. El Operador de Telecomunicaciones solo registrará las medidas a las que se hace alusión en el numeral 27.1, cuando estas medidas generan una afectación mayor a 10 minutos en la disponibilidad o afectación del funcionamiento esperado, tanto del Servicio de Acceso a Internet, como de alguna de las aplicaciones, acceso a contenidos, protocolos, tráficos específicos o servicios que lo componen.

27.3. Estas condiciones aplican tanto para las medidas con motivo de acciones maliciosas como con motivo de la gestión de tráfico ante situaciones de interrupción.

9

Artículo 28.-Control de la medida de emergencia implementada

28.1. El OSIPTEL tiene la facultad de evaluar si la medida de emergencia relativa a la Neutralidad de Red implementada por el Operador de Telecomunicaciones cumple con las condiciones establecidas en el presente Reglamento, pudiendo disponer el cese de la medida, si corresponde.

28.2. Para dar cumplimiento a lo dispuesto en el numeral anterior, el registro con la información de los eventos podrá ser requerido por el OSIPTEL cuando se considere conveniente y deberán ser remitidos al correo electrónico emergencianr@osiptel.gob.pe, en un plazo máximo de cuatro (4) horas contados desde el momento del requerimiento.

Artículo 29.- Solicitud de un Operador de Telecomunicaciones a otro Operador de Telecomunicaciones para la implementación de medidas de emergencia relativas a la Neutralidad de Red

29.1. El Operador de Telecomunicaciones, cuya red y/o servicios se vieran afectados por una situación de emergencia relativa a la Neutralidad de Red, pero que carezca de control sobre los elementos de red que le permitan implementar una acción, puede solicitar al Operador de Telecomunicaciones que le presta servicios de Acceso a Internet y tenga control sobre dichos elementos, que adopte oportunamente la medida respectiva.

29.2. El Operador de Telecomunicaciones que requiera solicitar al Operador de Telecomunicaciones que le presta servicios de Acceso a Internet, adoptar acciones frente a una situación de emergencia, deberá ajustar este procedimiento a lo establecido en el Anexo IV.

29.3. El Operador de Telecomunicaciones que brinda el Servicio de Acceso a Internet a otro operador asume la responsabilidad correspondiente ante el OSIPTEL por la implementación de la medida.

29.4. Las acciones que se requieran al Operador de Telecomunicaciones que brinda servicios a otro operador, deben circunscribirse estrictamente a los protocolos que el primero aplique ante dichas situaciones de emergencia.

Artículo 30.-Responsabilidad del Operador de Telecomunicaciones frente a sus usuarios por la implementación de medidas de emergencia

30.1. El Operador de Telecomunicaciones es responsable ante sus usuarios por las afectaciones al Servicio de Acceso a Internet u otros servicios soportados sobre Internet, generadas al implementar medidas de emergencia.

30.2. Las referidas afectaciones reciben el tratamiento de devoluciones y compensaciones previsto en el artículo 45 de las Condiciones de Uso.

CAPÍTULO III
MEDIDAS IMPLEMENTADAS POR MANDATO JUDICIAL

Artículo 31.-Medidas por mandato judicial

31.1. Las medidas relativas a la Neutralidad de Red implementadas por el Operador de Telecomunicaciones en cumplimiento de un mandato judicial, deben ser registradas por el Operador de Telecomunicaciones. El OSIPTEL podrá solicitar dicha información cuando lo considere oportuno.

31.2. La información registrada debe describir las medidas implementadas y su tiempo de ejecución en la red del Operador de Telecomunicaciones, durante el periodo transcurrido en cada comunicación. El registro debe resguardar la información confidencial de los usuarios y encontrarse completamente anónimo en lo que se refiera a la identidad del afectado por la medida.

TÍTULO IV
MEDIDAS PROHIBIDAS RELATIVAS A LA NEUTRALIDAD DE RED

Artículo 32.-Medidas prohibidas

El Operador de Telecomunicaciones está prohibido de implementar las siguientes medidas:

1. Gestión arbitraria de tráfico.
2. Filtro y/o Bloqueo arbitrario de servicios y/o aplicaciones legales.
3. Diferenciación arbitraria en la oferta comercial de productos de Acceso a Internet.

Artículo 33.- Gestión arbitraria del Tráfico

33.1. El Operador de Telecomunicaciones no podrá realizar Gestión de Tráfico relativa a la neutralidad de red, a un determinado servicio, aplicación, protocolo y/o tráfico; o en función al origen y destino de los mismos, salvo lo indicado en los siguientes incisos.

33.2. La Gestión de Tráfico relativa a la Neutralidad de Red, no será considerada una medida arbitraria cuando sea implementada por el operador con el fin de:

(i) Preservar la seguridad e integridad de la red.

(ii) Priorizar los sistemas de comunicaciones en emergencia contemplados en la normativa correspondiente.

(iii) Prevenir, reducir o mitigar los efectos imprevisibles de congestión severa de la red.

33.3. El Operador de Telecomunicaciones podrá, excepcionalmente, gestionar el tráfico entre clases de servicios, clases de aplicaciones y/o clases de protocolos o en función al origen o destino de los mismos, con el fin de garantizar la continuidad de servicios o aplicaciones, ante eventos imprevisibles de congestión severa de la red. Dicha gestión de tráfico será de carácter temporal y excepcional mientras persistan las situaciones que originan la necesidad de dicha gestión de tráfico. Para la priorización de las comunicaciones en emergencia se aplica lo indicado en los artículos 26.2 y 26.3. En estos casos, el operador estará obligado a registrar y comunicar sus acciones según lo indicado en los artículos 27 y 28 de la presente norma.

33.4. La gestión de tráfico, dentro del ancho de banda provisto a un usuario en particular y realizada por encargo expreso del usuario, pero sin afectar el ancho de banda de la red provisto a otros usuarios, no será considerada gestión arbitraria de tráfico.

Artículo 34.-Filtro y/o Bloqueo arbitrario de servicios y/o aplicaciones legales

El Operador de Telecomunicaciones no puede, de propia iniciativa y sin consentimiento expreso del abonado, bloquear puertas de entrada lógicas (puertos) en su red o en el equipo terminal del usuario, desde y hacia Internet, bloquear nombres de dominio o direcciones IP, o bloquear aplicaciones o servicios.

Artículo 35.- Diferenciación arbitraria en la oferta comercial de productos de Acceso a Internet

35.1. El Operador de Telecomunicaciones podrá diseñar planes o productos comerciales de Acceso a Internet que contengan Componentes con Tratamiento Diferenciado, ya sea a nivel de protocolos, tráfico, servicios, o aplicaciones.

35.2. Para efectos de este Reglamento, los componentes en los cuales el Operador de Telecomunicaciones no realiza ningún tratamiento a nivel de protocolos, tráfico,

servicios o aplicaciones, serán denominados como Componentes sin Tratamiento Diferenciado.

35.3. La medida asociada a la oferta comercial que contiene Componentes con Tratamiento Diferenciado, se considera arbitraria cuando presenta cualquiera de las siguientes características:

(i) Restricción al acceso: mediante la cual se establece alguna acción que restringe el acceso a aplicaciones o servicios equivalentes, disponibles en Internet, en perjuicio de la libre elección de los usuarios.

(ii) Priorización: priorización de cualquier tipo de tráfico, protocolo, servicio o aplicación en los Componentes con Tratamiento Diferenciado; en relación a los equivalentes disponibles en los Componentes sin Tratamiento Diferenciado.

(iii) Limitación de calidad y/o funcionalidad: cuando se incluye en los Componentes con Tratamiento Diferenciado servicios o aplicaciones con limitación en calidad, atributos y/o funcionalidad; y se pretende extender esta limitación a otros servicios o aplicaciones disponibles en los Componentes sin Tratamiento Diferenciado, que compiten con los componentes diferenciados de la oferta comercial.

(iv) Cobro adicional: cuando se incluye en los Componentes con Tratamiento Diferenciado servicios o aplicaciones con limitación en calidad, atributos y/o funcionalidad; y se exige un cobro adicional para restituir en el Componente sin Tratamiento Diferenciado, los atributos y/o funcionalidades limitados en los Componentes con Tratamiento Diferenciado.

35.4. Cuando los componentes de cualquier oferta comercial cuenten con tratamiento diferenciado no arbitrario, el usuario tiene la potestad de elegir, en cualquier momento y sin tener que realizar pagos adicionales, el acogerse o no a dicho beneficio.

TÍTULO V
RÉGIMEN DE INFRACCIONES Y SANCIONES

Artículo 36.-Régimen de Infracciones y Sanciones

En el Anexo V se establece el régimen de infracciones y sanciones aplicable al presente Reglamento, sin perjuicio de las demás consecuencias por el incumplimiento de otras obligaciones dispuestas en la normativa vigente.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- El presente Reglamento entra en vigencia el 1 de enero de 2017, salvo el artículo 6 que entra en vigencia el 1 de febrero de 2017.

Segunda.- A la entrada en vigencia del presente Reglamento, el Operador de Telecomunicaciones debe dejar de comercializar nuevos planes y/o promociones de productos relativos al Servicio de Acceso a Internet con características o elementos que contravengan las disposiciones del presente Reglamento.

Tercera.- Los contratos suscritos en cualquier modalidad con el abonado, así como los planes y/o promociones de productos relativos al Servicio de Acceso a Internet que se han suscrito y que se encuentran en vigor, se adecuarán a las disposiciones establecidas del presente Reglamento. Para tal efecto, el Operador de Telecomunicaciones tendrá un periodo de adecuación que vencerá indefectiblemente el 31 de enero de 2017. En dicho periodo, el operador deberá informar a sus usuarios las adecuaciones particulares que realice, a través de avisos específicos personalizados ya sea por escrito, mediante correo electrónico o, mensajes de texto SMS.

Cuarta.- La aplicación del presente Reglamento no enerva ni suple en caso alguno, lo dispuesto por los numerales 3 a 6 del artículo 62 del Reglamento de la Ley Nº 29904, en cuanto a la facultad del OSIPTEL de sancionar las conductas tipificadas en dicho Reglamento, ni de dictar las medidas correctivas que correspondan.

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

Primera.- El Operador de Telecomunicaciones remitirá al OSIPTEL dentro de los veinte (20) días calendario, contados desde la publicación del presente Reglamento en el Diario Oficial El Peruano, lo siguiente:

- Información de las medidas relativas a la neutralidad de red que serán aplicadas desde la entrada en vigencia del presente Reglamento y que, conforme lo dispuesto en el Anexo II, deberá ser publicada en su Sitio Web; y,

- Los Protocolos de Acción ante Situaciones de Emergencia que implementará a efectos de cumplir con lo dispuesto por el artículo 24 del presente Reglamento.

El Operador que incumpla con esta disposición total o parcialmente, incurrirá en infracción grave.

14

Segunda.- Los numerales 1 y 5 del Régimen de Infracciones y Sanciones detallado en el Anexo V, serán aplicables a partir del 1 de febrero de 2017. Asimismo, el numeral 9 del citado Régimen, será aplicable a partir del 1 de julio de 2017, sin perjuicio que el OSIPTEL realice las acciones de monitoreo que considere pertinentes; o, imponga las medidas de cese y/o medidas correctivas que correspondan, conforme a lo dispuesto en el presente Reglamento.

ANEXO I
DEFINICIONES

1. **Administración de red:** Conjunto de actividades, métodos, procedimientos y herramientas utilizadas por el Operador de Telecomunicaciones para la operación, administración, mantenimiento y provisión de una red de telecomunicaciones que facilite el Acceso a Internet.

   Las prácticas de administración de red engloban una serie de subprocesos como la gestión de facturación y contabilidad, gestión de fallos y averías, gestión de la calidad, gestión de tráfico, gestión de seguridad, gestión remota de CPE (del inglés *Customer Premises Equipment*) o equipos terminales de usuario, gestión del soporte de energía, entre otros.

2. **Ataque de denegación de servicio (DoS):** Ataque informático, desde un solo punto de origen hacia la red de datos del Operador de Telecomunicaciones, que causa que un servicio o recurso sea inaccesible a los usuarios legítimos de la red.

3. **Ataque distribuido de denegación de servicio (DDoS):** Ataque informático, desde varios puntos de origen hacia la red de datos de un Operador de Telecomunicaciones, que causa que un servicio o recurso sea inaccesible a los usuarios legítimos de la red.

4. **Componentes con Tratamiento Diferenciado:** En el diseño de ofertas y planes comerciales el Operador de Telecomunicaciones escoge uno o un grupo de componentes tales como protocolos, tráfico, servicios, o aplicaciones; a los cuales les da un tratamiento diferenciado a nivel comercial, es decir tarifas diferenciadas o gratuitas. Asimismo, a condición de ofrecer este beneficio, puede limitar o establecer menores atributos técnicos a dichos componentes. Por su parte, debe entenderse que todos los otros componentes sin tratamiento diferenciado, así como las funcionalidades que no fueron incluidas en los Componentes con Tratamiento Diferenciado, conforman el concepto "Componentes sin Tratamiento Diferenciado", el cual sigue teniendo el mismo tratamiento del producto de Acceso a Internet del plan regular ofrecido al usuario.

5. **Condiciones de Uso:** Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobadas por la Resolución de Consejo Directivo Nº 138-2012-CD-OSIPTEL y las normas que la modifiquen o la sustituyan.

6. **Configuración de Equipos Terminales:** Acciones de configuración realizadas sobre los equipos o dispositivos terminales, tanto fijos como móviles, comercializados por el Operador de Telecomunicaciones, que permiten que los referidos dispositivos cumplan con las características técnicas ofrecidas por el fabricante y que se adecuen a los parámetros de funcionamiento que requiere la red. Incluye la modificación de ciertas características de hardware o software del dispositivo, realizadas de forma local o remota, como la instalación de aplicaciones específicas, personalización del sistema operativo o firmware del dispositivo, activación o desactivación de puertos en los *routers* del cliente, entre otros. Se incluye en este supuesto a los equipos de terminación de red -CPE-, tales como routers, switches, modems, etc.

7. **ETSI:** (del inglés *European Telecommunications Standards Institute*) Organización de estandarización independiente, sin fines de lucro de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa.

8. **Gestión de tráfico:** Conjunto de acciones por las cuales se analiza, administra y/o gestiona los paquetes o flujo de paquetes de datos; asignándoles recursos, capacidades de red y niveles de servicios tales como ancho de banda, disponibilidad, retardo, pérdida de paquetes, *jitter*, etc. La priorización, ralentización o degradación intencional, entre otras, realizada sobre los paquetes o flujo de paquetes de aplicaciones o servicios específicos o grupos de estos, son ejemplos de la gestión de tráfico. Las medidas de Gestión de Tráfico relativas a la Neutralidad de Red son aquellas que "tienen la potencialidad de bloquear, interferir, discriminar, restringir o degradar cualquier tipo de tráfico, protocolo, servicio o aplicación, independientemente de su origen, destino, naturaleza o propiedad".

   Las medidas de gestión de tráfico relativas al aprovisionamiento de servicios a los usuarios según las características de los productos comerciales ofrecidos, tales como velocidades nominales, velocidades mínimas garantizadas, y otros, no serán consideradas medidas relativas a la Neutralidad de Red.

9. **IETF:** (del inglés *Internet Engineering Task Force)* El Grupo de Trabajo de Ingeniería de Internet es una comunidad internacional abierta de diseñadores de redes, operadores, vendedores e investigadores dedicados a la evolución de la arquitectura de Internet y el buen funcionamiento de Internet. Dicho grupo de trabajo pertenece a la Sociedad de Internet ISOC (del inglés *Internet Society*), organización de membresía profesional de expertos en Internet que comenta las políticas y prácticas y supervisa una serie de otras juntas y grupos de trabajo que se ocupan de cuestiones de política de red.

10. **Internet:** Sistema mundial de redes de datos interconectadas basadas en el uso del protocolo IP que les permite funcionar como un gran red virtual.

11. **Interrupción del Servicio:** Incapacidad total o parcial que imposibilite o dificulte la prestación del servicio, caracterizada por un inadecuado funcionamiento de uno o más elementos de red.

12. **Medida arbitraria relativa a la Neutralidad de Red:** Es toda aquella medida prohibida por el presente Reglamento.

13. **Medida no arbitraria relativa a la Neutralidad de Red:** Es toda aquella medida permitida por el presente Reglamento y la que a pesar de no estar contemplada, no vulnera los principios establecidos en el artículo 5.

14. **Medida relativa a la Neutralidad de Red:** Medidas de administración de red, tales como gestión de tráfico, configuración de equipos terminales, o alguna otra que tenga la potencialidad de bloquear, interferir, discriminar, restringir o degradar cualquier tipo de tráfico, protocolo, servicio o aplicación, independientemente de su origen, destino, naturaleza o propiedad.

15. **Normativa General Aplicable:** Conjunto de disposiciones legales que regulan o influyen directa o indirectamente respecto de la Neutralidad de Red. Incluyen la

Constitución Política del Perú, la Ley de promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fibra Óptica, Ley Nº 29904, el Reglamento de la Ley Nº 29904, Decreto Supremo Nº 014-2013-MTC, la Ley Nº 27336, Ley de Desarrollo de las Funciones y Facultades de OSIPTEL, la Ley Nº 27332, Ley Marco de Organismos Reguladores de la Inversión Privada en los Servicios Públicos, la Ley Nº 27444, Ley del Procedimiento Administrativo General, el Decreto Supremo Nº 008-2001-PCM, Reglamento General de OSIPTEL; así como las normas que los sustituyan, modifiquen o complementen.

16. **Operador de Telecomunicaciones:** Persona natural o jurídica que cuenta con concesión o registro para prestar uno o más servicios públicos de telecomunicaciones, en los cuales se incluye la prestación del servicio público de valor añadido de conmutación de datos por paquetes (provisión del Servicio de Acceso a Internet), y/o que participa directa o indirectamente en la provisión del servicio de acceso a Internet, ya sea brindándolo directamente, u ofreciendo sus redes para que a través de ellas se curse tráfico de acceso a Internet de terceros operadores.

    Para efectos del presente Reglamento, el Proveedor del Servicio de Acceso a Internet tiene el mismo tratamiento que el Operador de Telecomunicaciones.

17. **Proveedor de aplicaciones, servicios o contenidos en Internet:** Persona natural o jurídica que, vinculada o no, directa o indirectamente al Proveedor del Servicio de Acceso a Internet o al Operador de Telecomunicaciones, provee aplicaciones, servicios o contenidos, soportados en el Acceso a Internet, de forma gratuita o con una tarifa determinada.

18. **Proveedor del Servicio de Acceso a Internet:** Operador de Telecomunicaciones, que en la forma de persona natural o jurídica, cuenta con el registro correspondiente para prestar el servicio público de valor añadido de conmutación de datos por paquetes (Internet). Se encuentran comprendidos en esta categoría las empresas que se dedican únicamente a prestar servicios de Acceso a Internet; así como los concesionarios de servicios portadores, finales y de difusión, empresas con registro de comercialización de servicios públicos de telecomunicaciones, empresas con registro de operador móvil virtual, que además de sus respectivos servicios autorizados, también presten servicios de Acceso a Internet.

19. **Servicio de Acceso a Internet:** Servicio público de telecomunicaciones que permite el acceso a todos los nodos disponibles de Internet, independientemente de la tecnología de acceso o equipamiento del terminal utilizado para la prestación del servicio. El Servicio de Acceso a Internet no incluye a los servicios especializados.

20. **Servicios especializados:** Servicios que utilizan el protocolo IP y son distintos a los servicios de Acceso a Internet, o a los servicios o aplicaciones comúnmente disponibles a través del Acceso a Internet; y se ofrecen en forma independiente al Acceso a Internet, mediante optimización en la red IP del operador para soportar determinados tipos de tráfico o protocolos, siendo dicha optimización objetivamente necesaria para asegurar niveles de calidad mínimos requeridos para su funcionamiento.

21. **UIT:** Unión Internacional de Telecomunicaciones. Es el organismo especializado de

las Naciones Unidas en el campo de las telecomunicaciones.

22. UIT-T: Sector de Normalización de las Telecomunicaciones de la UIT. Es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

ANEXO II

INFORMACIÓN DE MEDIDAS AUTORIZADAS RELATIVAS A LA NEUTRALIDAD DE RED, PUBLICADAS A TRAVÉS DEL SITIO WEB DEL OPERADOR DE TELECOMUNICACIONES

La información provista por el Operador de Telecomunicaciones sobre las medidas autorizadas relativas a la Neutralidad de Red que contendrá el sitio web (mencionada en el artículo 6) es la siguiente:

Información de normativa sobre Neutralidad de Red

- Incluir la definición de cada medida reportada por el Operador de Telecomunicaciones (según el cuadro). La información deberá ser presentada en términos sencillos y amigables para el usuario final. La información debe estar relacionada a las definiciones establecidas en el Reglamento de Neutralidad de Red.
- Agregar un enlace que dirija al Reglamento de Neutralidad de Red alojado en el portal institucional del OSIPTEL.

Información de medidas relativas a la Neutralidad de Red implementadas

Las siguientes medidas relativas a la Neutralidad de Red fueron implementadas o continúan siendo implementadas en nuestra red para provisión de nuestros servicios:

	Tipo de medida(1)	*Servicio asociado a la medida (2)*	*Frecuencia de aplicación (3)*	*Parámetro adicional informativo (4)*
1				
2				
3				
4				
...				

(1) Mencionar cuáles de las medidas calificadas como permitidas son implementadas en la red del Operador de Telecomunicaciones.

(2) Especificar si la medida aplica a todo Servicio de Acceso a Internet o si solo se aplica al Servicio de Acceso a Internet fijo o móvil, de no ser a nivel nacional, indicar en qué ámbito geográfico se aplica la medida.

(3) Especificar si la medida permitida se aplica de manera permanente o en un lapso de tiempo específico.

(4) El parámetro adicional informativo, en los casos que aplique, deberá contener lo siguiente:

- Para Duración de la Sesión Dinámica en la Red, se deberá especificar el tiempo de inactividad (en horas o minutos) para proceder con el reinicio.
- Para el uso de CDN, indicar los tipos de servicios y/o aplicaciones incluidos en el CDN.
- Para Gestión de direcciones IP, se deberá especificar si la implementación afecta el normal funcionamiento del Servicio de Acceso a Internet del abonado, e indicar los protocolos, tipo de tráfico, aplicaciones o servicios excepcionalmente afectados, y las soluciones que el usuario o el operador podría adoptar para mitigar dichas afectaciones.
- Para Filtro y/o Bloqueo de Servicios y/o Aplicaciones en cumplimiento de obligaciones contractuales con el Estado o con motivo de una norma especifica, indicar los puertos desde y hacia Internet; nombres de dominio y/o direcciones IP; y/o aplicaciones y/o servicios bloqueados así como la justificación del bloqueo.
- Cualquier otra información relacionada a las medidas permitidas que el Operador de Telecomunicaciones considere importante.

ANEXO III

REGISTRO DE INFORMACIÓN DE IMPLEMENTACIÓN DE MEDIDAS DE EMERGENCIA

El contenido del registro de medidas implementadas ante una situación de emergencia, por cada evento de emergencia registrado, deberá contener la siguiente información:

REGISTRO DE MEDIDAS DE EMERGENCIA RELATIVA A LA NEUTRALIDAD DE RED		
Emergencia relativa a la Neutralidad de Red	Inicio (día y hora):	
	Fin (día y hora):	
	Tipo de emergencia:	
	Descripción de la emergencia:	
Implementación de la medida en la red	Inicio (día y hora):	
	Fin (día y hora): (Si la medida continúa activa, indicar el tiempo estimado que estará activa).	
	Tipo de implementación realizada en la red:	
	Acciones realizadas:	
	Servicios afectados:	
	Información adicional de sustento: (Adjuntar log de los sistemas de red, informe técnico de la empresa, informe técnico del proveedor, etc.)	

ANEXO IV

Procedimiento para la solicitud de un Operador de Telecomunicaciones a otro Operador de Telecomunicaciones para la implementación de medidas de emergencia relativas a la Neutralidad de Red

1. La solicitud puede ser remitida por correo electrónico, siempre que, previo consentimiento, estos consten en el contrato suscrito entre ambas partes o en documento posterior que acredite la autorización del uso de este mecanismo.

2. El Operador de Telecomunicaciones que remite la solicitud podrá remitir copia de la misma al OSIPTEL.

3. La solicitud debe contener de manera precisa, el problema presentado en su red y el objetivo de su requerimiento, el cual podría incluir la propuesta de medida de emergencia que debe ser implementada.

4. La medida de emergencia relativa a la Neutralidad de Red debe ser implementada por el operador que recibe la solicitud (Operador de Telecomunicaciones que brinda el Servicio de Acceso a Internet al operador solicitante), como máximo dentro de los dos (2) días hábiles, contados desde el día siguiente de recibida la solicitud.

5. En caso el Operador de Telecomunicaciones que recibe la solicitud requiera de un tiempo adicional para cumplir con la implementación solicitada, debe comunicarlo por escrito, dentro de los dos (2) días hábiles, contados desde el día siguiente de recibida la solicitud, indicando como mínimo las razones por las cuales requiere de más tiempo para cumplir con la implementación. El tiempo máximo en que se implemente la medida no puede exceder de ocho (8) días hábiles contados desde recibida la solicitud.

6. En caso el Operador de Telecomunicaciones que recibe la solicitud considere que la solicitud sea inviable de implementar, debe comunicarlo por escrito al OSIPTEL y al operador que solicita la acción, dentro de los dos (2) días hábiles, contados desde el día siguiente de recibida la solicitud, indicando, como mínimo las razones por las cuales la solicitud es inviable de ser implementada.

7. Cualquier efecto sobreviniente a causa de la no implementación de la medida solicitada es de exclusiva responsabilidad del operador que presta el Servicio de Acceso a Internet al operador que remitió la solicitud.

ANEXO V

INFRACCIONES Y SANCIONES

Ítem	Infracción	Sanción
1	Incurre en infracción leve el Operador de Telecomunicaciones que: a) no ponga a disposición de los usuarios, a través de su sitio web, la información relativa a la Neutralidad de Red y las medidas que implemente en sus redes; b) no haya comunicado al OSIPTEL al menos un día hábil antes de publicarse en su sitio web, la información relativa a la Neutralidad de Red y las medidas que implemente en sus redes o su actualización; c) no efectúe la publicación en su sitio web de dicha información en los términos dispuestos en el Anexo II; d) publique información que sea falsa o inexacta; y/o, e) aplique medidas relativas a la Neutralidad de Red, distintas a las comunicadas al OSIPTEL.	Leve
2	El Operador de Telecomunicaciones que no cumpla con la orden de cese temporal o definitivo emitida por el OSIPTEL, o lo efectúa fuera del plazo establecido para el caso particular, incurre en infracción muy grave (artículo 10).	Muy Grave
3	Incurre en infracción el Operador de Telecomunicaciones que: a) implemente medidas de gestión de Direcciones IP, sin cumplir con los requerimientos establecidos en el artículo 19; o, b) implemente medidas de Duración de la Sesión Dinámica en la Red, sin cumplir con los requerimientos establecidos en el artículo 20.	Leve
4	El Operador de Telecomunicaciones que mantenga una medida aplicada por encima del tiempo que duró el ataque, sin restituir la configuración inicial del servicio, incurre en infracción leve, por cada evento (artículo 23).	Leve
5	Incurre en infracción leve, el Operador de Telecomunicaciones que: a) no implemente y ejecute un Protocolo de Acción ante Situaciones de Emergencia (artículo 25); o,	Leve

Ítem	Infracción	Sanción
	b) no haya comunicado al OSIPTEL, al menos un día hábil antes de entrar en vigor, el Protocolo de Acción ante Situaciones de Emergencia implementado o su actualización; y/o, c) aplique protocolos, distintos a los comunicados al OSIPTEL (artículo 24).	
6	Incurre en infracción leve el Operador de Telecomunicaciones que al implementar una medida de emergencia relativa a la Neutralidad de Red, o implementar una medida de gestión de tráfico no arbitraria, no cumple con las obligaciones de registro y comunicación según los requerimientos establecidos en el artículo 27 y artículo 28.	Leve
7	Incurre en infracción leve, por cada evento, el Operador de Telecomunicaciones que: a) no implemente la medida de emergencia solicitada por el operador al cual le presta servicios, salvo que se acredite que su implementación es inviable (artículo 29); y/o, b) no cumpla con los plazos y términos establecidos en el Anexo IV, aun cuando acredite que la implementación de la medida de emergencia es inviable (artículo 29).	Leve
8	Incurre en infracción grave el Operador de Telecomunicaciones que bloquea puertas de entrada lógicas en el equipo terminal del usuario, desde y/o hacia Internet; dominios o direcciones IP; o, aplicaciones y/o servicios, siempre que: a) no haya sido solicitado expresamente por el abonado (artículo 34); b) no responda al cumplimiento de una obligación expresa establecida en norma específica o en las estipulaciones contractuales suscritas con el Estado (artículo 18); y/o, c) no responda a una medida solicitada por mandato judicial (artículo 12, inciso 3).	Grave
9	Incurre en infracción grave el Operador de Telecomunicaciones que realiza o aplica:	Grave

Ítem	Infracción	Sanción
	a) Cualquier Gestión arbitraria de Tráfico (artículo 33); b) Cualquier Diferenciación arbitraria en la oferta comercial de productos de Acceso a Internet (artículo 35).	
10	La presentación al OSIPTEL, de información falsa, incompleta o inexacta, proporcionada por el Operador de Telecomunicaciones en el cumplimiento del presente Reglamento, será evaluada, por cada periodo anual, de acuerdo a lo previsto en el Reglamento de Fiscalización, Infracciones y Sanciones, aprobado por Resolución N° 087-2013-CD/OSIPTEL, o la norma que lo modifique o sustituya.	

Anexo 11: Ley Argentina Digital

Título VII

Consideraciones generales sobre los Servicios de TIC

ARTÍCULO 54.— *Servicio Público Telefónico.* El Servicio Básico Telefónico mantiene su condición de servicio público.

ARTÍCULO 55.— *Objeto y alcance*. El Servicio de TIC comprende la confluencia de las redes tanto fijas como móviles que, mediante diversas funcionalidades, proporciona a los usuarios la capacidad de recibir y transmitir información de voz, audio, imágenes fijas o en movimiento y datos en general.

A los efectos de resguardar la funcionalidad del Servicio de TIC, éste deberá ser brindado en todo el territorio nacional considerado a tales efectos como una única área de explotación y prestación.

El Servicio Básico Telefónico, sin perjuicio de su particularidad normativa, reviste especial consideración dentro del marco de la convergencia tecnológica. Es por ello que la efectiva prestación del servicio debe ser considerada de manera independiente a la tecnología o medios utilizados para su provisión a través de las redes locales, siendo su finalidad principal el establecimiento de una comunicación mediante la transmisión de voz entre partes.

ARTÍCULO 56.— *Neutralidad de red.* Se garantiza a cada usuario el derecho a acceder, utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, servicio o protocolo a través de Internet sin ningún tipo de restricción, discriminación, distinción, bloqueo, interferencia, entorpecimiento o degradación.

ARTÍCULO 57.— *Neutralidad de red. Prohibiciones*. Los prestadores de Servicios de TIC no podrán:

a) Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o expresa solicitud del usuario.

b) Fijar el precio de acceso a Internet en virtud de los contenidos, servicios, protocolos o aplicaciones que vayan a ser utilizados u ofrecidos a través de los respectivos contratos.

c) Limitar arbitrariamente el derecho de un usuario a utilizar cualquier hardware o software para acceder a Internet, siempre que los mismos no dañen o perjudiquen la red.

ARTÍCULO 58.— *Velocidad Mínima de Transmisión (VMT).* La Autoridad de Aplicación definirá, en un plazo no mayor a ciento ochenta (180) días a contar desde la entrada en vigencia de la presente ley, la Velocidad Mínima de Transmisión (VMT) que deberán posibilitar las redes de telecomunicaciones a los fines de asegurar la efectiva funcionalidad de los Servicios de TIC. Los licenciatarios de Servicios de TIC deberán proveer a sus usuarios finales, no licenciatarios de estos servicios, la velocidad fijada. La VMT deberá ser revisada con una periodicidad máxima de dos (2) años.

Título VIII
Derechos y obligaciones de los usuarios y licenciatarios de Servicios de TIC

Capítulo I
Derechos y obligaciones de los usuarios de los Servicios de TIC

ARTÍCULO 59. — *Derechos.* El usuario de los Servicios de TIC tiene derecho a:

a) Tener acceso al Servicio de TIC en condiciones de igualdad, continuidad, regularidad y calidad.

b) Ser tratado por los licenciatarios con cortesía, corrección y diligencia.

c) Tener acceso a toda la información relacionada con el ofrecimiento o prestación de los servicios.

d) Elegir libremente el licenciatario, los servicios y los equipos o aparatos necesarios para su prestación, siempre que estén debidamente homologados.

e) Presentar, sin requerimientos previos innecesarios, peticiones y quejas ante el licenciatario y recibir una respuesta respetuosa, oportuna, adecuada y veraz.

f) La protección de los datos personales que ha suministrado al licenciatario, los cuales no pueden ser utilizados para fines distintos a los autorizados, de conformidad con las disposiciones vigentes.

g) Que el precio del servicio que recibe sea justo y razonable.

h) Los demás derechos que se deriven de la aplicación de las leyes, reglamentos y normas aplicables.

ARTÍCULO 60. — *Obligaciones.* El usuario de los Servicios de TIC tiene las siguientes obligaciones:

a) Abonar oportunamente los cargos por los servicios recibidos, de conformidad con los precios contratados o las tarifas establecidas.

b) Mantener las instalaciones domiciliarias a su cargo de manera adecuada a las normas técnicas vigentes.

c) No alterar los equipos terminales cuando a consecuencia de ello puedan causar daños o interferencias que degraden la calidad del servicio, absteniéndose de efectuar un uso indebido del servicio.

d) Permitir el acceso del personal de los licenciatarios y de la Autoridad de Aplicación, quienes deberán estar debidamente identificados a los efectos de realizar todo tipo de trabajo o verificación necesaria.

e) Respetar las disposiciones legales, reglamentarias y las condiciones generales de contratación y las demás obligaciones que se deriven de la aplicación de las leyes, reglamentos y normas aplicables.

Anexo 12: Ley Federal Telecomunicaciones México

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.

Anexo 13: FCC reglas para Internet Abierto

NEWS

Federal Communications Commission
445 12th Street, S.W.
Washington, D. C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

FOR IMMEDIATE RELEASE:
February 26, 2015

NEWS MEDIA CONTACT:
Mark Wigfield, 202-418-0253
E-mail: mark.wigfield@fcc.gov

FCC ADOPTS STRONG, SUSTAINABLE RULES TO PROTECT THE OPEN INTERNET

Rules Will Preserve the Internet as a Platform for Innovation, Free Expression and Economic Growth

Washington, D.C. – Ending lingering uncertainty about the future of the Open Internet, the Federal Communications Commission today set sustainable rules of the roads that will protect free expression and innovation on the Internet and promote investment in the nation's broadband networks.

The FCC has long been committed to protecting and promoting an Internet that nurtures freedom of speech and expression, supports innovation and commerce, and incentivizes expansion and investment by America's broadband providers. But the agency's attempts to implement enforceable, sustainable rules to protect the Open Internet have been twice struck down by the courts.

Today, the Commission—once and for all—enacts strong, sustainable rules, grounded in multiple sources of legal authority, to ensure that Americans reap the economic, social, and civic benefits of an Open Internet today and into the future. These new rules are guided by three principles: America's broadband networks must be fast, fair and open—principles shared by the overwhelming majority of the nearly 4 million commenters who participated in the FCC's Open Internet proceeding.

Absent action by the FCC, Internet openness is at risk, as recognized by the very court that struck down the FCC's 2010 Open Internet rules last year in *Verizon v. FCC*.

Broadband providers have economic incentives that "represent a threat to Internet openness and could act in ways that would ultimately inhibit the speed and extent of future broadband deployment," as affirmed by the U.S. Court of Appeals for the District of Columbia. The court upheld the Commission's finding that Internet openness drives a "virtuous cycle" in which innovations at the edges of the network enhance consumer demand, leading to expanded investments in broadband infrastructure that, in turn, spark new innovations at the edge.

However, the court observed that nearly 15 years ago, the Commission constrained its ability to protect against threats to the open Internet by a regulatory classification of broadband that precluded use of statutory protections that historically ensured the openness of telephone networks. The Order finds that the nature of broadband Internet access service has not only changed since that initial classification decision, but that broadband providers have even more incentives to interfere with Internet openness today. To respond to this changed landscape, the new Open Internet Order restores the FCC's legal authority to fully address threats to openness on today's networks by following a template for sustainability laid out in the D.C. Circuit Opinion itself, including reclassification of broadband Internet access as a telecommunications service under Title II of the Communications Act.

With a firm legal foundation established, the Order sets three "bright-line" rules of the road for behavior known to harm the Open Internet, adopts an additional, flexible standard to future-proof Internet openness rules, and protects mobile broadband users with the full array of Open Internet rules. It does so while preserving incentives for investment and innovation by broadband providers by affording them an even more tailored version of the light-touch regulatory treatment that fostered tremendous growth in the mobile wireless industry.

Following are the key provisions and rules of the FCC's Open Internet Order:

New Rules to Protect an Open Internet
While the FCC's 2010 Open Internet rules had limited applicability to mobile broadband, the new rules—in their entirety—would apply to fixed and mobile broadband alike, recognizing advances in technology and the growing significance of wireless broadband access in recent years (while recognizing the importance of reasonable network management and its specific application to mobile and unlicensed Wi-Fi networks). The Order protects consumers no matter how they access the Internet, whether on a desktop computer or a mobile device.

Bright Line Rules: The first three rules ban practices that are known to harm the Open Internet:

- **No Blocking**: broadband providers may not block access to legal content, applications, services, or non-harmful devices.

- **No Throttling**: broadband providers may not impair or degrade lawful Internet traffic on the basis of content, applications, services, or non-harmful devices.

- **No Paid Prioritization**: broadband providers may not favor some lawful Internet traffic over other lawful traffic in exchange for consideration of any kind—in other words, no "fast lanes." This rule also bans ISPs from prioritizing content and services of their affiliates.

The bright-line rules against blocking and throttling will prohibit harmful practices that target specific applications or classes of applications. And the ban on paid prioritization ensures that there will be no fast lanes.

A Standard for Future Conduct: Because the Internet is always growing and changing, there must be a known standard by which to address any concerns that arise with new practices. The Order establishes that ISPs cannot "unreasonably interfere with or unreasonably disadvantage" the ability of consumers to select, access, and use the lawful content, applications, services, or devices of their choosing; or of edge providers to make lawful content, applications, services, or devices available to consumers. Today's Order ensures that the Commission will have authority to address questionable practices on a case-by-case basis, and provides guidance in the form of factors on how the Commission will apply the standard in practice.

Greater Transparency: The rules described above will restore the tools necessary to address specific conduct by broadband providers that might harm the Open Internet. But the Order recognizes the critical role of transparency in a well-functioning broadband ecosystem. In addition to the existing transparency rule, which was not struck down by the court, the Order requires that broadband providers disclose, in a consistent format, promotional rates, fees and surcharges and data caps. Disclosures must also include packet loss as a measure of network performance, and provide notice of network management practices that can affect service. To further consider the concerns of small ISPs, the Order adopts a temporary exemption from the transparency enhancements for fixed and mobile providers with 100,000 or fewer subscribers, and delegates authority to our Consumer and Governmental Affairs Bureau to determine whether to retain the exception and, if so, at what level.

The Order also creates for all providers a "safe harbor" process for the format and nature of the required disclosure to consumers, which the Commission believes will lead to more effective presentation of consumer-focused information by broadband providers.

Reasonable Network Management: For the purposes of the rules, other than paid prioritization, an ISP may engage in reasonable network management. This recognizes the need of broadband providers to manage the technical and engineering aspects of their networks.

- In assessing reasonable network management, the Commission's standard takes account of the particular engineering attributes of the technology involved—whether it be fiber, DSL, cable, unlicensed Wi-Fi, mobile, or another network medium.

- However, the network practice must be primarily used for and tailored to achieving a legitimate network management—and not business—purpose. For example, a provider can't cite reasonable network management to justify reneging on its promise to supply a customer with "unlimited" data.

Broad Protection
Some data services do not go over the public Internet, and therefore are not "broadband Internet access" services (VoIP from a cable system is an example, as is a dedicated heart-monitoring service). The Order ensures that these services do not undermine the effectiveness of the Open Internet rules. Moreover, all broadband providers' transparency disclosures will continue to cover any offering of such non-Internet access data services—ensuring that the public and the Commission can keep a close eye on any tactics that could undermine the Open Internet rules.

Interconnection: New Authority to Address Concerns
For the first time the Commission can address issues that may arise in the exchange of traffic between mass-market broadband providers and other networks and services. Under the authority provided by the Order, the Commission can hear complaints and take appropriate enforcement action if it determines the interconnection activities of ISPs are not just and reasonable.

Legal Authority: Reclassifying Broadband Internet Access under Title II
The Order provides the strongest possible legal foundation for the Open Internet rules by relying on multiple sources of authority including both Title II of the Communications Act and Section 706 of the Telecommunications Act of 1996. At the same time, the Order refrains – or forbears – from enforcing 27 provisions of Title II and over 700 associated regulations that are not relevant to modern broadband service. Together Title II and Section 706 support clear rules of the road, providing the certainty needed for innovators and investors, and the competitive choices and freedom demanded by consumers, while not burdening broadband providers with anachronistic utility-style regulations such as rate regulation, tariffs or network sharing requirements.

- First, the Order reclassifies "broadband Internet access service"—that's the retail broadband service Americans buy from cable, phone, and wireless providers—as a telecommunications service under Title II. This decision is fundamentally a factual one. It recognizes that today broadband Internet access service is understood by the public as a transmission platform through which consumers can access third-party content, applications, and services of their choosing. Reclassification of broadband Internet access service also addresses any limitations that past classification decisions placed on the ability to adopt strong open Internet rules, as interpreted by the D.C. Circuit in the *Verizon* case. And it supports the Commission's authority to address interconnection disputes on a case-by-case basis, because the promise to consumers that they will be able to travel the Internet encompasses the duty to make the necessary arrangements that allow consumers to use the Internet as they wish.

- Second, the proposal finds further grounding in Section 706 of the Telecommunications Act of 1996. Notably, the *Verizon* court held that Section 706 is an independent grant of authority to the Commission that supports adoption of Open Internet rules. Using it here—without the limitations of the common carriage prohibition that flowed from earlier the "information service" classification—bolsters the Commission's authority.

- Third, the Order's provisions on mobile broadband also are based on Title III of the Communications Act. The Order finds that mobile broadband access service is best viewed as a commercial mobile service or its functional equivalent.

Forbearance: A modernized, light-touch approach

Congress requires the FCC to refrain from enforcing – forbear from – provisions of the Communications Act that are not in the public interest. The Order applies some key provisions of Title II, and forbears from most others. Indeed, the Order ensures that some 27 provisions of Title II and over 700 regulations adopted under Title II will not apply to broadband. There is no need for any further proceedings before the forbearance is adopted. *The proposed Order would apply fewer sections of Title II than have applied to mobile voice networks for over twenty years.*

- ***Major Provisions of Title II that the Order WILL APPLY:***
    - The proposed Order applies "core" provisions of Title II: Sections 201 and 202 (e.g., no unjust or unreasonable practices or discrimination)
    - Allows investigation of consumer complaints under section 208 and related enforcement provisions, specifically sections 206, 207, 209, 216 and 217
    - Protects consumer privacy under Section 222
    - Ensures fair access to poles and conduits under Section 224, which would boost the deployment of new broadband networks
    - Protects people with disabilities under Sections 225 and 255
    - Bolsters universal service fund support for broadband service in the future through partial application of Section 254.
- ***Major Provisions Subject to Forbearance:***
    - Rate regulation: the Order makes clear that broadband providers **shall not** be subject to utility-style rate regulation, including rate regulation, tariffs, and last-mile unbundling.
    - Universal Service Contributions: the Order **DOES NOT** require broadband providers to contribute to the Universal Service Fund under Section 254. The question of how best to fund the nation's universal service programs is being considered in a separate, unrelated proceeding that was already underway.
    - Broadband service will remain exempt from state and local taxation under the Internet Tax Freedom Act. This law, recently renewed by Congress and signed by the President, bans state and local taxation on Internet access regardless of its FCC regulatory classification.

Effective Enforcement

- The FCC will enforce the Open Internet rules through investigation and processing of formal and informal complaints
- Enforcement advisories, advisory opinions and a newly-created ombudsman will provide guidance
- The Enforcement Bureau can request objective written opinions on technical matters from outside technical organizations, industry standards-setting bodies and other organizations.

Fostering Investment and Competition

All of this can be accomplished while encouraging investment in broadband networks. To preserve incentives for broadband operators to invest in their networks, the Order will modernize Title II using the forbearance authority granted to the Commission by Congress—tailoring the application of Title II for the 21st century, encouraging Internet Service Providers to invest in the networks on which Americans increasingly rely.

- The Order forbears from applying utility-style rate regulation, including rate regulation or tariffs, last-mile unbundling, and burdensome administrative filing requirements or accounting standards.
- Mobile voice services have been regulated under a similar light-touch Title II approach, and investment and usage boomed.
- Investment analysts have concluded that Title II with appropriate forbearance is unlikely to have any negative on the value or future profitability of broadband providers. Providers such as Sprint, Frontier, as well as representatives of hundreds of smaller carriers that have voluntarily adopted Title II regulation, have likewise said that a light-touch, Title II classification of broadband will not depress investment.

Action by the Commission February 26, 2015, by Report and Order on Remand, Declaratory Ruling, and Order (FCC 15-24). Chairman Wheeler, Commissioners Clyburn and Rosenworcel with Commissioners Pai and O'Rielly dissenting. Chairman Wheeler, Commissioners Clyburn, Rosenworcel, Pai and O'Rielly issuing statements.

Docket No.: 14-28

-FCC-

News about the Federal Communications Commission can also be found on the Commission's web site www.fcc.gov.

Anexo 14: Directrices ORECE NR Europa

Body of European Regulators for Electronic Communications
BEREC

BoR (16) 127

BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules

August 2016

Contents

Background and general aspects

1. These BEREC Guidelines drafted in accordance with Article 5(3) of the Regulation[1] are designed to provide guidance on the implementation of the obligations of NRAs. Specifically, this includes the obligations to closely monitor and ensure compliance with the rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users rights as laid down in Articles 3 and 4. These Guidelines constitute recommendations to NRAs, and NRAs should take utmost account of the Guidelines.[2] The Guidelines should contribute to the consistent application of the Regulation, thereby contributing to regulatory certainty for stakeholders.

Terminology

2. For the purpose of these Guidelines, BEREC has used the following terms throughout the Guidelines to improve readability.[3]

Application	In these Guidelines, BEREC use the term "application" as a short expression for more lengthy expressions from the Regulation, like "applications and services", "content, application and service".
CAP (Content and Application Provider)	CAPs make content (e.g. web pages, blogs, video) and/or applications (e.g. search engines, VoIP applications) and/or services available on the Internet. CAPs may also make content, services and applications available via specialised services.
ISP (Internet Service Provider)	In these Guidelines, BEREC uses the term "ISP" to refer to providers of internet access services (IAS). ISPs may also be providers of specialised services.
Specialised service	In these Guidelines, BEREC uses the term "specialised services" as a short expression for "services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality" (ref. Article 3(5)).

[1] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying 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, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN

[2] As set out in Article 3(3) of the Regulation (EC) No 1211/2009 establishing the Body of European Regulators of Electronic Communications and the Office, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0001:0010:EN:PDF and recital 19 of Regulation (EU) 2015/2120

[3] Definitions of terms used in the Regulation are provided in the relevant parts of the Guidelines

Article 1
Subject matter and scope

This Regulation establishes common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights.

Recital 1
This Regulation aims to establish common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights. It aims to protect end-users and simultaneously to guarantee the continued functioning of the internet ecosystem as an engine of innovation.

Recital 2
The measures provided for in this Regulation respect the principle of technological neutrality, that is to say they neither impose nor discriminate in favour of the use of a particular type of technology.

Recital 3
The internet has developed over the past decades as an open platform for innovation with low access barriers for end-users, providers of content, applications and services and providers of internet access services. The existing regulatory framework aims to promote the ability of end-users to access and distribute information or run applications and services of their choice. However, a significant number of end-users are affected by traffic management practices which block or slow down specific applications or services. Those tendencies require common rules at the Union level to ensure the openness of the internet and to avoid fragmentation of the internal market resulting from measures adopted by individual Member States.

3. Article 1 sets out the subject matter and scope of the Regulation, which is to establish common rules to safeguard *"equal and non-discriminatory treatment of traffic in the provision of internet access services"* and *"related end-users' rights"*.

4. According to the Framework Directive,[4] *"end-user"* means a user not providing public communications networks or publicly available electronic communications services. In turn, *"user"* means a legal entity or natural person using or requesting a publicly available electronic communications service. On that basis, BEREC understands *"end-user"* to encompass individuals and businesses, including consumers as well as CAPs.

5. CAPs are protected as end-users under the Regulation in so far as CAPs use an IAS to reach other end-users. However, some CAPs may also operate their own networks and, as part of that, have interconnection agreements with ISPs; the provision of interconnection is a distinct service from the provision of IAS.

6. NRAs may take into account the interconnection policies and practices of ISPs in so far as they have the effect of limiting the exercise of end-user rights under Article 3(1). For

[4] Article 2 of Framework Directive (2002/21/EC) ref. lit. (n) and lit. (h). The directive has been amended by the regulation 717/2007/EC, the regulation 544/2009/EC and the directive 2009/140/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0021:20091219:EN:PDF)

example, this may be relevant in some cases, such as if the interconnection is implemented in a way which seeks to circumvent the Regulation.[5]

Article 2
Definitions

For the purposes of this Regulation, the definitions set out in Article 2 of Directive 2002/21/EC apply. The following definitions also apply:

7. The definitions of Article 2 of Directive 2002/21/EC also apply for the purposes of these Guidelines. This includes the terms *"end-user"*, *"consumer"*, *"electronic communications services", "electronic communications network"* and *"network termination point (NTP)"*.

"Provider of electronic communications to the public"

(1) 'provider of electronic communications to the public' means an undertaking providing public communications networks or publicly available electronic communications services;

8. The term *"provider of electronic communications to the public"* (PECP) comprises both *"public communications networks"* and *"electronic communications services"* (ECS), which are defined in Article 2 of the Framework Directive.[6]
9. Conversely, the definition of PECP does not cover providers of electronic communication services or communication networks that are *not* publicly available, which are therefore out of scope of this Regulation.
10. Electronic communication services or networks that are offered not only to a predetermined group of end-users but in principle to any customer who wants to subscribe to the service or network should be considered to be publicly available. Electronic communication services or networks that are offered only to a *predetermined* group of end-users could be considered to be not publicly available.
11. Virtual private network (VPN) services are typically offered by PECPs to anyone that wishes to enter a contract about the provision of such a service. These would therefore typically be considered to be publicly available, although the operation of a specific VPN would be a private network. The term 'private' describes the use of such a service which is usually limited to endpoints of the business entering the contract and is secured for internal communications. VPNs are further discussed in paragraph 115.
12. The following examples could be considered as services or networks not being made publicly available, subject to a case-by-case assessment by NRAs taking into account national practices:
    - access to the internet provided by cafés and restaurants;
    - internal corporate networks.

[5] Recital 7: *"Such agreements, as well as any commercial practices of providers of internet access services, should not limit the exercise of those rights and thus circumvent provisions of this Regulation safeguarding open internet access"*
[6] Ref. Article 2 (d) for *"public communications network"* and (c) for *"electronic communications service"*

Examples of criteria which could be used to make assessments include the contractual relationship under which the service is provided, the range of users and whether the range is predetermined.

"Internet access service"

(2) 'internet access service' means a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used.

Recital 4
An internet access service provides access to the internet, and in principle to all the end-points thereof, irrespective of the network technology and terminal equipment used by end-users. However, for reasons outside the control of providers of internet access services, certain end points of the internet may not always be accessible. Therefore, such providers should be deemed to have complied with their obligations related to the provision of an internet access service within the meaning of this Regulation when that service provides connectivity to virtually all end points of the internet. Providers of internet access services should therefore not restrict connectivity to any accessible end-points of the internet.

13. Article 2(2) defines an *"internet access service"* (IAS) as an ECS that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used.
14. For the purpose of the Regulation, BEREC understands the term *"internet"* as referring to a global system of interconnected networks that enables connected end-users to connect to one another. An IAS enables such access to the internet.
15. BEREC understands the term *"connectivity to virtually all end-points"* as a consequence of the fact that the internet is a distributed system where a single ISP controls a rather limited part. Due to reasons outside the control of an individual ISP (e.g. technical limitations, the policy of other ISPs or regulation in some countries), not all endpoints might be reachable all of the time. However, such a lack of reachability should not preclude that the service is defined as an IAS.
16. Where restrictions to reach end-points stem from the use of two different internet addressing schemes, IPv4 and IPv6, this typically does not mean the services cannot be defined as an IAS. While it is not possible to connect two different points with different types of addresses without any translation function, BEREC considers that the term *"virtually all end points"* should, at present, not be interpreted as a requirement on ISPs to offer connectivity with both IPv4 and IPv6.
17. BEREC understands a sub-internet service to be a service which restricts access to services or applications (e.g. banning the use of VoIP or video streaming) or enables access to only a pre-defined part of the internet (e.g. access only to particular websites). NRAs should take into account the fact that an ISP could easily circumvent the Regulation by providing such sub-internet offers. These services should therefore be considered to be in the scope of the Regulation and the fact that they provide a limited access to the internet should constitute an infringement of Articles 3(1), 3(2) and 3(3) of the Regulation. BEREC refers to these service offers as 'sub-internet services', as further discussed in paragraphs 38 and 55.

18. Services where the number of reachable end-points is limited by the nature of the terminal equipment used with such services (e.g. services designed for communication with individual devices, such as e-book readers as well as machine-to-machine[7] devices like smart meters etc.) are considered to be outside the scope of the Regulation unless they are used to circumvent this Regulation. They could use an IAS (but not provide an IAS nor constitute a substitute to an IAS), use a private network or constitute a specialised service. If these services are using an IAS or constitute a specialised service the connectivity service will be subject to the relevant rules applicable to IAS and specialised services in the Regulation.[8]

Article 3
Safeguarding of open internet access

19. Article 3 comprises measures intended to safeguard open internet access, covering the rights of the end-users of IAS, and obligations and permitted practices for the ISPs:

    - Article 3(1) sets out the rights of end-users of IAS;
    - Article 3(2) sets limits on the contractual conditions which may be applied to IAS and the commercial practices of ISPs providing IAS, and requires that these should not limit exercise of the end-user rights set out in paragraph 1. When assessing commercial practices, Article 3(3) should also be taken into account;
    - Article 3(3) constrains ISPs' traffic management practices, setting a requirement that ISPs should treat all data traffic equally and making provision for the specific circumstances under which ISPs may deviate from this rule;
    - Article 3(4) sets out the conditions under which traffic management measures may entail processing of personal data;
    - Article 3(5) sets out the freedom of ISPs and CAPs to provide specialised services as well as the conditions under which this freedom may be exercised.

20. The Regulation observes the fundamental rights of, and the principles recognised in, the Charter, notably the protection of personal data, the freedom of expression and information, the freedom to conduct a business, non-discrimination and consumer protection (ref. Recital 33).

21. BEREC considers that the Regulation does not require an ex ante authorisation in relation to commercial practices (Article 3(2)), traffic management practices (Article 3(3)) and specialised services (Article 3(5)). However, this should not preclude exchanges between NRAs and market players in relation to these issues, nor does it preclude NRAs from drawing on their obligations or powers to intervene under Article 5.

[7] However, some machine-to-machine communication services may also represent a specialised service according to Article 3(5) of the Regulation (ref. Recital 16 and paragraph 113 of these Guidelines). Moreover, a provider of an M2M device or M2M service (e.g. car manufacturer, provider of energy including smart meter) typically does not seem to provide an ECS under the present regulatory framework, whereas the connectivity service provider which provides connectivity over a public network for remuneration is generally the provider of an ECS in the IoT value chain (ref. BEREC Report on Enabling the Internet of Things, BoR (16) 39, pages 21-23).

[8] Notwithstanding, the provisions regarding specialised services apply – see paragraphs 99-127

Article 3(1)

End-users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end-user's or provider's location or the location, origin or destination of the information, content, application or service, via their internet access service.

This paragraph is without prejudice to Union law, or national law that complies with Union law, related to the lawfulness of the content, applications or services.

Recital 5
When accessing the internet, end-users should be free to choose between various types of terminal equipment as defined in Commission Directive 2008/63/EC (1). Providers of internet access services should not impose restrictions on the use of terminal equipment connecting to the network in addition to those imposed by manufacturers or distributors of terminal equipment in accordance with Union law.

Recital 6
End-users should have the right to access and distribute information and content, and to use and provide applications and services without discrimination, via their internet access service. The exercise of this right should be without prejudice to Union law, or national law that complies with Union law, regarding the lawfulness of content, applications or services. This Regulation does not seek to regulate the lawfulness of the content, applications or services, nor does it seek to regulate the procedures, requirements and safeguards related thereto. Those matters therefore remain subject to Union law, or national law that complies with Union law.

22. Article 3(1) sets out the end-users' rights with regard to the open internet. The notion of end-user is explained in paragraph 4 of these Guidelines.

"Access and distribute information and content"

23. Firstly, end-users have the right to access and distribute information and content. *"Access and distribute"* means that the provisions of this Regulation apply to both sending and receiving data over the IAS. *"Information and content"* is intended to cover any form of data that can be sent or received over the IAS.

"Use and provide applications and services"

24. Secondly, end-users have the right to use and provide applications and services. *"Use and provide"* means that the right applies both to consumption and provision of applications and services. *"Applications and services"* means both applications (including client and server software) as well as services.

"Use terminal equipment of their choice"

25. Thirdly, end-users have the right to use terminal equipment of their choice. Directive 2008/63/EC defines *"terminal equipment"* as *"equipment directly or indirectly connected to the interface of a public telecommunication network"*. The right to choose terminal equipment therefore covers equipment which connects to the interface of the public telecommunications network. This interface, the network termination point (NTP), is defined in Article 2 (da) of the Framework Directive (2002/21/EC), meaning the physical point at which a subscriber is provided with access to a public communications network.

26. In considering whether end-users may use the terminal equipment of their choice, NRAs should assess whether an ISP provides equipment for its subscribers and restricts the end-users' ability to replace that equipment with their own equipment, i.e. whether it provides *"obligatory equipment"*.

27. Moreover, NRAs should consider whether there is an objective technological necessity for the obligatory equipment to be considered as part of the ISP network. If there is not, and if the choice of terminal equipment is limited, the practice would be in conflict with the Regulation. For example, the practice of restricting tethering[9] is likely to constitute a restriction on choice of terminal equipment because ISPs *"should not impose restrictions on the use of terminal equipment connecting to the network in addition to those imposed by manufacturers or distributors of terminal equipment in accordance with Union law"* (Recital 5).

Legislation related to the lawfulness of the content, applications or services

28. Article 3(1) second subparagraph specifies that Union law, and national law that complies with Union law, related to the lawfulness of content, applications or services still applies. The TSM Regulation does not seek to regulate the lawfulness of the content, applications or services (ref. Recital 6).

29. Whereas Article 3(1) second subparagraph contains a clarification with regard to the applicability of such legislation, Article 3(3) (a) provides for an exception for ISPs to implement measures going beyond reasonable traffic management measures in order to comply with legislation or measures as specified in that exception.

Article 3(2)

Agreements between providers of internet access services and end-users on commercial and technical conditions and the characteristics of internet access services such as price, data volumes or speed, and any commercial practices conducted by providers of internet access services, shall not limit the exercise of the rights of end-users laid down in paragraph 1.

Recital 7

In order to exercise their rights to access and distribute information and content and to use and provide applications and services of their choice, end-users should be free to agree with providers of internet access services on tariffs for specific data volumes and speeds of the internet access service. Such agreements, as well as any commercial practices of providers of internet access services, should not limit the exercise of those rights and thus circumvent provisions of this Regulation safeguarding open internet access. National regulatory and other competent authorities should be empowered to intervene against agreements or commercial practices which, by reason of their scale, lead to situations where end-users' choice is materially reduced in practice. To this end, the assessment of agreements and commercial practices should, inter alia, take into account the respective market positions of those providers of internet access services, and of the providers of content, applications and services, that are involved. National regulatory and other competent authorities should be required, as part of their monitoring and enforcement function, to intervene when

[9] Tethering allows an end-user to share the internet connection of a phone or tablet with other devices such as laptops.

agreements or commercial practices would result in the undermining of the essence of the end-users' rights.

30. Article 3(2) clarifies that agreements between ISPs and end-users on commercial and technical conditions and the characteristics of IAS such as price, data volumes or speed, and any commercial practices conducted by ISPs are allowed, but shall not limit the exercise of the rights of end-users laid down in Article 3(1).

31. To BEREC's understanding, Article 3(2) contains two relevant aspects:

- the freedom to conclude agreements between ISPs and end-users relating to commercial and technical conditions as well as characteristics of IAS;
- the provision that such agreements and commercial practices shall not limit the exercise of the end-users' rights laid down in Article 3(1).

Agreements on commercial and technical conditions and the characteristics of internet access services

32. Agreements refer to contractual relationships between ISPs and end-users that may include, as stated in the Regulation, commercial conditions (such as pricing), technical conditions (such as data volumes and speed) and any characteristics of the IAS. It should be noted that it will often be the case that commercial and technical conditions can be intertwined.

Commercial practices

33. Commercial practices may consist of all relevant aspects of ISPs' commercial behaviour, including unilateral practices, of the ISP.[10]

Shall not limit the exercise of end-users' rights

34. With regard to characteristics of IAS, agreeing on tariffs for specific data volumes and speeds of the IAS would not represent a limitation of the exercise of the end-users' rights (ref. Recital 7). Moreover, BEREC considers that end-users' rights are likely to be unaffected, at least in the case that data volume and speed characteristics are applied in an application-agnostic way (applying equally to all applications).

35. Examples of commercial practices which are likely to be acceptable would include:

- application-agnostic offers where an end-user gets uncapped[11] access to the internet (and not just for certain applications) during a limited period of time, e.g. during night-time or at weekends (when the network is less busy);

[10] NRAs should also consider whether the definition of "commercial practices" in Article 2(d) the Unfair Commercial Practices Directive (UCPD) could also provide guidance in understanding the term, ref. *"any acts, omission, course of conduct or representation, commercial communication, including advertising and marketing, by a trader, directly connected with a promotion, sale or supply of a product"*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:EN:PDF. However, it should also be noted that the goal of the UCPD is different from the goal of Regulation 2015/2120 in as much as the former mainly addresses commercial practices which are directly connected with a promotion, sale or supply of a product (i.e. mainly advertising and marketing) whereas the latter establishes common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights.

[11] i.e. which does not count against a data cap

- the ability for an end-user to access the ISP's customer services when their data cap is reached in order to purchase access to additional data.

36. An ISP may bundle the provision of the IAS with an application. For instance, a mobile operator may offer free subscription to a music streaming application for a period of time to all new subscribers (as opposed to commercial practices such as zero-rating, which is explained in paragraphs 40-43). Where the traffic associated with this application is not subject to any preferential traffic management practice, and is not priced differently than the transmission of the rest of the traffic, such commercial practices are deemed not to limit the exercise of the end-users' rights granted under Article 3(1).

37. When assessing agreements or commercial practices, NRAs should also take Article 3(3) into account given that, typically, infringements of Article 3(3) (e.g. technical practices, such as blocking access to applications or types of applications) will limit the exercise of the end-users' rights, and constitute an infringement of Articles 3(2) and 3(1). Details about this assessment can be found in paragraphs 49-93.

38. If an ISP contractually (as opposed to technically) banned the use of specific content, or one or more applications/services or categories thereof (for example, banning the use of VoIP) this would limit the exercise of the end-user rights set out in Article 3(1). This would be considered to be an offer of a sub-internet service (see paragraph 17).

39. However, some commercial conditions or practices, most obviously those involving price differentiation applied to categories of applications, are more likely to influence end-users' exercise of the rights defined in Article 3(1) without necessarily limiting it.

40. There is a specific commercial practice called zero-rating. This is where an ISP applies a price of zero to the data traffic associated with a particular application or category of applications (and the data does not count towards any data cap in place on the IAS). There are different types of zero-rating practices which could have different effects on end-users and the open internet, and hence on the end-user rights protected under the Regulation.

41. A zero-rating offer where all applications are blocked (or slowed down) once the data cap is reached except for the zero-rated application(s) would infringe Article 3(3) first (and third) subparagraph (see paragraph 55).

42. The ISP could either apply or offer zero-rating to an entire category of applications (e.g. all video or all music streaming applications) or only to certain applications thereof (e.g. its own services, one specific social media application, the most popular video or music applications). In the latter case, an end-user is not prevented from using other music applications. However, the zero price applied to the data traffic of the zero-rated music application (and the fact that the data traffic of the zero-rated music application does not count towards any data cap in place on the IAS) creates an economic incentive to use that music application instead of competing ones. The effects of such a practice applied to a specific application are more likely to *"undermine the essence of the end-users' rights"* or lead to circumstances where *"end-users' choice is materially reduced in practice"* (Recital 7) than when it is applied to an entire category of applications.

43. When assessing such agreements or commercial practices like zero-rating in relation to Article 3(2), the assessment should take into account the aim of the Regulation to

"safeguard equal and non-discriminatory treatment of traffic" (Article 1) and to "*guarantee the continued functioning of the internet ecosystem as an engine of innovation*" (Recital 1) as well as Recital 7, which directs intervention against agreements or commercial practices which, "*by reason of their scale, lead to situations where end-users' choice is materially reduced in practice*", or which would result in *"the undermining of the essence of the end-users' rights"*.

44. Recital 7 also indicates that the assessment should take into account the *"respective market positions of those providers of internet access services, and of the providers of content, applications and services, that are involved"*.

45. When assessing whether an ISP limits the exercise of rights of end-users, NRAs should consider to what extent end-users' choice is restricted by the agreed commercial and technical conditions or the commercial practices of the ISP. It is not the case that every factor affecting end-users' choices should necessarily be considered to limit the exercise of end-users' rights under Article 3(1). The Regulation also foresees intervention in case such restrictions result in choice being materially reduced, but also in other cases that could qualify as a limitation of the exercise of the end-users' rights under Article 3(1).

46. In light of the aforementioned considerations, BEREC considers that a comprehensive assessment of such commercial and technical conditions may be required, taking into account in particular:

- the goals of the Regulation and whether the relevant agreements and/or commercial practices circumvent these general aims;
- the market positions of the ISPs and CAPs involved - a limitation of the exercise of end-user rights is more likely to arise where an ISP or a CAP has a 'strong' market position (all else being equal) compared to a situation where the ISP or CAP has a 'weak' market position. The market positions should be analysed in line with competition law principles;
- the effects on consumer and business customer end-user rights, which encompasses an assessment of inter alia:
  - whether there is an effect on the range and diversity of content and applications which consumer end-users may use[12] and, if so, whether the range and diversity of applications which end-users can choose from is reduced in practice;
  - whether the end-user is incentivised to use, for example, certain applications;
  - whether the IAS subscription contains characteristics which materially reduce end-user choice (see in more detail in paragraph 48).
- the effects on CAP end-user rights, which encompasses an assessment of, inter alia:

[12] This may also concern the effect on freedom of expression and information, including media pluralism

- whether there is an effect on the range and diversity of content and applications which CAPs provide,[13] and to what extent the range and diversity of applications may not be effectively accessed;
- whether CAPs are materially discouraged from entering the market or forced to leave the market, or whether there are other material harms to competition in the market concerned (see in more detail in the fourth bullet of paragraph 48 with regard to offers);
- whether the continued functioning of the internet ecosystem as an engine of innovation is impacted, for example, whether it is the ISP that picks winners and losers, and on the administrative and/or technical barriers for CAPs to enter into agreements with ISPs.

- the scale of the practice and the presence of alternatives - a practice is more likely to limit the exercise of end-user rights in a situation where, for example, many end-users are concerned and/or there are few alternative offers and/or competing ISPs for the end-users to choose from.

47. Each of these factors may contribute to a material reduction in end-user choice and hence a limitation of the exercise of end-users' rights under Article 3(2). In any specific case, the presence of one or more of these factors may in fact limit the exercise of end-user rights.

48. In applying such a comprehensive assessment, the following considerations may also be taken into account:

- Any agreements or practices which have an effect similar to technical blocking of access (see paragraph 55) are likely to infringe Articles 3(1) and 3(2), given their strong impact on end-user rights.
- Commercial practices which apply a *higher* price to the data associated with a specific application or class of applications are likely to limit the exercise of end-users' rights because of the potentially strong disincentive created to the use of the application(s) affected, and consequent restriction of choice. Also, the possibility that higher prices may be applied to an application or category of application may discourage the development of new applications.
- End-users of an IAS whose conditions include a lower (or zero) price for the data associated with a specific application or class of applications will be incentivised to use the zero-rated application or category of applications and not others. Furthermore, the lower the data cap, the stronger such influence is likely to be.
- Price differentiation between *individual* applications within a category has an impact on competition between providers in that class. It may therefore be more likely to impact the "*continued functioning of the internet ecosystem as an engine of innovation"* and thereby undermine the goals of the Regulation than would price differentiation between *classes* of application.

Article 3(3) first subparagraph

Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the

[13] This may also concern the effect on freedom and pluralism of media

sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.

Recital 8
When providing internet access services, providers of those services should treat all traffic equally, without discrimination, restriction or interference, independently of its sender or receiver, content, application or service, or terminal equipment. According to general principles of Union law and settled case-law, comparable situations should not be treated differently and different situations should not be treated in the same way unless such treatment is objectively justified.

49. A basic principle of the Regulation relates to traffic management and is the obligation on ISPs to treat all traffic equally when providing IAS. Typically, infringements of this principle which are not justified according to Article 3(3) would also constitute an infringement of the end-user rights set out in Article 3(1).

50. As Article 3(3) concerns the equal treatment of all traffic *"when providing internet access service",* the scope of this paragraph excludes IP interconnection practices.

51. In assessing whether an ISP complies with this principle, NRAs should apply a two-step assessment:
    - In a first step, they should assess whether all traffic is treated equally.
    - In a second step, they should assess whether situations are comparable or different and whether there are objective grounds which could justify a different treatment of different situations (under Article 3(3) second subparagraph – see paragraphs 57-75 below).

52. Moreover, NRAs should ensure that traffic on an IAS is managed:

    - *"without discrimination, restriction or interference"*;
    - *"irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used"*.

53. NRAs should take into account that equal treatment does not necessarily imply that all end-users will experience the same network performance or quality of service (QoS). Thus, even though packets can experience varying transmission performance (e.g. on parameters such as latency or jitter), packets can normally be considered to be treated equally as long as all packets are processed agnostic to sender and receiver, to the content accessed or distributed, and to the application or service used or provided.

54. Endpoint-based congestion control[14] (a typical example is Transmission Control Protocol (TCP) congestion control) does not contravene Article 3(3) first subparagraph since, by definition, it takes place within terminal equipment and terminal equipment is not covered by the Regulation.[15] NRAs should consider network-internal mechanisms of ISPs which assist endpoint-based congestion control[16] to be in line with equal treatment, and therefore permissible, as long as these network-internal mechanisms

[14] This should not be confused with network-internal congestion management as described under Article 3(3) (c)). IETF, RFC 5783, Congestion Control in the RFC Series
[15] See details about terminal equipment under Article 3(1)
[16] Active Queue Management, see IETF, RFC 7567

are agnostic to the applications running in the endpoints and a circumvention of the Regulation does not take place.

55. In case of agreements or practices involving technical discrimination, this would constitute unequal treatment which would not be compatible with Article 3(3). This holds in particular for the following examples:

- A practice where an ISP blocks, slows down, restricts, interferes with, degrades or discriminates access to specific content, one or more applications (or categories thereof), except when justified by reference to the exceptions of Article 3(3) third subparagraph.
- IAS offers where access to the internet is restricted to a limited set of applications or endpoints by the end-user's ISP (sub-internet service offers) infringe upon Article 3(3) first subparagraph, as such offers entail blocking of applications and / or discrimination, restriction or interference related to the origin or destination of the information.
- A zero-rating offer where all applications are blocked (or slowed down) once the data cap is reached except for the zero-rated application(s), as it would infringe Article 3(3) first (and third) subparagraph.

56. NRAs should apply a comprehensive assessment of compatibility with the Regulation for all those IAS offers which are not as clear as the examples mentioned in paragraph 55.

Article 3(3) second subparagraph

The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures. In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.

Recital 9
The objective of reasonable traffic management is to contribute to an efficient use of network resources and to an optimisation of overall transmission quality responding to the objectively different technical quality of service requirements of specific categories of traffic, and thus of the content, applications and services transmitted. Reasonable traffic management measures applied by providers of internet access services should be transparent, non-discriminatory and proportionate, and should not be based on commercial considerations. The requirement for traffic management measures to be non-discriminatory does not preclude providers of internet access services from implementing, in order to optimise the overall transmission quality, traffic management measures which differentiate between objectively different categories of traffic. Any such differentiation should, in order to optimise overall quality and user experience, be permitted only on the basis of objectively different technical quality of service requirements (for example, in terms of latency, jitter, packet loss, and bandwidth) of the specific categories of traffic, and not on the basis of commercial considerations. Such differentiating measures should be proportionate in relation to the purpose of overall quality optimisation and should treat equivalent traffic equally. Such measures should not be maintained for longer than necessary.

Recital 10
Reasonable traffic management does not require techniques which monitor the specific content of data traffic transmitted via the internet access service.

Traffic management measures[17]

57. In assessing whether an ISP complies with the principle of equal treatment set out in Article 3(3) first subparagraph, NRAs should take into account whether a measure is a reasonable traffic management measure. The principle of equal treatment of traffic does not prevent ISPs from implementing reasonable traffic management measures in compliance with Article 3(3) second subparagraph.

"Transparent, non-discriminatory and proportionate"

58. In considering whether a traffic management measure is reasonable, NRAs should in a first step assess whether the traffic management measure is transparent, non-discriminatory and proportionate. These terms are legal principles that are already used in everyday regulatory practice when applying EU law and respective national law.

59. Under Article 3(3), NRAs should require ISPs to provide *transparent* information about traffic management practices and the impact of these practices (see also Articles 4 and 5).

60. When considering whether a traffic management measure is non-discriminatory, NRAs should consider the following:

- The requirement for traffic management measures to be non-discriminatory does not preclude ISPs from implementing - in order to optimise the overall transmission quality and user experience - traffic management measures which differentiate between objectively different categories of traffic (ref. Recital 9 and paragraphs 62-67 below);
- Similar situations in terms of similar technical QoS requirements should receive similar treatment;
- Different situations in terms of objectively different technical QoS requirements can be treated in different ways if such treatment is objectively justified;
- In particular, the mere fact that network traffic is encrypted should not be deemed by NRAs to be an objective justification for different treatment by ISPs.

61. When considering whether a traffic management measure is proportionate, NRAs should consider the following:

- There has to be a legitimate aim for this measure, as specified in the first sentence of Recital 9, namely contributing to an efficient use of network resources and to an optimisation of overall transmission quality;
- The traffic management measure has to be suitable to achieve this aim (with a requirement of evidence to show it has that effect and that it is not manifestly inappropriate);
- The traffic management measure has to be necessary to achieve this aim;

[17] A definition of traffic management measures can be found on page 18 of the BEREC 2011 Net Neutrality QoS Framework (BoR (11) 53)

- There is not a less interfering and equally effective alternative way of managing traffic to achieve this aim (e.g. equal treatment without categories of traffic) with the available network resources;
- The traffic management measure has to be appropriate, e.g. to balance the competing requirements of different traffic categories or competing interests of different groups.

"Objectively different technical QoS requirements of traffic categories"

62. In assessing whether a traffic management measure is reasonable, NRAs should assess the justification put forward by the ISP. In order to be considered to be reasonable, a traffic management measure has to be based on objectively different technical QoS requirements of specific categories of traffic. Examples for technical QoS requirements are latency, jitter, packet loss, and bandwidth.

63. Traffic categories should typically be defined based on QoS requirements, whereby a traffic category will contain a flow of packets from applications with similar requirements. Therefore, if ISPs implement different technical QoS requirements of specific categories of traffic, this should be done objectively by basing them on the sensitivity to QoS requirements of the applications (e.g. latency, jitter, packet loss, and bandwidth). For example, such a category may consist of real-time applications requiring a short time delay between sender and receiver.[18]

64. Furthermore, as explained in Recital 9, ISPs' traffic management measures are *"responding to"* the QoS requirements of the categories of traffic in order to optimise the overall transmission quality and enhance the user-experience. In order to identify categories of traffic, the ISP relies on the information provided by the application when packets are sent into the network. (See also paragraph 70 regarding which information can legitimately be considered by ISPs). Encrypted traffic should not be treated less favourably by reason of its encryption.

65. When NRAs consider network-internal mechanisms of ISPs which assist endpoint-based congestion control (see paragraph 54) in the context of Article 3(3) second subparagraph, the queue management of the different traffic categories[19] should be assessed under the same criteria as described in general for Article 3(3) second subparagraph.

66. Based on this, reasonable traffic management may be applied to differentiate between objectively different *"categories of traffic"*, for example by reference to an application layer protocol or generic application types (such as file sharing, VoIP or instant messaging), only in so far as:

    - the application layer protocol or generic application types require objectively different technical QoS;
    - applications with equivalent QoS requirements are handled agnostically in the same traffic category; and
    - justifications are specific to the objectives that are pursued by implementing traffic management measures based on different categories of traffic.

[18] IETF, RFC 7657, Differentiated Services and Real-Time Communication
[19] See section 2.1 "AQM and Multiple Queues" in IETF RFC 7567

67. ISPs may prioritise network management and control traffic over the rest of their traffic. Such traffic management practices should be considered as reasonable, provided that they are transparent and are aimed at properly configuring and securing the network and its equipment by efficiently balancing load, e.g. by reacting as fast as possible in case of congestion, failures, outages, etc.

"Not based on commercial considerations"

68. In the event that traffic management measures are based on commercial grounds, the traffic management measure is not reasonable. An obvious example of this could be where an ISP charges for usage of different traffic categories or where the traffic management measure reflects the commercial interests of an ISP that offers certain applications or partners with a provider of certain applications. However, NRAs do not need to prove that a traffic management measure is based on commercial grounds; it is sufficient to establish that the traffic management measure is not based on objectively different technical QoS requirements.

"Shall not monitor the specific content"

69. In assessing traffic management measures, NRAs should ensure that such measures do not monitor the specific content (i.e. transport layer protocol payload).

70. Conversely, traffic management measures that monitor aspects other than the specific content, i.e. the generic content, should be deemed to be allowed. Monitoring techniques used by ISPs which rely on the information contained in the IP packet header, and transport layer protocol header (e.g. TCP) may be deemed to be generic content, as opposed to the specific content provided by end-users themselves (such as text, pictures and video).

"Shall not be maintained longer than necessary"

71. In assessing traffic management measures, NRAs should take into account that such measures shall not be maintained longer than necessary.

72. BEREC understands this term as relating to the proportionality of reasonable traffic management measures in terms of duration, in parallel to the explicit precondition *"shall be proportionate"* which relates to their proportionality in terms of scope (type and proportion of traffic affected, impact on the rest of traffic, equal treatment of comparable situations etc.).

73. This does not prevent, per se, a trigger function to be implemented and in place (but with the traffic management measure not yet effective) on an ongoing basis inasmuch as the traffic management measure only becomes effective in times of necessity. Necessity can materialise several times, or even regularly, over a given period of time. However, where traffic management measures are in effect on a permanent or recurring basis, their necessity might be questionable and NRAs should, in such scenarios, consider whether the traffic management measures can still be qualified as reasonable within the meaning of Article 3(3) second subparagraph.

Distinction from exceptional traffic management measures

74. Article 3(3) third subparagraph clarifies that, under Article 3(3) second subparagraph, inter alia, the following traffic management measures are prohibited: blocking, slowing

down, alteration, restriction, interference with, degradation, and discrimination between specific content, applications or services, or specific categories thereof.

Distinction from specialised services

75. BEREC understands that *"categories of traffic"* should be clearly distinguished from specialised services. Article 3(5) clarifies that specialised services may be provided for optimisation reasons in order to meet requirements for a specific level of quality. On the other hand, the use of *"categories of traffic"* under Article 3(3) second subparagraph is permitted for the optimisation of the overall transmission quality (ref. Recital 9).

Article 3(3) third subparagraph

Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:

Recital 11
Any traffic management practices which go beyond such reasonable traffic management measures, by blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between specific content, applications or services, or specific categories of content, applications or services, should be prohibited, subject to the justified and defined exceptions laid down in this Regulation. Those exceptions should be subject to strict interpretation and to proportionality requirements. Specific content, applications and services, as well as specific categories thereof, should be protected because of the negative impact on end-user choice and innovation of blocking, or of other restrictive measures not falling within the justified exceptions. Rules against altering content, applications or services refer to a modification of the content of the communication, but do not ban non-discriminatory data compression techniques which reduce the size of a data file without any modification of the content. Such compression enables a more efficient use of scarce resources and serves the end-users' interests by reducing data volumes, increasing speed and enhancing the experience of using the content, applications or services concerned.

Recital 12
Traffic management measures that go beyond such reasonable traffic management measures may only be applied as necessary and for as long as necessary to comply with the three justified exceptions laid down in this Regulation.

76. Article 3(3), third subparagraph contains two aspects:

- a prohibition for ISPs to apply traffic management measures going beyond reasonable traffic management measures; as well as
- an exhaustive list of three exceptions in which traffic management measures that go beyond such reasonable traffic management are permissible.

77. In order to safeguard the open Internet, Article 3(3) third subparagraph describes traffic management practices that are prohibited, unless under specific exception. These are practices that, inter alia, are banned in that regard, and can be described by these seven basic principles which should be used by NRAs when assessing ISPs' practices:

- no blocking;
- no slowing down;

- no alteration;
- no restriction;
- no interference with;
- no degradation; and
- no discrimination

between specific content, applications or services, or specific categories thereof. This is a non-exhaustive list of traffic management measures that are prohibited, and any other measure going beyond reasonable traffic management is also prohibited. Practices not complying with the seven basic principles, or that otherwise go beyond reasonable traffic management, may be used by ISPs only based on the three specific exceptions elaborated below under Article 3(3) (a), (b) and (c).

78. By way of example, ISPs should not block, slow down, alter, restrict, interfere with, degrade or discriminate advertising when providing an IAS, unless the conditions of the exceptions a), b) or c) are met in a specific case. In contrast to network-internal blocking put in place by the ISP, terminal equipment-based restrictions put in place by the end-user are not targeted by the Regulation.

79. The three exceptions set out in Article 3(3) third subparagraph have as common preconditions that the traffic management measure has to be necessary for the achievement of the respective exception (*"except as necessary"*) and that it may be applied *"only for as long as necessary"*. These requirements follow from the principle of proportionality.[20] Moreover, as exceptions, they should be interpreted in a strict manner.[21]

80. The prohibition of monitoring of specific content does not apply to traffic management *going beyond reasonable traffic management* (i.e. traffic management complying with the exceptions in (a), (b), or (c)). It should be noted that, according to Article 3(4), any processing of personal data has to be carried out in line with Directive 95/46/EC and Directive 2002/58/EC.

Article 3(3) (a)

(a) comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers;

Recital 13
First, situations may arise in which providers of internet access services are subject to Union legislative acts, or national legislation that complies with Union law (for example, related to the lawfulness of content, applications or services, or to public safety), including criminal law, requiring, for example, blocking of specific content, applications or services. In addition, situations may arise in which those providers are subject to measures that comply with Union law, implementing or applying Union legislative acts or national legislation, such as measures of general application, court orders, decisions of public authorities vested with relevant powers, or other measures ensuring compliance

[20] See Recital 11
[21] See Recital 11

with such Union legislative acts or national legislation (for example, obligations to comply with court orders or orders by public authorities requiring to block unlawful content). The requirement to comply with Union law relates, inter alia, to the compliance with the requirements of the Charter of Fundamental Rights of the European Union ('the Charter') in relation to limitations on the exercise of fundamental rights and freedoms. As provided in Directive 2002/21/EC of the European Parliament and of the Council (1), any measures liable to restrict those fundamental rights or freedoms are only to be imposed if they are appropriate, proportionate and necessary within a democratic society, and if their implementation is subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms, including its provisions on effective judicial protection and due process.

81. If an ISP applies traffic management measures which cannot be regarded as reasonable, NRAs should assess whether an ISP does so because it has to do so for legal reasons, namely to comply with the legislation or measures by public authorities specified in that exception.

82. As explained in Recital 13, such legislation or measures must comply with the requirements of the Charter of Fundamental Rights, and notably Article 52 which states in particular that any limitation of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms.

Article 3(3) (b)

(b) preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users;

Recital 14
Second, traffic management measures going beyond such reasonable traffic management measures might be necessary to protect the integrity and security of the network, for example by preventing cyber-attacks that occur through the spread of malicious software or identity theft of end-users that occurs as a result of spyware.

83. Typical attacks and threats that will trigger integrity and security measures include:

- flooding network components or terminal equipment with traffic to destabilise them (e.g. Denial of Service attack);
- spoofing IP addresses in order to mimic network devices or allow for unauthorised communication;
- hacking attacks against network components or terminal equipment;
- distribution of malicious software, viruses etc.

84. Conducting traffic management measures in order to preserve integrity and security of the network could basically consist of restricting connectivity or blocking of traffic to and from specific endpoints. Typical examples of such traffic management measures include:

- blocking of IP addresses, or ranges of them, because they are well-known sources of attacks;
- blocking of IP addresses from which an actual attack is originating;
- blocking of IP addresses/IAS showing suspicious behaviour (e.g. unauthorised communication with network components, address spoofing);

- blocking of IP addresses where there are clear indications that they are part of a bot network;
- blocking of specific port numbers which constitute a threat to security and integrity.

85. NRAs should consider that, in order to identify attacks and activate security measures, the use of security monitoring systems by ISPs is often justified. In such cases, the monitoring of traffic to detect security threats (such as those listed in paragraph 84) may be implemented in the background on a continuous basis,[22] while the actual traffic management measure preserving integrity and security is triggered only when concrete security threats are detected. Therefore, the precondition *"only for as long as necessary"* does not preclude implementation of such monitoring of the integrity and security of the network.

86. Besides monitoring the integrity and security of the network, possible security threats may also be identified on the basis of reports/complaints from end-users or blocking lists from recognised security organisations.

87. This exception could be used as a basis for circumvention of the Regulation because security is a broad concept. NRAs should therefore carefully assess whether the requirements of this exception are met and to request that ISPs provide adequate justifications[23] when necessary.

Article 3(3) (c)

(c) prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

Recital 15
Third, measures going beyond such reasonable traffic management measures might also be necessary to prevent impending network congestion, that is, situations where congestion is about to materialise, and to mitigate the effects of network congestion, where such congestion occurs only temporarily or in exceptional circumstances. The principle of proportionality requires that traffic management measures based on that exception treat equivalent categories of traffic equally. Temporary congestion should be understood as referring to specific situations of short duration, where a sudden increase in the number of users in addition to the regular users, or a sudden increase in demand for specific content, applications or services, may overflow the transmission capacity of some elements of the network and make the rest of the network less reactive. Temporary congestion might occur especially in mobile networks, which are subject to more variable conditions, such as physical obstructions, lower indoor coverage, or a variable number of active users with changing location. While it may be predictable that such temporary congestion might occur from time to time at certain points in the network – such that it cannot be regarded as exceptional – it might not recur so often or for such extensive periods that a capacity expansion would be economically justified. Exceptional congestion should be understood as referring to unpredictable and unavoidable situations of congestion, both in mobile and fixed networks. Possible causes of those situations include a

[22] Such monitoring should be subject to strict interpretation and to proportionality requirements, and should be assessed by NRAs in line with paragraph 87.

[23] Such justifications should also be in line with Articles 13(a) and 13(b) of the Framework Directive

technical failure such as a service outage due to broken cables or other infrastructure elements, unexpected changes in routing of traffic or large increases in network traffic due to emergency or other situations beyond the control of providers of internet access services. Such congestion problems are likely to be infrequent but may be severe, and are not necessarily of short duration. The need to apply traffic management measures going beyond the reasonable traffic management measures in order to prevent or mitigate the effects of temporary or exceptional network congestion should not give providers of internet access services the possibility to circumvent the general prohibition on blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between specific content, applications or services, or specific categories thereof. Recurrent and more long-lasting network congestion which is neither exceptional nor temporary should not benefit from that exception but should rather be tackled through expansion of network capacity.

88. In exceptional cases, and for no longer than necessary, ISPs may engage in traffic management beyond the limits of Article 3(3) second subparagraph to manage certain types of network congestion, namely impending network congestions (which may be prevented) and exceptional or temporary network congestions (the effects of which may be mitigated). Recital 15 provides detailed information on identifying situations where exceptional and temporary congestion occurs. Impending network congestion is defined as situations where congestion is about to materialise, i.e. it is imminent.

89. Recital 15 focuses on exceptional and temporary network congestion; thus, actions for preventing impending network congestion only apply to cases of such congestion.

90. When assessing congestion management exceptions under (c), NRAs should refer to the general criteria of strict interpretation and proportionality set out in Article 3(3) third subparagraph. Furthermore, NRAs should check that congestion management is not used to circumvent the ban on blocking, throttling and discrimination (ref. Recital 15).

91. Due to the requirement that exceptional traffic management can only be applied as necessary, and only for as long as necessary, NRAs should consider that in cases when application-agnostic congestion management (i.e. congestion management which is not targeting specific applications or categories thereof) is not sufficient, congestion can be dealt with according to Article 3(3) (c). Furthermore, in such cases, equivalent categories of traffic must be treated equally. Any throttling action should be limited to the section of the network where congestion occurs, if feasible.

92. Congestion management can be done on a general basis, independent of applications.[24] NRAs should consider whether such types of congestion management would be sufficient and equally effective to manage congestion, in light of the principle of proportionality. For the same reason, NRAs should consider whether *throttling* of traffic, as opposed to *blocking* of traffic, would be sufficient and equally effective to manage congestion.

93. As part of their scrutiny of congestion management practices, NRAs may monitor that ISPs properly dimension their network, and take into account the following:

    - if there is recurrent and more long-lasting network congestion in an ISP's network, the ISP cannot invoke the exception of congestion management (ref. Recital 15);

[24] IETF, RFC 6057, Comcast's Protocol-Agnostic Congestion Management and IETF, RFC 6789, Congestion Exposure (Conex) Concepts and Use Cases

- application-specific congestion management should not be applied or accepted as a substitute for more structural solutions, such as expansion of network capacity.

Article 3(4)

Any traffic management measure may entail processing of personal data only if such processing is necessary and proportionate to achieve the objectives set out in paragraph 3. Such processing shall be carried out in accordance with Directive 95/46/EC of the European Parliament and of the Council. Traffic management measures shall also comply with Directive 2002/58/EC of the European Parliament and of the Council.

94. In the course of traffic management, personal data may be processed. Article 3(4) provides that such measures may only process personal data if certain requirements are met, and only under certain conditions.

95. Article 3(3) distinguishes between reasonable traffic management measures and traffic management measures going beyond reasonable traffic management measures. Article 3(4) applies to both of these traffic management forms *("any traffic management measure"*). With regard to reasonable traffic management measures, these requirements are further specified by Article 3(3) second subparagraph which states that *"such measures shall not monitor the specific content"*.

96. The objectives referred to in Article 3(4) are those set out in Article 3(3).

"Necessary and proportionate"

97. The processing of personal data within the course of traffic management is also subject to the proportionality requirement. NRAs should assess whether the processing of personal data undertaken by ISPs is necessary and proportionate to achieve the objectives set out in Article 3(3).

"Compliance with Union law on data protection"

98. The competent national authority should assess whether the processing of personal data complies with Union law on data protection.[25]

Article 3(5) first subparagraph

Providers of electronic communications to the public, including providers of internet access services, and providers of content, applications and services shall be free to offer services other than internet access services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality.

[25] Whereas NRAs are not competent to enforce the Privacy Directive (Directive 95/46/EC as amended by Regulation (EC) 1882/2003 (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l14012&from=EN), they are in many countries empowered to enforce the ePrivacy Directive (Directive 2002/58/EC, as amended by Directive 2006/24/EC and Directive 2009/136/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF)

Recital 16
There is demand on the part of providers of content, applications and services to be able to provide electronic communication services other than internet access services, for which specific levels of quality, that are not assured by internet access services, are necessary. Such specific levels of quality are, for instance, required by some services responding to a public interest or by some new machine-to-machine communications services. Providers of electronic communications to the public, including providers of internet access services, and providers of content, applications and services should therefore be free to offer services which are not internet access services and which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet the requirements of the content, applications or services for a specific level of quality. National regulatory authorities should verify whether and to what extent such optimisation is objectively necessary to ensure one or more specific and key features of the content, applications or services and to enable a corresponding quality assurance to be given to end-users, rather than simply granting general priority over comparable content, applications or services available via the internet access service and thereby circumventing the provisions regarding traffic management measures applicable to the internet access services.

99. Beyond the delivery of applications through the IAS, there can be demand for services that need to be carried at a specific level of quality that cannot be assured by the standard best effort delivery.

100. Such services can be offered by providers of electronic communications to the public (PECPs), including providers of internet access services (ISPs), and providers of content, applications and services (CAPs).

101. These providers are free to offer services referred to in Article 3(5), which BEREC refers to as specialised services[26], only when various requirements are met. Article 3(5) provides the safeguards for the provisioning of specialised services which are characterised by the following features in Article 3 (5) first subparagraph:

- they are services other than IAS services;
- they are optimised for specific content, applications or services, or a combination thereof;
- the optimisation is objectively necessary in order to meet requirements for a specific level of quality.

102. Their provision is subject to a number of conditions in Article 3(5) second subparagraph, namely that:

- the network capacity is sufficient to provide the specialised service in addition to any IAS provided;
- specialised services are not usable or offered as a replacement for IAS;
- specialised services are not to the detriment of the availability or general quality of the IAS for end-users.

103. According to Recital 16, the service shall not be used to circumvent the provisions regarding traffic management measures applicable to IAS.

104. All these safeguards aim to ensure the continued availability and general quality of best effort IAS.

[26] Network-slicing in 5G networks may be used to deliver specialised services

105. NRAs should verify whether the application could be provided over IAS at the specific levels of quality which are objectively necessary in relation to the application, or whether they are instead set up in order to circumvent the provisions regarding traffic management measures applicable to IAS, which would not be allowed.

Assessment according to Article 3(5) first subparagraph

106. Initially, the requirement of an application can be specified by the provider of the specialised service, although requirements may also be inherent to the application itself. For example, a video application could use standard definition with a low bitrate or ultra-high definition with high bitrate, and these will obviously have different QoS requirements. A typical example of inherent requirements is low latency for real-time applications.

107. When assessing whether the practices used to provide specialised services comply with Article 3(5) first subparagraph, NRAs should apply the approach set out in paragraphs 108-115).

108. NRAs could request from the provider relevant information about their specialised services, using powers conferred by Article 5(2). In their responses, the provider should give information about their specialised services, including what the relevant QoS requirements are (e.g. latency, jitter and packet loss), and any contractual requirements. Furthermore, the "*specific level of quality*" should be specified, and it should be demonstrated that this specific level of quality cannot be assured over the IAS and that the QoS requirements are objectively necessary to ensure one or more key features of the application.

109. Based on this information, the NRA should assess the requirements mentioned in Article 3(5) first subparagraph.

110. If assurance of a specific level of quality is objectively necessary, this cannot be provided by simply granting general priority over comparable content.[27] Specialised services do not provide connectivity to the internet and they can be offered, for example, through a connection that is logically separated from the traffic of the IAS in order to assure these levels of quality.

111. NRAs should verify whether, and to what extent, optimised delivery is objectively necessary to ensure one or more specific and key features of the applications, and to enable a corresponding quality assurance to be given to end-users. To do this, the NRA should assess whether an electronic communication service, other than IAS, requires a level of quality that cannot be assured over a IAS. If not, these electronic communication services are likely to circumvent the provisions of the Regulation and are therefore not allowed.

112. The internet and the nature of IAS will evolve over time. A service that is deemed to be a specialised service today may not necessarily qualify as a specialised service in the

[27] As explained in Recital 16, NRAs *"should verify whether and to what extent such optimisation is objectively necessary to ensure one or more specific and key features of the content, applications or services and to enable a corresponding quality assurance to be given to end-users, rather than simply granting general priority over comparable content, applications or services available via the internet access service and thereby circumventing the provisions regarding traffic management measures applicable to the internet access services"*

future due to the fact that the optimisation of the service may not be objectively necessary, as the general standard of IAS may have improved. On the other hand, additional services might emerge that need to be optimised, even as the standard of IAS improves. Given that we do not know what specialised services may emerge in the future, NRAs should assess whether a service qualifies as a specialised service on a case-by-case basis.

113. Typical examples of specialised services provided to end-users are VoLTE and linear broadcasting IPTV services with specific QoS requirements, subject to them meeting the requirements of the Regulation, in particular Article 3(5) first subparagraph. Under the same preconditions, other examples would include real-time health services (e.g. remote surgery) or *"some services responding to a public interest or by some new machine-to-machine communications services"* (Recital 16).

114. QoS might be especially important to corporate customers and these customers might be in need of specialised services which – as they are addressing businesses – are often referred to as "business services". Such "business services" cover a wide array of services and have to be assessed on a case-by-case basis.

115. VPNs could qualify as specialised services in accordance with Article 3(5) of the Regulation. However, in accordance with Recital 17, to the extent that corporate services such as VPNs also provide access to the internet, the provision of such access to the internet by a provider of electronic communications to the public should comply with Article 3(1) to (4) of the Regulation.

Article 3(5) second subparagraph

Providers of electronic communications to the public, including providers of internet access services, may offer or facilitate such services only if the network capacity is sufficient to provide them in addition to any internet access services provided. Such services shall not be usable or offered as a replacement for internet access services, and shall not be to the detriment of the availability or general quality of internet access services for end-users.

Recital 17
In order to avoid the provision of such other services having a negative impact on the availability or general quality of internet access services for end-users, sufficient capacity needs to be ensured. Providers of electronic communications to the public, including providers of internet access services, should, therefore, offer such other services, or conclude corresponding agreements with providers of content, applications or services facilitating such other services, only if the network capacity is sufficient for their provision in addition to any internet access services provided. The provisions of this Regulation on the safeguarding of open internet access should not be circumvented by means of other services usable or offered as a replacement for internet access services. However, the mere fact that corporate services such as virtual private networks might also give access to the internet should not result in them being considered to be a replacement of the internet access services, provided that the provision of such access to the internet by a provider of electronic communications to the public complies with Article 3(1) to (4) of this Regulation, and therefore cannot be considered to be a circumvention of those provisions. The provision of such services other than internet access services should not be to the detriment of the availability and general quality of internet access services for end-users. In mobile networks, traffic volumes in a given radio cell are more difficult to anticipate due to the varying number of active end-users, and for this reason an impact on the quality of internet access services for end-users might occur in unforeseeable circumstances. In mobile

networks, the general quality of internet access services for end-users should not be deemed to incur a detriment where the aggregate negative impact of services other than internet access services is unavoidable, minimal and limited to a short duration. National regulatory authorities should ensure that providers of electronic communications to the public comply with that requirement. In this respect, national regulatory authorities should assess the impact on the availability and general quality of internet access services by analysing, inter alia, quality of service parameters (such as latency, jitter, packet loss), the levels and effects of congestion in the network, actual versus advertised speeds, the performance of internet access services as compared with services other than internet access services, and quality as perceived by end-users.

Sufficient network capacity for specialised services in addition to IAS

116. Specialised services shall only be offered when the network capacity is sufficient such that the IAS is not degraded (e.g. due to increased latency or jitter or lack of bandwidth) by the addition of specialised services. Both in the short and in the long term, specialised services shall not lead to a deterioration of the general IAS quality for end-users. This can, for example, be achieved by additional investments in infrastructure which allow for additional capacity so that there is no negative impact on IAS quality.

117. In a network with limited capacity, IAS and specialised services could compete for overall network resources. In order to safeguard the availability of general quality of IAS, the Regulation does not allow specialised services if the network capacity is not sufficient to provide them in addition to any IAS provided, because this would lead to degradation of the IAS and thereby circumvent the Regulation. It is the general quality of the IAS which is protected from degradation by the Regulation, rather than specialised services.

118. NRAs should assess whether, in order to ensure the quality of specialised services, ISPs have ensured sufficient network capacity for both any IAS offers provided over the infrastructure and for specialised services. If not, provision of specialised services would not be allowed under the Regulation.

119. NRAs could request information from ISPs regarding how sufficient capacity is ensured, and at which scale the service is offered (e.g. networks, coverage and end-users). NRAs could then assess how ISPs have estimated the additional capacity required for their specialised services and how they have ensured that network elements and connections have sufficient capacity available to provide specialised services in addition to any IAS provided.

120. NRAs should assess whether or not there is sufficient capacity for IAS when specialised services are provided, for example, by performing measurements of IAS.[28] Methodologies for such measurements have been relatively well developed during BEREC's Net Neutrality QoS workstreams in recent years and will continue to be improved.

"Not to the detriment of the availability or general quality of IAS"

121. Specialised services are not permissible if they are to the detriment of the availability and general quality of the IAS. There is a correlation between the performance of the IAS offer (i.e. its availability and general quality) and whether there is sufficient capacity

[28] See paragraphs 174-176

to provide specialised services in addition to IAS. IAS quality measurements could be performed with and without specialised services, both in the short term for individual end-users (measuring with specialised services on and off respectively) and in the long term (which would include measurements before the specialised services are introduced in the market as well as after). As Recital 17 clarifies, NRAs should *"assess the impact on the availability and general quality of IAS by analysing, inter alia, QoS parameters (such as latency, jitter and packet loss), the levels and effects of congestion in the network, actual versus advertised speeds and the performance of IAS as compared with services other than IAS"*.

122. While IAS and specialised services directly compete for the dedicated part of an end-user's capacity, the end-user himself may determine how to use it. When it is technically impossible to provide the specialised service in parallel to IAS without detriment to the end-user's IAS quality, NRAs should not consider this competition for capacity to be an infringement of Article 3(5) second subparagraph, as long as the end-user is informed pursuant to Article 4(1)(c) of the impact on his IAS and can obtain the contractually-agreed speeds[29] for any IAS subscribed to in parallel. NRAs should not consider it to be to the detriment of the general quality of IAS when activation of the specialised service by the individual end-user only affects his own IAS. However, detrimental effects should not occur in those parts of the network where capacity is shared between different end-users.

123. Furthermore, as stated in Recital 17, in mobile networks - where the number of active users in a given cell, and consequently traffic volumes, are more difficult to anticipate than in fixed networks - the general quality of IAS for end-users should not be deemed to incur a detriment where the aggregate negative impact of specialised services is unavoidable, minimal and limited to a short duration. By contrast, such unforeseeable circumstances related to the number of users and traffic volumes should not normally occur in fixed networks.

124. NRAs could assess whether the provision of specialised services reduces general IAS quality by lowering measured download or upload speeds or, for example, by increasing delay, delay variation or packet loss. Normal small-scale temporal network fluctuation should not be considered to be to the detriment of the general quality. Network outages and other temporary problems caused by network faults, for example, should be treated separately.

125. NRAs should intervene if persistent decreases in performance are detected for IAS. This could be detected if the measured performance is consistently above (for metrics such as latency, jitter or packet loss) or below (for metrics such as speed) a previously detected average level for a relatively long period of time such as hours or days), or if the difference between measurement results before and after the specialised service is introduced is statistically significant. In the case of short-term assessments, the difference between measurement results with and without the specialised service should be assessed similarly.

[29] As discussed in Article 4(1)(d)

"Not be usable or offered as a replacement for IAS"

126. It is of utmost importance that the provisions regarding specialised services do not serve as a potential circumvention of the Regulation. Therefore, NRAs should assess whether a specialised service is a potential substitute for the IAS, and if the capacity needed for their provision is to the detriment of the capacity available for IAS.

127. In deciding whether a specialised service is considered as a replacement for an IAS, one important aspect that NRAs should assess is whether the service is actually providing access to the internet but in a restricted way, at a higher quality, or with differentiated traffic management. If so, this would be considered a circumvention of the Regulation.

Article 4
Transparency measures for ensuring open internet access

Article 4(1)

Providers of internet access services shall ensure that any contract which includes internet access services specifies at least the following:

[…letters (a) – (b) – (c) – (d) – (e)…]

Providers of internet access services shall publish the information referred to in the first subparagraph.

Recital 18

The provisions on safeguarding of open internet access should be complemented by effective end-user provisions which address issues particularly linked to internet access services and enable end-users to make informed choices. Those provisions should apply in addition to the applicable provisions of Directive 2002/22/EC of the European Parliament and of the Council (1) and Member States should have the possibility to maintain or adopt more far- reaching measures. Providers of internet access services should inform end-users in a clear manner how traffic management practices deployed might have an impact on the quality of internet access services, end-users' privacy and the protection of personal data as well as about the possible impact of services other than internet access services to which they subscribe, on the quality and availability of their respective internet access services. In order to empower end-users in such situations, providers of internet access services should therefore inform end-users in the contract of the speed which they are able realistically to deliver. The normally available speed is understood to be the speed that an end-user could expect to receive most of the time when accessing the service. Providers of internet access services should also inform consumers of available remedies in accordance with national law in the event of non-compliance of performance. Any significant and continuous or regularly recurring difference, where established by a monitoring mechanism certified by the national regulatory authority, between the actual performance of the service and the performance indicated in the contract should be deemed to constitute non- conformity of performance for the purposes of determining the remedies available to the consumer in accordance with national law. The methodology should be established in the guidelines of the Body of European Regulators for Electronic Communications (BEREC) and reviewed and updated as necessary to reflect technology and infrastructure evolution. National regulatory authorities should enforce compliance with the rules in this Regulation on transparency measures for ensuring open internet access.

128. NRAs should ensure that ISPs include relevant information referred to in Article 4(1) (a) to (e) in a clear, comprehensible and comprehensive manner in contracts that include IAS, and publish that information, for example on an ISP's website.

129. NRAs should also note that the transparency requirements laid down in Articles 4(1) and 4(2) are in addition to the measures provided in directive 2002/22/EC (the Universal Service Directive), particularly in Chapter IV thereof. National law may also lay down additional monitoring, information and transparency requirements, including those concerning the content, form and manner of the information to be published.

130. NRAs should look to ensure that ISPs adhere to the following practices in order to ensure that information is clear and comprehensible:

- it should be easily accessible and identifiable for what it is;
- it should be accurate and up to date;
- it should be meaningful to end-users, i.e. relevant, unambiguous and presented in a useful manner;
- it should not create an incorrect perception of the service provided to the end-user;
- it should be comparable at least between different offers, but preferably also between different ISPs, so that end-users are able to compare the offers (including the contractual terms used by different ISPs) and ISPs in such a way that the comparison can show differences and similarities.

131. NRAs should ensure that ISPs include in the contract and publish the information referred to in Article 4(1) (a) to (e). This could be presented in two parts (levels of detail):[30]

- The first part should provide high-level (general) information. The information about the IAS provided should include, for example, an explanation of speeds, examples of popular applications that can be used with a sufficient quality, and an explanation of how such applications are influenced by the limitations of the provided IAS. This part should include reference to the second part where the information required by Article 4(1) of the Regulation is provided in more detail.
- The second part would consist of more detailed technical parameters and their values and other relevant information required by Article 4(1) of the Regulation and in these Guidelines.

132. Examples of how information could be disclosed in a transparent way can be found in BEREC's 2011 Net Neutrality Transparency Guidelines.[31]

133. Contract terms that would inappropriately exclude or limit the exercise of the legal rights of the end-user vis-à-vis the ISP in the event of total or partial non-performance or

[30] NRAs should note that ISPs are also under an obligation to provide information to consumers before being bound by the contract under other EU instruments: the Consumer Rights Directive (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1), the Unfair Commercial Practices Directive (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:EN:PDF) and the e-Commerce Directive (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN)

[31] BEREC Guidelines on Transparency in the scope of Net Neutrality, BoR (11) 67), http://berec.europa.eu/doc/berec/bor/bor11_67_transparencyguide.pdf

inadequate performance by the ISP of any of the contractual obligations might be deemed unfair under national legislation, including the implementation of Directive 93/13/EEC on unfair terms in consumer contracts.[32]

134. Articles 4(1), 4(2) and 4(3) apply to all contracts regardless of the date the contract is concluded or renewed. Article 4(4) applies only to contracts concluded or renewed from 29 November 2015. Modifications to contracts are subject to national legislation implementing Article 20(2) of the Universal Service Directive.

Article 4(1) (a)

(a) information on how traffic management measures applied by that provider could impact on the quality of the internet access services, on the privacy of end-users and on the protection of their personal data;

135. NRAs should ensure that ISPs include in the contract and publish a clear and comprehensive explanation of traffic management measures applied in accordance with the second and third subparagraphs of Article 3(3), including the following information:

- how the measures might affect the end-user experience in general and with regard to specific applications (e.g. where specific categories of traffic are treated differently in accordance with Article 3). Practical examples should be used for this purpose;
- the circumstances and manner under which traffic management measures possibly having an impact as foreseen in Article 4(1) (a) are applied;[33]
- any measures applied when managing traffic which uses personal data, the types of personal data used, and how ISPs ensure the privacy of end-users and protect their personal data when managing traffic.

136. The information should be clear and comprehensive. The information should not simply consist of a general condition stating possible impacts of traffic management measures that could be applied in accordance with the Regulation. Information should also include, at least, a description of the possible impacts of traffic management practices which are in place on the IAS.

Article 4(1) (b)

(b) a clear and comprehensible explanation as to how any volume limitation, speed and other quality of service parameters may in practice have an impact on internet access services, and in particular on the use of content, applications and services;

[32] See Annex, paragraph 1(b) of Council Directive 93/13/EEC on unfair terms in consumer contracts, (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:en:HTML). NRAs may or may not be empowered to monitor compliance with said directive.

[33] The Universal Service Directive (Directive 2002/22/EC, Article 20(1)(b) 2nd and 4th indents) may also require such information to be specified in contracts. Article 20(1)(b) 2nd indent requires that contracts specify information on conditions limiting access to and/or use of services and applications, where such conditions are permitted under national law in accordance with Community law

137. Besides speed, the most important QoS parameters are delay, delay variation (jitter) and packet loss. These other QoS parameters should be described if they might, in practice, have an impact on the IAS and use of applications. NRAs should ensure that ISPs provide end-users with information which is effects-based. End-users should be able to understand the implications of these parameters to the usage of applications and whether certain applications (e.g. interactive speech/video or 4K video streaming) cannot in fact be used due to the long delay or slow speed of the IAS. Categories of applications or popular examples of these affected applications could be provided.

138. Regarding volume limitations, contracts should specify the 'size' of the cap (in quantitative terms, e.g. GB), what that means in practice and the consequences of exceeding it (e.g. additional charges, speed restrictions, blocking of all traffic etc.). If the speed will decrease after a data cap has been reached, that should be taken into account when specifying speeds in a contract and publishing the information. Information and examples could also be provided about what kind of data usage would lead to a situation where the data cap is reached (e.g. indicative amount of time using popular applications, such as SD video, HD video and music streaming).

Article 4(1) (c)

(c) a clear and comprehensible explanation of how any services referred to in Article 3(5) to which the end-user subscribes might in practice have an impact on the internet access services provided to that end-user;

139. NRAs should ensure that ISPs include in the contract and publish clear and comprehensible information about how specialised services included in the end-user's subscription might impact the IAS. This is further discussed in paragraph 122.

Article 4(1) (d)

(d) a clear and comprehensible explanation of the minimum, normally available, maximum and advertised download and upload speed of the internet access services in the case of fixed networks, or of the estimated maximum and advertised download and upload speed of the internet access services in the case of mobile networks, and how significant deviations from the respective advertised download and upload speeds could impact the exercise of the end-users' rights laid down in Article 3(1);

140. In order to empower end-users, speed values required by the Article 4(1) (d) should be specified in the contract and published in such a manner that they can be verified and used to determine any discrepancy between the actual performance and what has been agreed in contract. Upload and download speeds should be provided as single numerical values in bits/second (e.g. kbit/s or Mbit/s). Speeds should be specified on the basis of the IP packet payload or transport layer protocol payload, and not based on a lower layer protocol.

141. In order for the contractual speed values to be understandable, contracts should specify factors that may have an effect on the speed, both within and outside the ISP's control.

142. BEREC understands that the requirement on ISPs to include in the contract and publish information about *advertised speeds* does not entail a requirement to advertise speeds; rather, it is limited to including in the contract and publishing information about speeds

which are advertised by the ISP. The requirement to specify the advertised speed requires an ISP to explain the advertised speed of the particular IAS offer included in the contract, if its speed has been advertised. An ISP may naturally also advertise other IAS offers of higher or lower speeds that are not included in the contract to which the subscriber is party (whether by choice or due to unavailability of the service at their location), in accordance with laws governing marketing.

Specifying speeds for an IAS in case of fixed networks

Minimum speed

143. The minimum speed is the lowest speed that the ISP undertakes to deliver to the end-user, according to the contract which includes the IAS. In principle, the actual speed should not be lower than the minimum speed, except in cases of interruption of the IAS. If the actual speed of an IAS is significantly, and continuously or regularly, lower than the minimum speed, it would indicate non-conformity of performance regarding the agreed minimum speed.

144. NRAs[34] could set requirements on defining minimum speed under Article 5(1), for example that the minimum speed could be in reasonable proportion to the maximum speed.

Maximum speed

145. The maximum speed is the speed that an end-user could expect to receive at least some of the time (e.g. at least once a day). An ISP is not required to technically limit the speed to the maximum speed defined in the contract.

146. NRAs could set requirements on defining maximum speeds under Article 5(1), for example that they are achievable a specified number of times during a specified period.

Normally available speed

147. The normally available speed is the speed that an end-user could expect to receive most of the time when accessing the service. BEREC considers that the normally available speed has two dimensions: the numerical value of the speed and the availability (as a percentage) of the speed during a specified period, such as peak hours or the whole day.

148. The normally available speed should be available during the specified daily period. NRAs could set requirements on defining normally available speeds under Article 5(1). Examples include:

- specifying that normally available speeds should be available at least during off-peak hours and 90% of time over peak hours, or 95% over the whole day;
- requiring that the normally available speed should be in reasonable proportion to the maximum speed.

[34] National regulatory authority as referred to in Article 2(g) of the Framework Directive means the body or bodies charged by national law with any of the regulatory tasks assigned in the framework for electronic communications

149. In order to be meaningful, it should be possible for the end-user to evaluate the value of the normally available speed vis-à-vis the actual performance of the IAS on the basis of the information provided.

Advertised speed

150. Advertised speed is the speed an ISP uses in its commercial communications, including advertising and marketing, in connection with the promotion of IAS offers. In the event that speeds are included in an ISP's marketing of an offer (see also paragraph 142), the advertised speed should be specified in the published information and in the contract for each IAS offer.

151. NRAs could set requirements in accordance with Article 5(1) on how speeds defined in the contract relate to advertised speeds, for example that the advertised speed should not exceed the maximum speed defined in the contract.

Specifying speeds of an IAS in mobile networks

152. Estimated maximum and advertised download and upload speeds should be described in contracts according to paragraphs 153-157.

Estimated maximum speed

153. The estimated maximum speed for a mobile IAS should be specified so that the end-user can understand the realistically achievable maximum speed for their subscription in different locations in realistic usage conditions. The estimated maximum speed could be specified separately for different network technologies that affect the maximum speed available for an end-user. End-users should be able to understand that they may not be able to reach the maximum speed if their mobile terminal does not support the speed.

154. NRAs could set requirements on defining estimated maximum speeds under Article 5(1).

155. Estimated maximum download and upload speeds could be made available in a geographical manner providing mobile IAS coverage maps with estimated/measured speed values of network coverage in all locations.

Advertised speed

156. The advertised speed for a mobile IAS offer should reflect the speed which the ISP is realistically able to deliver to end-users. Although the transparency requirements regarding IAS speed are less detailed for mobile IAS than for fixed IAS, the advertised speed should enable end-users to make informed choices, for example, so they are able to evaluate the value of the advertised speed vis-à-vis the actual performance of the IAS. Significant factors that limit the speeds achieved by end-users should be specified.

157. NRAs could set requirements in accordance with Article 5(1) on how speeds defined in the contract relate to advertised speeds, for example that the advertised speed for an IAS as specified in a contract should not exceed the estimated maximum speed as defined in the same contract. See also paragraph 142.

Article 4(1) (e)

(e) a clear and comprehensible explanation of the remedies available to the consumer in accordance with national law in the event of any continuous or regularly recurring discrepancy between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated in accordance with points (a) to (d).

158. Remedies available to consumers as described in Article 4(1) (e) are defined in national law. Examples of possible remedies for a discrepancy are price reduction, early termination of the contract, damages, or rectification of the non-conformity of performance, or a combination thereof. NRAs should ensure that ISPs provide consumers with information specifying such remedies.

Article 4(2)

Providers of internet access services shall put in place transparent, simple and efficient procedures to address complaints of end-users relating to the rights and obligations laid down in Article 3 and paragraph 1 of this Article.

159. NRAs should ensure that ISPs adhere to certain good practices regarding procedures for addressing complaints, such as:

- informing end-users in the contract as well as on their website, in a clear manner, about the procedures put in place, including the usual or maximum time it takes to handle a complaint;
- providing a description of how the complaint will be handled, including what steps the ISP will take to investigate the complaint and how the end-user will be notified of the progress or resolution of the complaint;
- enabling end-users to easily file a complaint using different means, at least online (e.g. a web-form or email) and at the point of sale, but possibly also using other means such as post or telephone;
- providing a single point of contact for all complaints related to the provisions set out in Article 3 and Article 4(1), regardless of the topic of the complaint;
- enabling an end-user to be able to enquire about the status of their complaint in the same manner in which the complaint was raised;
- informing end-users of the result of the complaint in a relatively short time, taking into account the complexity of the issue;
- informing the end-user of the means to settle unresolved disputes according to national law if the end-user believes a complaint has not been successfully handled by the ISP (depending upon the cause of the complaint, the competent authority or authorities under national law may be the NRA, a court or an alternative dispute resolution entity etc.).

Article 4(3)

The requirements laid down in paragraphs 1 and 2 are in addition to those provided for in Directive 2002/22/EC and shall not prevent Member States from maintaining or introducing additional monitoring, information and transparency requirements, including those

concerning the content, form and manner of the information to be published. Those requirements shall comply with this Regulation and the relevant provisions of Directives 2002/21/EC and 2002/22/EC.

160. This provision is aimed at Member States and no guidance to NRAs is required.

Article 4(4)

Any significant discrepancy, continuous or regularly recurring, between the actual performance of the internet access service regarding speed or other quality of service parameters and the performance indicated by the provider of internet access services in accordance with points (a) to (d) of paragraph 1 shall, where the relevant facts are established by a monitoring mechanism certified by the national regulatory authority, be deemed to constitute non-conformity of performance for the purposes of triggering the remedies available to the consumer in accordance with national law.

This paragraph shall apply only to contracts concluded or renewed from 29 November 2015.

161. The relevant facts proving a significant discrepancy may be established by any monitoring mechanism certified by the NRA, whether operated by the NRA or by a third party. The Regulation does not require Member States or an NRA to establish or certify a monitoring mechanism. The Regulation does not define how the certification must be done. If the NRA provides a monitoring mechanism implemented for this purpose it should be considered as a certified monitoring mechanism according to Article 4(4).

162. It would help make the rights enshrined in the Regulation more effective if NRAs were to establish or certify one or more monitoring mechanisms that allow end-users to determine whether there is non-conformity of performance and to obtain related measurement results for use in proving non-conformity of performance of their IAS. The use of any certified mechanism should not be subject to additional costs to the end-user and should be accessible also to disabled end-users.

163. The methodologies that could be used by certified monitoring mechanisms are further discussed in the next section on *Methodology for monitoring IAS performance*. The purpose of this guidance regarding methodologies is to contribute to the consistent application of the Regulation. However, NRAs should be able to use their existing measurement tools and these Guidelines do not require NRAs to change them.

Methodology for monitoring IAS performance

164. NRAs should consider BoR (14) 117[35] when implementing a measurement methodology. Measurements should mitigate, to the extent possible, confounding factors which are internal to the user environment, such as existing cross-traffic and the wireless/wireline interface.

165. When implementing measurement methodologies, NRAs should consider guidance on methodologies developed during BEREC's work on QoS in the context of Net Neutrality, especially those found in:

[35] See Chapter 4.8 *Conclusions and recommendations* of BoR (14) 117 "Monitoring quality of Internet access services in the context of net neutrality"

- the 2012 framework for Quality of Service in the scope of Net Neutrality;[36]
- the 2014 Monitoring quality of Internet access services in the context of net neutrality BEREC report;[37]
- the feasibility study of quality monitoring in the context of net neutrality;[38] and
- the planned BEREC 2016-17 workstream on the Regulatory Assessment of QoS in the context of Net Neutrality.[39]

166. Following this existing guidance, the speed is calculated by the amount of data divided by the time period. These speed measurements should be done in both download and upload directions. Furthermore, speed should be calculated based on IP packet payload, e.g. using TCP as transport layer protocol. Measurements should be performed beyond the ISP leg. The details of the measurement methodology should be made transparent.

Article 5
Supervision and enforcement

Article 5(1)

National regulatory authorities shall closely monitor and ensure compliance with Articles 3 and 4, and shall promote the continued availability of non-discriminatory internet access services at levels of quality that reflect advances in technology. For those purposes, national regulatory authorities may impose requirements concerning technical characteristics, minimum quality of service requirements and other appropriate and necessary measures on one or more providers of electronic communications to the public, including providers of internet access services.

National regulatory authorities shall publish reports on an annual basis regarding their monitoring and findings, and provide those reports to the Commission and to BEREC.

Recital 19
National regulatory authorities play an essential role in ensuring that end-users are able to exercise effectively their rights under this Regulation and that the rules on the safeguarding of open internet access are complied with. To that end, national regulatory authorities should have monitoring and reporting obligations, and should ensure that providers of electronic communications to the public, including providers of internet access services, comply with their obligations concerning the safeguarding of open internet access. Those include the obligation to ensure sufficient network capacity for the provision of high quality non-discriminatory internet access services, the general

[36] BoR (11) 53, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/117-a-framework-for-quality-of-srvice-in-the-scope-of-net-neutrality
[37] BoR (14) 117, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/4602-monitoring-quality-of-internet-access-services-in-the-context-of-net-neutrality-berec-report
[38] BoR (15) 207, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5576-feasibility-study-of-quality-monitoring-in-the-context-of-net-neutrality
[39] BoR (15) 213, section 11.2, http://berec.europa.eu/eng/document_register/subject_matter/berec/annual_work_programmes/5551-berec-work-programme-2016

quality of which should not incur a detriment by reason of the provision of services other than internet access services, with a specific level of quality. National regulatory authorities should also have powers to impose requirements concerning technical characteristics, minimum quality of service requirements and other appropriate measures on all or individual providers of electronic communications to the public if this is necessary to ensure compliance with the provisions of this Regulation on the safeguarding of open internet access or to prevent degradation of the general quality of service of internet access services for end-users. In doing so, national regulatory authorities should take utmost account of relevant guidelines from BEREC.

The general approach for supervision

167. With regard to the duties and powers of NRAs set out in Article 5, there are three types of NRA actions to monitor and ensure compliance with Articles 3 and 4.

- Supervision, which encompasses monitoring by the NRA as set out in Article 5(1), and facilitated by the powers to gather information from ISPs in Article 5(2), on:
  - Monitoring of restrictions of end-user rights (Article 3(1)
  - Monitoring of contractual conditions and commercial practices (Article 3(2))
  - Monitoring of traffic management (Article 3(3))
  - Monitoring and assessment of IAS performance and impact of specialised services on the general quality of IAS (Article 3(5) and Article 4)
  - Monitoring of transparency requirements on ISPs (Article 4);
- Enforcement, which can include a variety of interventions and measurements as set out in Article 5(1);
- Reporting by NRAs on the findings from their monitoring, as set out in Article 5(1).

168. BEREC should foster the exchange of experiences by NRAs, on an ongoing basis, on their implementation of the Regulation.

169. To monitor compliance, NRAs may request that ISPs and end-users provide relevant information. Information that can be requested from ISPs is discussed under Article 5(2) and NRAs may collect end-user complaints and ask end-users to complete surveys and questionnaires.

170. Further guidance for specific Articles of the Regulation is described in paragraphs 171-183, and under Articles 3(2) and 3(5).

Monitoring traffic management practices

171. NRAs have the power to collect traffic management information, for instance by:

- evaluating traffic management practices applied by ISPs, including exceptions (allowed by Article 3(3) third subparagraph);
- requesting more comprehensive information from ISPs about implemented traffic management practices, including:
  - a description of, and technical details about, affected networks, applications or services;
  - how they are affected and any other specific differentiation with regards to the application of the practice (such as if the practice is applied only for specific time of day, or in a specific area);

quality of which should not incur a detriment by reason of the provision of services other than internet access services, with a specific level of quality. National regulatory authorities should also have powers to impose requirements concerning technical characteristics, minimum quality of service requirements and other appropriate measures on all or individual providers of electronic communications to the public if this is necessary to ensure compliance with the provisions of this Regulation on the safeguarding of open internet access or to prevent degradation of the general quality of service of internet access services for end-users. In doing so, national regulatory authorities should take utmost account of relevant guidelines from BEREC.

The general approach for supervision

167. With regard to the duties and powers of NRAs set out in Article 5, there are three types of NRA actions to monitor and ensure compliance with Articles 3 and 4.

- Supervision, which encompasses monitoring by the NRA as set out in Article 5(1), and facilitated by the powers to gather information from ISPs in Article 5(2), on:
  - Monitoring of restrictions of end-user rights (Article 3(1)
  - Monitoring of contractual conditions and commercial practices (Article 3(2))
  - Monitoring of traffic management (Article 3(3))
  - Monitoring and assessment of IAS performance and impact of specialised services on the general quality of IAS (Article 3(5) and Article 4)
  - Monitoring of transparency requirements on ISPs (Article 4);
- Enforcement, which can include a variety of interventions and measurements as set out in Article 5(1);
- Reporting by NRAs on the findings from their monitoring, as set out in Article 5(1).

168. BEREC should foster the exchange of experiences by NRAs, on an ongoing basis, on their implementation of the Regulation.

169. To monitor compliance, NRAs may request that ISPs and end-users provide relevant information. Information that can be requested from ISPs is discussed under Article 5(2) and NRAs may collect end-user complaints and ask end-users to complete surveys and questionnaires.

170. Further guidance for specific Articles of the Regulation is described in paragraphs 171-183, and under Articles 3(2) and 3(5).

Monitoring traffic management practices

171. NRAs have the power to collect traffic management information, for instance by:

- evaluating traffic management practices applied by ISPs, including exceptions (allowed by Article 3(3) third subparagraph);
- requesting more comprehensive information from ISPs about implemented traffic management practices, including:
  - a description of, and technical details about, affected networks, applications or services;
  - how they are affected and any other specific differentiation with regards to the application of the practice (such as if the practice is applied only for specific time of day, or in a specific area);

- transparency purposes, by publishing statistics as well as interactive maps showing mobile network coverage or average performance in a geographic area for fixed access networks;
- considering the availability of different IAS offers or offer ranges provided by ISPs, as well as their penetration among end-users;
- assessing the quality for a specific type of IAS, e.g. based on an access technology (such as DSL, cable or fibre);
- comparison of IAS offers in the market;
- investigating possible degradation caused by specialised services.

Monitoring of transparency requirements on ISPs

177. NRAs should monitor transparency requirements on ISPs and could do this by:

- monitoring that ISPs have specified and published the required information according to Article 4(1);
- checking that such information is clear, accurate, relevant and comprehensible;
- cross-checking that the published information is consistent with monitoring results regarding Article 3, such as traffic management practices, IAS performance and specialised services;
- monitoring that ISPs put in place transparent, simple and efficient procedures to address complaints as required by Article 4(2);
- collecting information on complaints related to infringements of the Regulation.

Enforcement

178. In order to ensure compliance with the Regulation, and to promote the continued availability of non-discriminatory IAS at levels of quality that reflect advances in technology, NRAs could decide to:

- require an ISP to take measures to eliminate or remove the factor that is causing the degradation;
- set requirements for technical characteristics to address infringements of the Regulation, for example, to mandate the removal or revision of certain traffic management practices;
- impose minimum QoS requirements;
- impose other appropriate and necessary measures, for example, regarding the ISPs' obligation to ensure sufficient network capacity for the provision of high-quality non-discriminatory IAS (Recital 19);
- issue cease and desist orders in case of infringements, possibly combined with periodical (daily/weekly) penalties, in accordance with national law;
- impose cease orders for specific specialised services unless sufficient capacity is made available for IAS within a reasonable and effective timeframe set by the NRA, possibly combined with periodical (daily/weekly) penalties, in accordance with national law;
- impose fines for infringements, in accordance with national law.

179. In the case of blocking and/or throttling, discrimination etc. of single applications or categories of applications, NRAs could prohibit restrictions of the relevant ports or limitations of application(s) if no valid justification is provided for non-compliance with

the Regulation, especially Article 3(3) third subparagraph. Measures under Article 5(1) could be particularly useful to prohibit practices that clearly infringe the Regulation. Measures could include:

- prohibiting the blocking and/or throttling of specific applications;
- prohibiting a congestion management practice which is specific to individual applications;
- requiring access performance, such as minimum or normally available speeds, to be comparable to advertised/maximum speeds;
- placing qualitative requirements on the performance of application-specific traffic.

180. Requirements and measures could be imposed on one or more ISPs, and it may also, in exceptional cases, be reasonable to impose such requirements in general to all ISPs in the market.

181. The imposition of any of these requirements and measures should be assessed based on their effectiveness, necessity and proportionality:

- Effectiveness requires that the requirements can be implemented by undertakings and are likely to swiftly prevent or remove degradation of IAS offer available to end-users or other infringements of the Regulation.
- Necessity requires that, among the effective requirements or measures, the least burdensome is chosen, i.e. other regulatory tools should be considered and deemed insufficient, ineffective or not able to be used fast enough to remedy the situation.
- Proportionality implies limiting the requirements to the adequate scope, and that the obligation imposed by the requirement is in pursuit of a legitimate aim, appropriate to the pursued aim and there is no less interfering and equally effective alternative way of achieving this aim. For example, if specific ISPs offer degraded IAS services or infringe the traffic management rules of the Regulation, then the proportionate requirements may focus on these ISPs in particular.

Annual reporting of NRAs

182. The reports must be published on an annual basis, and NRAs should publish their annual reports by 30th June for the periods starting from 1st May to 30th April. The first report is to be provided by 30th June 2017, covering the period from 30th April 2016 to 30th April 2017 (the first 12 months following application of the provisions).

183. As well as being published, the reports should be provided to the Commission and to BEREC. To enable the Commission and BEREC to more easily compare the reports, BEREC recommends that NRAs include at least the following sections in their annual reports:

- overall description of the national situation regarding compliance with the Regulation;
- description of the monitoring activities carried out by the NRA;
- the number and types of complaints and infringements related to the Regulation;
- main results of surveys conducted in relation to supervising and enforcing the Regulation;

- main results and values retrieved from technical measurements and evaluations conducted in relation to supervising and enforcing the Regulation;
- an assessment of the continued availability of non-discriminatory IAS at levels of quality that reflect advances in technology;
- measures adopted/applied by NRAs pursuant to Article 5(1).

Article 5(2)

At the request of the national regulatory authority, providers of electronic communications to the public, including providers of internet access services, shall make available to that national regulatory authority information relevant to the obligations set out in Articles 3 and 4, in particular information concerning the management of their network capacity and traffic, as well as justifications for any traffic management measures applied. Those providers shall provide the requested information in accordance with the time-limits and the level of detail required by the national regulatory authority.

184. NRAs may request from ISPs information relevant to the obligations set out in Articles 3 and 4 in addition to the information provided in contracts or made publicly available. The requested information may include, but is not limited to:

- more details and clarifications about when, how and to which end-users a traffic management practice is applied;
- justifications of any traffic management practice applied, including whether such practices adhere to the exceptions of Article 3(3) (a)-(c). In particular,
  - regarding Article 3(3) (a), the exact legislative act, law, or order based on which it is applied;
  - regarding Article 3(3) (b), an assessment of the risk to the security and integrity of the network;
  - regarding Article 3(3) (c), a justification of why congestion is characterised as impending, exceptional or temporary, along with past data regarding congestion that confirms this characterisation, and why less intrusive and equally effective congestion management does not suffice.
- requirements for specific services or applications that are necessary in order to run an application with a specific level of quality;
- information allowing NRAs to verify whether, and to what extent, optimisation of specialised services is objectively necessary;
- information about the capacity requirements of specialised services and other information that is necessary to determine whether or not sufficient capacity is available for specialised services in addition to any IAS provided, and the steps taken by an ISP to ensure that;
- information demonstrating that the provision of one or all specialised services provided or facilitated by an ISP is not to the detriment of the availability or general quality of IAS for end-users;
- details about the methodology by which the speeds or other QoS parameters defined in contracts or published by the ISP are derived;

- details about any commercial agreements and practices that may limit the exercise of the rights of end-users according to Article 3(1), including details of commercial agreements between CAPs and ISPs;
- details about the processing of personal data by ISPs;
- details about the type of information provided to the end-users from ISPs in customer centres, helpdesks or websites regarding their IAS;
- the number and type of end-user complaints received for a specific period;
- details about the complaints received from a specific end-user and the steps taken to address them.

Article 5(3)

By 30 August 2016, in order to contribute to the consistent application of this Regulation, BEREC shall, after consulting stakeholders and in close cooperation with the Commission, issue guidelines for the implementation of the obligations of national regulatory authorities under this Article.

185. These Guidelines constitute compliance with this provision. BEREC will review and update the Guidelines as and when it considers it to be appropriate.

Article 5(4)

This Article is without prejudice to the tasks assigned by Member States to the national regulatory authorities or to other competent authorities in compliance with Union law.

186. NRAs and other competent authorities may also have other supervision and enforcement tasks assigned to them by Member States in compliance with Union law. Such duties may arise out of, for example, consumer and competition law, in addition to the regulatory framework for electronic communications. Article 5 does not affect the tasks of NRAs or other competent national or European authorities arising from such laws, regardless of the fact that such tasks may overlap with the duties of NRAs (or other competent authorities) as set out in the Article. The Regulation does not affect NRAs' or other national authorities' competences to supervise and enforce Directive 95/46/EC or Directive 2002/58/EC referred to in Article 3(4), as such tasks continue to be assigned by national law.

Article 6
Penalties

Member States shall lay down the rules on penalties applicable to infringements of Articles 3, 4 and 5 and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by 30 April 2016 and shall notify the Commission without delay of any subsequent amendment affecting them.

187. This provision is aimed at Member States and no guidance to NRAs is required.

Article 10
Entry into force and transitional provisions

Article 10(1)

> This Regulation shall enter into force on the third day following that of its publication in the Official Journal of the European Union.

188. The Regulation entered into force on 29 November 2015.

Article 10(2)

> It shall apply from 30 April 2016, except for the following:
>
> […]
>
> (c) Article 5(3) shall apply from 29 November 2015;
>
> […]

189. The Regulation applies from 30 April 2016, except for Article 5(3) which obliges BEREC to issue these Guidelines and which applies from 29 November 2015.

190. When monitoring and ensuring compliance with Articles 3 and 4, NRAs should take into account that the provisions of the Regulation apply to all existing and new contracts with the exception of Article 4(4), which applies only to contracts concluded or renewed from 29 November 2015.[42] In turn, this means that, for a transitional period, Article 4(4) is not applicable to a certain amount of contracts. However, Article 4(4) will become applicable to more and more contracts over time once they are renewed or newly concluded.

Article 10(3)

> Member States may maintain until 31 December 2016 national measures, including self-regulatory schemes, in place before 29 November 2015 that do not comply with Article 3(2) or (3). Member States concerned shall notify those measures to the Commission by 30 April 2016.

191. Article 10(3) is addressed to Member States. However, when assessing compliance with Article 3(2) and (3), NRAs should take into account that national measures, including self-regulatory schemes, might benefit from a transitional period until 31 December 2016 when they may be maintained, provided that they were in place before 29 November 2015 and have been notified by the respective Member State to the Commission by 30 April 2016. In that event, no breach of Article 3(2) and Article 3(3) would be found during this transitional period.

[42] See paragraph 134 of these Guidelines

Anexo 15: Entrevista Francisco Balarezo tabla

Preguntas y respuestas en entrevista realizada al Ing. Francisco Balarezo, Gerente General de Netlife en Ecuador y Director Ejecutivo de la AEPROVI.

¿Qué es la neutralidad de la red (NN)?

- Es un concepto universal. Se debe tomar en cuenta como este principio se encuentra consagrado en la normativa ecuatoriana, en este caso la LOT, que abarca la neutralidad de la red y neutralidad tecnológica.

- En este contexto, la neutralidad de la red debe permitir la interoperabilidad de las redes; en una intranet país los diferentes proveedores deben permitir que los operadores desarrollen sus redes y mejoren sus tecnologías en función del mercado (geografía, condiciones) en donde se desenvuelve. En este contexto la neutralidad de la red se enfoca a que no exista bloqueo de contenido en la red Internet (por más que exista riesgo de redes o efectos nocivos); frente a consultas expuestas al regulador al respecto se indica que no existe respuesta todavía (por ejemplo por motivos de seguridad/bloqueo de puerto 25); únicamente se tiene la opción de bloqueo por solicitud de usuario.

Desde el punto de vista de los ISP, ¿Existe NN? y ¿Es conveniente contar con lineamientos frente a este principio?

- Los operadores aplican la neutralidad de la red de acuerdo a lo que permite la Ley, tanto a nivel de los operadores y consumidores, se considera que se cumple con este principio. Lo que existe en la red es libre, no obstante se identifica problemática sobre la piratería que minaría los servicios y frente a ello sí se identifica la necesidad de que se generen reglas por cuanto hay afectación en dos (2) aspectos: la prestación del servicio de audio y video por suscripción y el costo de uso de servicio a los usuarios.

En cuanto a la piratería y contenido ¿Cómo se enfoca la NN en cuanto a contenido por parte de las grandes empresas frente a las medianas y pequeñas empresas?

- Se explica que el mayor porcentaje de tráfico se encuentra concentrado en las redes de las grandes operadoras, cuestión que es común en cualquier lugar del mundo, incluyendo en el Ecuador.

- En el país existen alrededor de 400 ISP pequeños que tendrían aproximadamente el 5% de tráfico de Internet; de esta manera un factor importante que se observa es que las empresas realizan inversiones sobre la expansión de las redes, lo cual implica inversiones altamente importantes, de esta manera se observa un concepto adicional importante que es el pago de un "peaje" de contenidos (quien pueda pagar por pasar contenido por las redes implementadas, ese contenido será disponible).

- Es necesario que en el país se incentive la conectividad (reducción de la brecha digital) y social (campo laboral por acceso a tecnología, información). El déficit de acceso en Internet Fijo es de alrededor del 60%; por lo tanto, los indicadores deben ser evaluados en la parte marginal por la falta de oportunidades.

- Las operadoras grandes tendrán la oportunidad de desplegar redes con mayor oportunidad, se ha sugerido a las autoridades la emisión de títulos habilitantes de despliegue de redes que al momento no se tiene.

¿Se considera que se aplica transparencia de la información en el Ecuador?

- La existencia de la LOT es suficiente para el cumplimiento de la transparencia; no obstante, existen prestadores que no necesariamente cumplen con esta obligación.

- Para hacer cumplir con la oferta de valor, se ha creado la cultura del reclamo por la falta de cumplimiento, se debe hacer conciencia sobre lo que se ofrece al usuario y lo que se brinda realmente.

- ¿Se hace conciencia al respecto? Existe una gran insatisfacción de los clientes por la falta de cumplimiento de la oferta brindada por los prestadores, siendo éste un

tema revelador. Es un tema de comportamiento ético en donde debe fomentarse la cultura de calidad más que del reclamo.

Frente a la decisión reciente de los EE.UU para dar de baja los lineamientos sobre NN del 2015, ¿Cuál es su opinión de qué es lo que puede pasar?

- Existe una diferencia entre los mercados de los EE.UU. y la Región.

- Los ISP mantienen la neutralidad de la red; en la región no existe una gran industria de los contenidos. Por el contrario en los EE.UU. se produce esta polémica por los grandes proveedores de contenidos, ganando para ello, los operadores de redes.

- A corto plazo en el Ecuador lo que se piensa que pasará es el establecimiento de normas básicas y elementales para garantizar la calidad del servicio y poco con el contenido, con ello se puede lograr mayor simetría.

- Es importante también la generación de esta normativa dada la existencia de los llamados OTT (Over-The-Top de libre transmisión), los cuales no tienen regulación alguna hasta la presente fecha.

- En el Ecuador no existen proveedores de contenido; no obstante si se quisiera impulsar estos desarrollos, es necesario pensar detenidamente sobre el contenido de una normativa sobre neutralidad de la red.

¿Qué implica la neutralidad de la red frente a las aplicaciones?

- Es un tema totalmente comercial, por cuanto los usuarios pueden acceder a las aplicaciones que se requiera por parte de los usuarios.

- Lo que se observa es que se limite el acceso a ciertas aplicaciones; estos son aspectos que no se consideran requiere regulación porque no se debe limitar el desarrollo de los contenidos y aplicaciones. Para ello lo que sí es exigido es el despliegue de una mayor cantidad de redes en donde se trate la calidad del servicio.

¿Se debe generar lineamientos en el país sobre la NN basado en las normativas y experiencias internacionales?

- Amerita como urgente que se genere legislación orientada a la piratería, sea factible el bloqueo cuando se identifique que la distribución del contenido sea pirata, bajo los justificativos debidamente fundamentados.

- Se debe diferenciar entre las responsabilidades de los proveedores de acceso a Internet, de aquellas responsabilidades de los proveedores de contenidos (responsabilidad de derechos de autor por ejemplo).

Aspectos finales sobre la entrevista realizada

- En términos de NN, el país requiere generar normas básicas y urgentes, especialmente para detener la piratería en el mercado y en la misma línea definir lineamientos para que los proveedores de contenido puedan tener al menos su jurisdicción controlada de manera local, caso contrario es necesario tomar otras medidas de carácter tributario.

- No se está de acuerdo con la decisión de la FCC para el pago indiscriminado de peaje por paso de contenido sobre las redes; es decir la aplicación de bloqueo en los casos de no poder transitar contenido, se dividiría en este sentido a Internet en dos capas: Internet abierto y libre y por otro lado un Internet pagado. Se debe tomar en cuenta que el Internet ha tenido éxito porque no ha sido regulado.

- Es importante este tema para colocarlo sobre la mesa de trabajo de normativa que se desarrolle en el Ecuador y es importante compartir los trabajos realizados al respecto.