MRCET

MAESTRÍA EN REGULACIÓN Y COMPETENCIA ECONÓMICA DE LAS TELECOMUNICACIONES

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"LA OBLIGACIÓN DE TRANSPARENCIA BAJO LAS REGLAS DE NEUTRALIDAD DE LA RED EN LOS ESTADOS UNIDOS DE AMÉRICA: EL CASO VERIZON WIRELESS"

CASO PRÁCTICO
Que para obtener el grado de MAESTRA EN REGULACIÓN Y COMPETENCIA ECONÓMICA DE LAS TELECOMUNICACIONES

Presenta:

Adriana Regina Begné de Larrea

Asesora:

Dra. Olivia Andrea Mendoza Enríquez

Ciudad de México, octubre, 2019.

CONACYT

INSTITUTO DE INVESTIGACIONES JURÍDICAS unam

INFOTEC POSGRADOS

ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

Autorización de Impresión

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

MAESTRÍA EN REGULACIÓN Y COMPETENCIA ECONÓMICA DE LAS TELECOMUNICACIONES

Ciudad de México, 17 de octubre de 2019
INFOTEC-DAIC-GCH-SE-0126/19.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

LA OBLIGACIÓN DE TRANSPARENCIA BAJO LAS REGLAS DE NEUTRALIDAD DE LA RED EN LOS ESTADOS UNIDOS DE AMÉRICA: EL CASO VERIZON WIRELESS

Desarrollado por la alumna **Adriana Regina Begné de Larrea** y bajo la asesoría de la **Dra. Olivia Andrea Mendoza Enríquez**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.

Mtra. Julieta Alcibar Hermosillo
Coordinadora de biblioteca

***Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.**

C.p.p Servicios Escolares

Agradecimientos

A mi hijo, Rodrigo Soto Begné, por ser la persona que más amo en mi vida y respecto de la cual quiero ser un ejemplo a seguir en cuanto a fortaleza.

A mis padres, Elsa y Eduardo, por haber sido excepcionales y hacer de mí la persona que soy hoy; los quiero y extraño siempre.

Al Instituto Federal de Telecomunicaciones, por darme la oportunidad de estudiar este posgrado.

A mi asesora, Dra. Olivia Andrea Mendoza Enriquez, por guiarme y apoyarme en la elaboración de este trabajo de investigación.

A mis amigos y compañeros de trabajo y de la maestría por acompañarme en este camino de aprendizaje.

Tabla de contenido

Índice de cuadros

Introducción

El concepto de neutralidad de la red tiene su origen en un concepto más amplio que es el de apertura de Internet y que, no obstante que en éste coincide la mayoría de los actores que se benefician de lo que representa tener acceso de manera rápida a la información en línea tal como lo conocemos hoy, así como a una gran cantidad de servicios y contenidos a través de Internet, el primero de ellos ha generado múltiples controversias y debates, particularmente en los Estados Unidos de América en relación con la necesidad de regular o no las actividades o prácticas en las que los proveedores de acceso a Internet (ISP, por sus siglas en inglés) de banda ancha suelen incurrir o llevar a cabo con motivo de la prestación de este servicio a sus usuarios finales a través de su red.

Si bien desde el punto de vista meramente técnico, la neutralidad de la red implica la gestión del tráfico, en cuanto a su enrutamiento, así como en cuanto al control y manipulación de las comunicaciones, sin que ello implique una discriminación o diferenciación del tráfico que resulte arbitraria o irracional por parte de los operadores de redes de telecomunicaciones, la preocupación por contar con reglas que promuevan y defiendan la libertad y la apertura en internet en contra de prácticas que se consideran contrarias a ésta, ha sido una constante desde hace muchos años en los Estados Unidos. Considerando que este país constituye una referencia para el resto del mundo en materia de telecomunicaciones e internet y que, en el transcurso de los últimos años, ha cambiado de enfoque e interpretación a través de la Comisión Federal de Comunicaciones, en relación con el alcance que deben tener tales reglas en beneficio de los usuarios y de la competencia, y sobre la necesidad de prohibir o no prácticas como el bloqueo de contenidos o sitios web, la ralentización de la velocidad de las conexiones a internet, o bien, el envío de información o publicidad debido al rastreo no consentido de hábitos de consumo de los suscriptores de banda ancha, resulta importante entender el enfoque que ha tenido esa autoridad en relación con la obligación de los proveedores de banda de actuar de manera transparente.

Esta obligación de ser transparentes en relación con sus políticas de gestión de red, así como respecto de los términos y condiciones comerciales y técnicos bajo los cuales prestan el servicio de banda ancha, ha permanecido a lo largo de la política regulatoria de la Comisión Federal de Comunicaciones como una exigencia a cargo de los proveedores de servicios de acceso a internet de banda ancha. Así, tomando en cuenta los principios de libertad de elección y transparencia que caracterizan el concepto de Internet como un entorno abierto para el acceso y el intercambio de información entre sus usuarios y entre éstos y otros proveedores de servicios, contenidos y aplicaciones, conocidos como *edge providers*, resulta fundamental conocer cómo la Comisión Federal de Comunicaciones de los Estados Unidos ha entendido la transparencia hacia los consumidores por parte de los proveedores del servicio de acceso a Internet de banda ancha, considerado éste como el medio indispensable a través del cual se tiene acceso a una gran cantidad de información y servicios en internet.

El tema central del caso cuyo análisis se propone a través de este trabajo, se refiere a la violación cometida a partir de 2012 por la empresa de telefonía celular Verizon Wireless a la regla de transparencia prevista en las Reglas de Internet Abierto emitidas por la Comisión Federal de Comunicaciones en 2010, la cual mandata, entre otros aspectos, que los proveedores de servicios de acceso a internet divulguen sus políticas de privacidad en relación con la información que manejan de sus clientes. Fue así que, con motivo de la práctica de rastreo de información realizada por el operador inalámbrico sin el consentimiento de sus usuarios de banda ancha móvil, la oficina de cumplimiento de la Comisión (*Enforcement Bureau*) inició una investigación a finales del año 2014 para conocer si Verizon protegió o no adecuadamente la información generada por sus clientes, propiedad de éstos.

Es por ello que en el primer capítulo de este trabajo se analizan los conceptos de apertura en Internet, así como el principio de transparencia en el cual se basa y las implicaciones que puede tener la falta de transparencia en la privacidad de las personas físicas en relación con las prácticas cometidas por algunos ISP. En el segundo apartado de este documento se explica asimismo el marco jurídico del cual

provienen, tanto la regla de transparencia aplicable a los ISP en los Estados Unidos, así como la obligación de confidencialidad y privacidad que les atañe dentro del mismo contexto de internet. En el último capítulo se explica el caso concreto que permitirá conocer cómo la autoridad reguladora de ese país decidió resolverlo tomando en cuenta no solo lo que establece el marco legal como obligación a cargo de los proveedores del servicio de acceso a internet sino también la opinión de organizaciones de la sociedad civil y de protección a los consumidores que buscan salvaguardar y proteger su derecho a la privacidad e incluso las actuaciones por parte del operador inalámbrico cuyas prácticas fueron objeto de investigación. De todo lo anterior, se concluirá en el apartado correspondiente con las posturas y hallazgos que el autor realiza al respecto con el fin de determinar si a la luz de la regla de transparencia señalada, y tomando en cuenta las políticas de privacidad del operador inalámbrico, resultan éstas suficientes para proteger a los usuarios contra actos que atentan contra la libertad y apertura de Internet.

Capítulo 1

Neutralidad de la red: internet abierto, transparencia y privacidad

Capítulo 1: Neutralidad de la red: internet abierto, transparencia y privacidad

1.1 Internet abierto

La apertura en Internet ha sido una constante en las decisiones de la Comisión Federal de Comunicaciones de los Estados Unidos de América (en adelante, la FCC, por sus siglas en inglés) a lo largo de los años, así como parte de su regulación con el objeto de salvaguardar, entre otras cuestiones, el derecho de información y adecuada elección de los consumidores en Internet en relación con los servicios y contenidos a los que tienen acceso. Desde la decisión considerada como histórica en 1968 sobre el asunto Carterfone[1] hasta la última orden de internet abierto adoptada en diciembre de 2017,[2] la FCC ha reconocido la importancia de las redes de telecomunicaciones cuando éstas sirven al interés público al empoderar a los usuarios para que éstos tomen sus propias decisiones sobre cómo acceder y utilizarlas sin impedimentos u obstáculos innecesarios. Así, bajo la Declaración de Política de Internet emitida en 2005 por esa autoridad, conocida como *Internet Policy Statement*, se establecieron cuatro principios rectores para fomentar el despliegue de banda ancha y "preservar y promover la naturaleza abierta e

1 Véase: In the Matter of Use of the Carterfone Device in Message Toll Telephone Service; *Federal Communications Commission*, 13 F.C.C. 2d 420, junio de 1968, párrafo 424, disponible en https://web.archive.org/web/20150120021035/http://www.uiowa.edu/~cyberlaw/FCCOps/1968/13F2-420.html, última fecha de consulta el 16 de septiembre de 2018. En este caso la FCC consideró como irrazonable e ilegal la práctica de AT&T de evitar que los consumidores pudieran conectar a la red telefónica residencial cualquier equipo que no fuese provisto por AT&T, aun cuando éste no implicara un riesgo a la red, de modo que esa autoridad reconoció que los consumidores tienen derecho a conectar los dispositivos de su elección a su red telefónica, mientras no la afecten de manera negativa. En el original se lee: "Our conclusion here is that a customer desiring to use an interconnecting device to improve the utility to him of both the telephone system and a private radio system should be able to do so, so long as the interconnection does not adversely affect the telephone company's operations or the telephone system's utility for others".

2 Al día de hoy la Comisión Federal de Comunicaciones ha emitido las siguientes reglas de internet abierto bajo la figura de una orden: *Preserving the Open Internet*, adoptada el 21 de diciembre de 2010; *Protecting and Promoting the Open Internet*, emitida el 26 de febrero de 2015, y *Restoring Internet Freedom*, del 14 de diciembre de 2017, en las cuales reconoce la importancia y necesidad continua de preservar y proteger un internet abierto. Disponibles en: https://www.fcc.gov/document/preserving-open-internet, https://www.fcc.gov/document/protecting-and-promoting-open-internet-0 y https://www.fcc.gov/restoring-internet-freedom.

interconectada de Internet",[3] buscando asimismo garantizar que los consumidores tengan derecho a acceder y utilizar en línea el contenido, las aplicaciones y los dispositivos legales de su elección.

Cómo entiende la FCC la apertura de internet o, más bien, qué reglas son necesarias para su protección es lo que ha variado en el transcurso de los últimos años según se verá en el presente trabajo; no obstante lo anterior, los principios que permanecen constantes como parte de la política de la Comisión son los relativos al acceso abierto, la competencia y la elección de los consumidores.

1.1.1 Qué se entiende por internet abierto y por neutralidad de la red

El término Internet Abierto conocido como *Open Internet* suele equipararse al de neutralidad de la red que inició su auge a partir de 2003[4] en los Estados Unidos de América en un contexto en el que ya existía un debate entre aquellos que propugnan por un internet sin restricciones y aquellos que defienden la necesidad de establecer cierta regulación que garantice la no discriminación, pero fue a principios de los años noventa cuando los hacedores de políticas y los ingenieros comenzaron a referirse a Internet como un sistema abierto conformado voluntariamente por una "federación" de usuarios y proveedores, tal como prevalece hoy en día, en contraste con lo que fue su precursor, la Red de la Agencia de Proyectos de Investigación Avanzada por sus siglas en inglés ARPANET,[5] creada y patrocinada por el gobierno

3 Comisión Federal de Comunicaciones, *Policy Statement*, FCC 05-151, Washington DC, 2005, p. 3, disponible en https://docs.fcc.gov/public/attachments/FCC-05-151A1.pdf. Última fecha de consulta 26 de septiembre de 2018.

4 Véase, por ejemplo, el artículo escrito en 2003 por Tim Wu, abogado influyente en la política y regulación en materia de telecomunicaciones e internet en los Estados Unidos, *Net Neutrality, Broadband Discrimination,* en el que ya preveía el conflicto que los reguladores habrían de presenciar la siguiente década entre los intereses privados de los proveedores de banda ancha y el interés público en un ambiente de innovación competitiva centrado en Internet. Disponible en: http://dx.doi.org/10.2139/ssrn.388863. Última fecha de consulta 16 de septiembre de 2018.

5 ARPANET fue creada a solicitud del departamento de Defensa de los Estados Unidos para la comunicación de larga distancia entre distintos organismos e instituciones académicas, científicas, industriales y gubernamentales de ese país. http://www.computerhistory.org/internethistory/. Última fecha de consulta el 26 de agosto de 2018.

de los Estados Unidos en un ambiente deliberadamente cerrado en virtud de sus fines.[6]

El concepto de apertura es central para considerar a Internet como un sistema que incluye usuarios, aplicaciones e infraestructura y que incide en todos sus aspectos tal como lo conocemos hoy, técnico, económico, político y social. Así, desde un punto de vista técnico, la apertura de Internet es un principio básico que tiene que ver con el diseño mismo de la red en el sentido de que la misma se encuentra abierta a la interconexión de otras redes o de cualquier dispositivo mientras éstos cumplan con los protocolos necesarios para su interoperabilidad y adecuado funcionamiento. Lo anterior a su vez conlleva el uso de estándares técnicos abiertos en el desarrollo y aplicación de tecnologías los cuales se adoptan de manera consensuada y permiten el desarrollo de nuevas tecnologías sin constreñir la innovación; es decir, se habla de la apertura de la red en cuanto a la participación de los productores de tecnología[7] lo cual permite que los usuarios tengan acceso a nuevas tecnologías o nuevos usos de las tecnologías ya existentes, puesto que se trata de un sistema que permite el despliegue o la ejecución de las mismas sin necesidad de hacer cambios en la red o sin la intervención del operador de la red; desde un enfoque económico, a diferencia de las redes tradicionales de telefonía que fueron creadas en sus inicios como monopolios, el diseño de Internet permite la entrada continua de nuevos proveedores de servicios; un ejemplo de lo anterior lo constituyen los acuerdos de intercambio de tráfico, conocidos como *peering*, entre los distintos proveedores de acceso a Internet que se rigen por acuerdos flexibles, tales como la regla del mejor esfuerzo para el envío de paquetes, sin necesidad de un control central. Por otra parte, considerando que Internet es un conjunto de redes operadas y controladas individualmente por las decisiones y acciones de sus propios miembros, la apertura permite un espectro de opciones disponibles entre los distintos modelos de

6 Internet Society, *The Open Internet, What is, and how to avoid mistaking it for something else,* Estados Unidos, 2014. Disponible en: https://www.internetsociety.org/resources/doc/2014/the-open-internet-what-it-is-and-how-to-avoid-mistaking-it-for-something-else/. Última fecha de consulta el 20 de agosto de 2018.

7 Pisanty, Alejandro, "Principios fundamentales de la gobernanza de Internet", *Pensar Internet*, México, Universidad Iberoamericana, 2016, pp. 16-53.

colaboración que no se limita a un modelo que requiere de un alto grado de uniformidad o centralización como lo es en el caso de una red única centralizada, puesto que, desde un punto de vista de organización política, se trata de un modelo de múltiples partes interesadas que reconoce este principio de apertura. Finalmente, desde un enfoque social si bien Internet ha modificado las relaciones tradicionales para llevar a cabo intercambios de información entre las personas, ello no significa que se anulen o invaliden, por ejemplo, las leyes que existen en materia de derechos de autor o de privacidad. No obstante, la apertura en internet puede significar o aumentar daños potenciales, especialmente aquellos que involucran la privacidad de las personas y el control de información personal.

Así lo refiere la Sociedad de Internet,[8] destacando no solo los aspectos técnico, económico, social y político en los que tiene incidencia la apertura de la red, sino señalando como dimensiones relevantes de un internet abierto la transparencia, el acceso y la participación, reconociendo asimismo el aspecto de vulnerabilidad que ha caracterizado a Internet en virtud de su carácter abierto. Es decir, la apertura en Internet permite que las características de acceso, elección y transparencia por parte de los usuarios y hacia éstos se garanticen al considerar, respectivamente, que:

- el acceso a servicios de internet, aplicaciones, sitios y contenidos mejora la experiencia de los usuarios y el potencial de internet para impulsar la innovación, la creatividad y el desarrollo económico;
- la elección y control por parte de los usuarios sobre sus actividades en línea, incluidos proveedores, servicios y aplicaciones, reconociendo que existen limitaciones legales y técnicas, y

8 La Internet Society es una organización sin fines de lucro creada en 1992 para proporcionar guía y liderazgo en todos los aspectos relacionados con estandarización técnica, educación y políticas en materia de Internet. Tiene sus oficinas en Washington, D.C. y en Ginebra, Suiza y como objetivo asegurar el desarrollo, evolución y uso abiertos de Internet para beneficio de todas las personas alrededor del mundo. La página oficial de la Internet Society está disponible en: http://InternetSociety.org. Última fecha de consulta el 20 de agosto de 2018.

- la transparencia, incluida la provisión de información precisa sobre el ancho de banda y las políticas de gestión de red, permite a los usuarios tomar decisiones informadas sobre sus servicios de Internet.[9]

Comprender el concepto de apertura de internet de una manera unívoca no es tarea fácil puesto que en muchos casos se equipara sin distinciones al concepto de neutralidad de la red dependiendo del contexto en el que se le emplea y de los objetivos de política que se buscan lograr como más adelante se explica; no obstante, la apertura en Internet va más allá del concepto de neutralidad de la red, puesto que implica que el acceso a Internet no esté obstaculizado por factores tales como la incompatibilidad técnica, o bien, la falta de capacidad para administrar u operar la red,[10] mientras que la neutralidad de la red implica ante todo la no discriminación por parte de los operadores de red en el manejo del tráfico de Internet.

El concepto de Internet como una plataforma abierta también ha sido reconocido a lo largo del tiempo por muchas organizaciones y actores, como un lugar en el que "empresas, ciudadanos y gobiernos pueden innovar y desarrollar espontáneamente aplicaciones y servicios",[11] lo cual conduce en un ambiente de economía digital a una gran cantidad de innovaciones.

Cabe destacar que para la Comisión Federal de Comunicaciones de los Estados Unidos la neutralidad de la red es una forma de abarcar y entender el concepto de internet abierto. En 2005, como se mencionó anteriormente, en su declaración de política sobre Internet, la FCC adoptó en beneficio de los consumidores, cuatro principios torales para promover y proteger el carácter abierto e interconectado de Internet que dicho organismo reconoce. Es decir, dada la

9 Internet Society, *Open Inter-networking: Getting the fundamentals right: access, choice, and transparency*, Estados Unidos, 2010, disponible en: http://www.internetsociety.org/open-inter-networking-getting-fundamentals-right-access-choice-and-transparency. Última fecha de consulta el 20 de agosto de 2018.

10 Pisanty, Alejandro y Huesca, Erik, *Neutralidad de la red en Internet*, México, 2015, disponible en línea en: https://www.isoc.mx/wp-content/uploads/2017/11/Neutralidad_de_la_Red_en_Internet-1.pdf. Última fecha de consulta 3 de septiembre de 2018.

11 Organización para la Cooperación y el Desarrollo Económicos, *Perspectivas de la OCDE sobre la economía digital 2015,* París, 2015, disponible en: http://dx.doi.org/10.1787/9789264259256-es, última fecha de consulta el 6 de septiembre de 2018.

naturaleza abierta de Internet, la FCC señaló que dichos principios, si bien no constituían parte de la regulación en ese momento puesto que se trataba de una mera declaratoria de principios, estarían presentes continuamente en sus actividades como hacedor de políticas.[12] Así, con el objeto de garantizar y fomentar que las redes de banda ancha sean ampliamente desplegadas, abiertas, accesibles y asequibles para todos los consumidores, la FCC adoptó los siguientes principios, de modo que los consumidores tengan derecho a:

- acceder a cualquier contenido legal en Internet que sea de su preferencia o elección;
- ejecutar aplicaciones y utilizar los servicios que sean de su elección;
- conectar los dispositivos o equipos terminales legales de su elección que no dañen la red, y
- que exista competencia entre los proveedores de red, proveedores de aplicaciones y servicios, y proveedores de contenido; y, por tanto, a elegir entre ellos.[13]

Cinco años después, la Comisión Federal de Comunicaciones, a través de las reglas de internet abierto de 2010, reconoció que los fundadores de Internet crearon intencionalmente una red abierta, en el sentido de que no requiere guardianes que limiten la innovación y la comunicación a través de la red.[14]

Así, en sus reglas de internet abierto de 2010, que siguieron a los principios de internet abierto emitidos en 2005 por dicha autoridad, ésta señaló que la apertura de internet en virtud de la cual éste ha prosperado, se caracteriza por la ausencia de un proveedor de acceso a Internet de banda ancha[15] que controle dicho acceso,

---

12 Comisión Federal de Comunicaciones*, Policy…, cit.,* p. 3.

13 Lo anterior sujeto a una administración razonable de la red. *Idem,* nota al pie 15.

14 Comisión Federal de Comunicaciones, *Federal Register*, "Preserving the Open Internet; Final Rule", Vol. 76, No. 185, septiembre 2011, pp. 59193-59194, disponible en https://www.federalregister.gov/documents/2011/09/23/2011-24259/preserving-the-open-internet Última fecha de consulta 3 de febrero de 2019.

15 *Ibidem,* pp. 55192-55193; p. 59201.

La definición del servicio de acceso a internet de banda ancha propuesta por la Comisión comprende cualquier transmisión de datos bajo el protocolo de internet entre un usuario final y el Internet y comprende servicios que proveen la capacidad de transmitir y recibir datos, desde y hacia, todos o substancialmente todos los puntos terminales de Internet.

conocidos como *gatekeepers*,[16] mediante el bloqueo de los usos legales de internet, lo que implica que los consumidores e innovadores no tienen que solicitar permiso antes de usar internet ya sea para lanzar nuevas tecnologías, iniciar negocios, conectar con personas, o bien, simplemente para expresar y compartir sus opiniones.[17] Lo anterior implica que los consumidores, usuarios de internet, puedan elegir libremente las aplicaciones y servicios que sean de su preferencia, así como decidir el contenido al cual quieran tener acceso, o bien, crear contenido y compartirlo con otros, de modo que esta apertura promueve la competencia y un ciclo virtuoso en aras de la innovación y la inversión en redes de banda ancha.[18]

En este contexto es como el concepto de neutralidad de la red ha sido utilizado ya que es un término que puede abarcar múltiples objetivos, desde garantizar la libertad de expresión, la capacidad de elección de los usuarios y la no discriminación, hasta cuestiones de carácter comercial o técnico, incluidos la gestión del tráfico, los precios y los modelos de negocio; es por ello que, siguiendo la recomendación de la Internet Society, el enfoque apropiado deberá ser aquel con miras a obtener el resultado deseado: una continua interoperabilidad de redes abierta.[19]

En cualquier caso, podemos considerar que la capacidad de conectar, comunicar, innovar, elegir, compartir y confiar, en relación con la información que se genera y circula a través de Internet, se basa en el concepto de apertura de internet, característica ésta que no debiera subordinarse a otros aspectos de Internet.

---

16 Comisión Federal de Comunicaciones, *Federal Register*, "Protecting and Promoting the Open Internet; Final Rule", Vol. 80, No. 70, abril 2015, p. 19747, disponible en línea en https://www.federalregister.gov/documents/2015/04/13/2015-07841/protecting-and-promoting-the-open-internet. Última fecha de consulta 23 de febrero de 2019. Al respecto, se considera que los proveedores de acceso a Internet de banda ancha tienen la capacidad de controlar o limitar dicho acceso, concepto que corresponde o se asimila al anglicismo *gatekeeper.* La FCC ha reconocido que los proveedores de banda ancha funcionan como *gatekeepers* tanto para los usuarios finales que tienen acceso a internet, así como para los proveedores de contenidos, aplicaciones y servicios que ofrecen o venden sus servicios a los clientes de los primeros.

17 Comisión Federal de Comunicaciones, *Preserving the Open*…, *cit.,* p. 59224.

18 *Idem*.

19 Internet Society, *Open Inter-networking: …, cit.,* p. 1.

1.1.2 Limitaciones al Internet abierto

La cada vez más creciente demanda de conexiones de banda ancha a Internet conlleva una mayor presión sobre la capacidad de la red, situación que no va a disminuir debido a la evidente importancia de contar con acceso a Internet con motivo de su ubicuidad y rapidez, lo que implica necesariamente que los operadores de red utilicen herramientas de gestión de tráfico de red lo que ha llevado a que traten los paquetes de datos de distinta manera cobrando incluso por ello a los usuarios; todo lo anterior ha generado una multiplicidad de debates en el sentido de que el carácter abierto de Internet esté en riesgo por lo que algunos consideran que la regulación es necesaria para preservarlo y su capacidad para actuar como motor del crecimiento, la innovación y la libertad de expresión.[20]

En términos generales, el concepto de neutralidad de la red conlleva el mandato para que los operadores de red no incurran en prácticas discriminatorias en contra de los proveedores de aplicaciones y contenidos en Internet.[21] Si bien existen múltiples prácticas que tienen como resultado la discriminación, habrá algunos que consideran que no necesariamente tales desviaciones del principio de neutralidad de la red causan un daño al consumidor o a la innovación; tal es el caso de Yoo, quien considera que esas desviaciones podrían estar justificadas en la medida en que se trata de intentos por parte de los propietarios de la red para satisfacer las cada vez más intensas y heterogéneas demandas de los usuarios finales, de modo que sugiere que la innovación, así como la competencia, podrían ser mejor atendidas si los hacedores de políticas adoptasen un principio de "diversidad de redes" que permita a los operadores de red tener distintos enfoques para el enrutamiento del tráfico. Yoo contrasta, a manera de ejemplo, el caso de las aplicaciones que predominaban en los inicios de Internet, como el correo electrónico y la navegación web,[22] en las que los retrasos de medio segundo eran casi

20 *Idem.*

21 Wu, Tim y Yoo, Christopher, "Keeping the Internet neutral?: Tim Wu and Christopher Yoo Debate", *Federal Communications Law Journal*, 2007, Vol. 59: Iss. 3, artículo 6, p. 575, disponible en: http://www.repository.law.indiana.edu/fclj/vol59/iss3/6. Última fecha de consulta el 10 de octubre de 2018.

22 Tim Berners Lee es considerado como el padre de la *web* o *World Wide Web*, quien la concibió en 1989 originalmente como una malla (*mesh*) o sistema de información distribuida para enlazar contenidos y

imperceptibles, mientras que en el caso de aplicaciones más nuevas como lo fueron en su momento la telefonía por internet o la transmisión de video (*streaming*), un retraso podría ser considerado catastrófico, lo cual dio lugar a adoptar como solución justificada la priorización de cierto tipo de aplicaciones sensibles a los retrasos sobre otras que no lo fueran tanto, siendo éste, a su juicio, el tipo de discriminación desafortunada que la neutralidad de la red ha condenado.[23]

Por su parte, en un debate sobre este tipo de prácticas discriminatorias, Wu considera que el bloqueo de contenidos o servicios es el más claro ejemplo de ello hablando de neutralidad de la red, ya que en un extremo puede evitar que un producto mejor o más barato ingrese al mercado, como la voz sobre el protocolo de internet (por sus siglas en inglés, *voice over internet protocol, VoIP*) en relación con la telefonía tradicional y, a menudo, como ha sido el caso en los Estados Unidos e incluso en México, se evite por parte de los incumbentes el que dichos servicios se ofrezcan de una manera efectiva. Precisamente en eso radica el problema ya que, si uno piensa que la entrada en los mercados y la innovación están vinculados con el crecimiento económico de un país, tales prácticas obstaculizan su tasa de crecimiento, razón por la cual Wu considera que lo anterior es la justificación más fuerte para que existan reglas sobre neutralidad de la red.[24]

De acuerdo con Wu, la neutralidad de la red se ha convertido en una norma de conducta que determina lo que una persona o empresa puede o no puede hacer

---

hacerlos accesibles de modo compartido, lo anterior bajo el lenguaje HTML (*HyperText Markup Language*), el protocolo HTTP (*Hypertext Transfer Protocol)* y el URL (*Uniform Resource Locator*). Esto dio lugar a la creación de los primeros servidores web que permiten alojar páginas con contenidos de información, así como a los primeros navegadores. Actualmente Berners-Lee es miembro fundador de la fundación web, una organización internacional establecida en 2009 que busca promover la web abierta considerándola como un bien público y un derecho básico. A 30 años de la invención de la *web*, que hoy en día permite el acceso a una enorme cantidad de fuentes de información, Berners-Lee ha señalado en 2019 tres fuentes de disfuncionalidad entre las cuales destacan los modelos de negocio en línea basados en la publicidad poniendo en riesgo los intereses del usuario. En lo que se denomina "un contrato para la web" que refleje los principios de ésta compartidos por gobierno, empresas y usuarios, Berners-Lee y su fundación han considerado que debe mantenerse y preservarse el carácter abierto de la web, es decir, que se preserve esa comunidad global como un espacio libre y abierto en el que las empresas y el gobierno respeten el derecho de acceso completo a Internet de la personas así como la privacidad de los ciudadanos en línea y en la que éstos busquen preservar a la web como un recurso público global y abierto para cualquier persona, en el que cualquier participante pueda ser creador y colaborar con contenidos ricos e importantes. Véase https://fortheweb.webfoundation.org/principles/ y https://webfoundation.org/2019/03/web-birthday-30/, última fecha de consulta 14 de marzo de 2019.

23 *Ibidem,* p. 576.

24 *Idem.*

apropiadamente en Internet, considerando que éste debe ser abierto, exceptuando aquellos casos en los que, habiendo un propósito legítimo como lo es la protección de la red en sí misma, no debería haber discriminación ya sea en contra de una u otra forma de contenido, o bien, en contra de un proveedor u otro.[25]

Por su parte, la FCC consideró en 2010 que la apertura de Internet se encuentra expuesta a la amenaza en el sentido de que los proveedores de acceso a Internet de banda ancha bloqueen o degraden los contenidos y las aplicaciones, es decir, que actúen de manera discriminatoria, sin revelar sus prácticas a los usuarios finales ni a los proveedores de aplicaciones, servicios y contenidos,[26] no obstante los principios de internet abierto que fueron emitidos en 2005 por dicha autoridad.[27] Lo anterior se debe, de acuerdo a las consideraciones de la propia FCC que dieron lugar a la Orden de Internet Abierto de 2010, al hecho de que los proveedores de acceso a Internet que proveen servicios de telefonía y de televisión de paga tienen incentivos fuertes para bloquear contenidos en línea provistos a través de Internet que compiten con sus propios servicios; tal es la razón por la cual la FCC determinó en ese momento la necesidad de emitir las denominadas reglas de internet abierto.[28]

En consecuencia, se puede decir que el internet abierto es un concepto básico de la neutralidad de la red en virtud del cual se entiende que la información

---

25 Sommer, Jeff, *Defending the Open Internet*, New York Times, 10 de mayo de 2014, disponible en https://www.nytimes.com/2014/05/11/business/defending-the-open-internet.html, última fecha de consulta, 5 de septiembre de 2018.

26 En términos de la propia Orden de Internet Abierto de 2010 de la FCC, se entiende por usuario final a cualquier persona que utiliza el servicio de acceso a Internet de banda ancha, y el término proveedor de la orilla, conocido como *edge provider*, se refiere a cualquier contenido, aplicación o servicio o dispositivos de un proveedor, ya que estos últimos generalmente operan en la orilla y no en el núcleo o centro de la red. Se trata de términos que no son necesariamente mutuamente excluyentes puesto que un proveedor de acceso a Internet a su vez puede proveer sus propios contenidos, aplicaciones y servicios en Internet, así como un usuario final puede ser creador de contenidos. Véase Comisión Federal de Comunicaciones, *Preserving the Open*…, *cit., nota 1*, p. 59192.

27 Comisión Federal de Comunicaciones, *Preserving the Open*…, *cit.,* p. 59192.

28 En su voto disidente en contra de la aprobación de la orden de internet abierto 2010, la Comisionada Meredith Attwell Baker señaló que las prácticas descritas por la mayoría de los comisionados que aprobaron dicha Orden no son evidencia suficiente o generalizada de conductas anticompetitivas o abusivas que causen daños al consumidor, sino que se trata de incidentes aislados que no ameritaban la expedición de unas reglas de internet abierto. Véase Comisión Federal de Comunicaciones, *Report and Order in the matter of Preserving the Open Internet*, Washington, D.C., 2010, p. 18087, disponible en: https://docs.fcc.gov/public/attachments/FCC-10-201A1_Rcd.pdf

que circula a través de la red de Internet es igualmente libre y accesible para los usuarios que tienen acceso a ella, tal como ha sido reconocido por parte de la FCC a lo largo de los últimos años como se ha expuesto; en razón de ello, se verá cómo en el acceso libre a la información que se envía y recibe a través de Internet, el principio de transparencia se encuentra imbuido en cada aspecto de la política sobre Internet que esa autoridad ha emitido.

1.2 Transparencia de la información y privacidad de los consumidores en Internet

En el fondo de las prácticas descritas, ya sea que impliquen bloqueo de contenidos o degradación de los mismos o de la velocidad con que se transmiten, subyace siempre la importancia de la transparencia a la que se ha referido la Sociedad de Internet, pues muchas de ellas se cometen sin que los usuarios afectados tengan conocimiento de ello sino hasta que ya tuvieron lugar; si bien, tal como lo ha reconocido la autoridad regulatoria en los Estados Unidos, la transparencia garantiza la apertura característica de Internet, en ocasiones también se ha reconocido por la misma que no necesariamente es suficiente para ello como más adelante se tratará.

Aun cuando en los principios a que se refiere la Declaración de política de internet de la FCC de 2005, mediante los cuales se buscaba asegurar que los consumidores tuvieran derecho a acceder y usar en línea los contenidos, aplicaciones y dispositivos de su elección, no se hace referencia expresa a una regla sobre transparencia, la realización de los mismos implica que los usuarios tienen derecho a conocer la información relevante sobre el servicio provisto por parte de los operadores de red.

Fue hasta 2010, en las reglas de internet abierto de la FCC donde se definió por primera vez una regla de transparencia exigible tanto a los proveedores de banda ancha fijos como móviles en relación con la provisión de sus servicios. En el marco de una internet abierta, robusta y que funcione correctamente, esa autoridad también ha reconocido la necesidad de que los proveedores de banda ancha tengan flexibilidad para administrar razonablemente sus redes. En ese sentido, las prácticas

de gestión de red son razonables si son apropiadas y están diseñadas para lograr un propósito legítimo de gestión de red, sin embargo, por otro lado, la transparencia y el control del usuario final son "piedras de toque de razonabilidad".[29]

En el mismo cuerpo normativo la FCC aclaró que, a manera de orientación, proporcionaba una lista de qué tipo de información debía divulgarse y la manera de hacerlo en su caso, enfatizando la importancia de la flexibilidad de la regla y aclarando que una divulgación efectiva puede incluir todos o algunos de los tipos de información que enlistó como más adelante se verá.[30]

La transparencia y la capacidad de elección de los usuarios que aquí se menciona, junto con la seguridad de la información, son la base para la protección de la privacidad de los consumidores, tal como lo señaló la FCC en 2016. Mientras que, por un lado, el acceso a Internet es una "herramienta crítica" para los consumidores debido a que expande su acceso a enormes cantidades de información e incontables nuevos servicios, considerando que los proveedores de banda ancha son quienes proporcionan la vía de acceso a Internet, derivado de dicha función estos tienen, a su vez, acceso a una gran cantidad de información acerca de sus clientes, ya que tienen la posibilidad de conocer lo que éstos ven en línea, donde están físicamente ubicados, cuándo se conectan y cuánto tiempo permanecen en línea, qué dispositivos utilizan para tener acceso a Internet, qué sitios web visitan y qué aplicaciones utilizan.[31] Lo anterior ha sido la razón para que la FCC recurriera a la aplicación de reglas sobre confidencialidad, ya que, sin la adecuada protección a la privacidad, el uso o divulgación de información que los proveedores de banda ancha recopilan de sus clientes iría en contra de los intereses que subyacen a la privacidad de los individuos.[32] Como la propia FCC ha reconocido, no se trata de prohibir a los proveedores de banda ancha de utilizar o incluso compartir la información de sus clientes, sino de proteger la capacidad de

29 Comisión Federal de Comunicaciones, *Preserving the Open…*, *cit.,* p. 59193.

30 *Op. cit.,* pp. 59203-59204; p. 59211.

31 Comisión Federal de Comunicaciones, *Privacy Order, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Washington, D.C., 2016, p. 3, disponible en https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy. Última fecha de consulta 7 de enero de 2019.

32 *Idem.*

elección de los usuarios y que tengan conocimiento de ello mediante acciones de transparencia y ejerzan su consentimiento mediante herramientas adecuadas para ello respecto del tratamiento y uso que los proveedores de banda ancha hagan de su información confidencial.

Diversos actores interesados en proteger las actividades en línea que realizan los usuarios, en particular las asociaciones de consumidores, han reconocido que los proveedores de banda ancha representan un riesgo único y mucho más intenso para la privacidad de sus suscriptores, debido a los datos tan detallados y completos a los que tienen acceso en virtud de la provisión de sus servicios de banda ancha. Los datos de Internet transmitidos entre los suscriptores y los servicios en línea contienen una gran cantidad de información solo por lo que se refiere al enrutamiento utilizado para entregar esos datos a su destino. Al respecto, Public Knowledge[33] indica que:

> Los proveedores de acceso a internet de banda ancha que optan por participar en la práctica conocida como "inspección profunda de paquetes" tienen a su disposición una gran cantidad de información sobre sus suscriptores.
>
> Los proveedores pueden extraer, analizar y vender esta rica información de los consumidores a empresas de marketing y otros, y los suscriptores cuentan con pocos recursos técnicos para evitar esa actividad invasiva de la privacidad.

Existen numerosos ejemplos en los que los proveedores de banda ancha han realizado la recolección de datos e información de sus usuarios, desde adjuntar herramientas de rastreo de las transmisiones en línea realizadas por sus usuarios hasta incluso modificar páginas web a las que han tenido acceso sus suscriptores para incluir mensajes publicitarios, debido precisamente a que el mercado que representan los suscriptores que tienen acceso a internet es extremadamente valioso. Incluso, los proveedores de banda ancha tienen una ventaja superior sobre

33 Public Knowledge es una organización que promueve y protege los intereses de los consumidores en internet y que ha interactuado con diversas autoridades, como la FCC, entre otras, para lograr influir en la política pública del gobierno estadounidense en materia de telecomunicaciones e internet. La página oficial de Public Knowledge está disponible en línea en: https://www.publicknowledge.org/

los dueños de las páginas web o de otros proveedores de servicios en línea como los denominados *edge providers*, ya que los primeros reciben y tienen conocimiento de toda la información en línea que realizan sus usuarios y prácticamente parecería que la única forma que tienen éstos de evitar que recolecten su información es desconectarse de Internet.[34]

Incluso en relación con lo anterior, se tiene cuenta de numerosas prácticas en virtud de las cuales empresas, consideradas como terceras partes, rastrean los hábitos de navegación de los individuos que, a través de sus dispositivos móviles, tienen acceso a alguna página web de su interés o hacen uso de aplicaciones móviles con el fin de enviarles en línea publicidad dirigida no solicitada. Tales usuarios son clientes de algún proveedor de acceso a Internet o simplemente tienen acceso a una determinada página o sitio web, considerados como primera parte o dueños de la información, en la que a su vez aparecen una gran cantidad de anuncios publicitarios de terceras partes.[35] Dado que el historial de navegación por internet se encuentra inextricablemente ligado con información personal ello causa preocupaciones en torno a la privacidad de las personas que pueden sufrir un daño en este contexto.

Al respecto, Jonathan R. Mayer[36] ha hecho referencia a los diversos puntos de vista que existen en relación con la política que debe seguirse en cuanto al rastreo en línea por parte de terceras personas. Si bien todos los actores involucrados están de acuerdo en que son los consumidores quienes deberían tener cierto grado de control sobre el seguimiento en línea de sus actividades, existen especificidades en relación al alcance de dicho control. Así, según explica el autor citado, los hacedores de políticas y los defensores de los consumidores consideran que éstos deberían tener control en cuanto a la recopilación de la información

34 Public Knowledge, *Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World*, Washington, D.C., 2016, pp. 4-5, disponible en https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper.pdf. Última fecha de consulta 1 de marzo de 2019.

35 Mayer, Jonathan R. y Mitchell, John C., *Third Party Web Tracking. Policy and Technology*, Foro Mundial sobre Seguridad y Privacidad del Instituto de Ingenieros Eléctricos y Electrónicos, California, 2012, Disponible en https://jonathanmayer.org/publications/trackingsurvey12.pdf, Última fecha de consulta el 1 de marzo de 2019.

36 *Op. cit.*, Nota 35.

derivada de dicho rastreo, en tanto que los grupos que representan a empresas de publicidad en línea han argumentado que el control debería extenderse únicamente a ciertos usos específicos de la información y no a todos. Así, los primeros consideran que el no seguimiento debe ser el punto de partida, mientras que los segundos consideran que el rastreo debería serlo. En cuanto al diseño del mecanismo de elección, los grupos que representan a las empresas de publicidad en línea consideran que son ellos quienes deberían controlar el diseño de tal mecanismo, en tanto que los hacedores de políticas y los defensores de los consumidores consideran que los proveedores de navegadores son quienes deben mantener la responsabilidad en cuanto a dicho diseño.

De hecho, cada punto de vista varía de acuerdo a las prioridades que subyacen en función de sus intereses. Así, algunos defensores de consumidores y hacedores de políticas, principalmente en Europa, consideran que la privacidad en línea es un derecho humano fundamental; otros, incluyendo hacedores de políticas en los Estados Unidos, consideran que la elección del consumidor en cuanto a los riesgos que el seguimiento en línea comporta a la privacidad, constituye un medio para maximizar la riqueza. De hecho, es interesante el punto de vista de las empresas de publicidad en línea y los sitios web de terceras partes que han defendido sus prácticas de rastreo con base en argumentos de carácter económico en el sentido de que el subsidio que reciben los usuarios por el acceso al contenido en internet de manera gratuita compensa o supera los riesgos a la privacidad de los consumidores.

Por otra parte, Mayer incluso ha citado diversas encuestas realizadas a lo largo de varios años, en virtud de las cuales, los usuarios han manifestado oposición a que terceras partes, que no están relacionadas con la página web que visitan, recolecten sus datos y hagan uso de los mismos en virtud de su actividad en la red.

Por lo que se refiere a los proveedores de internet de banda ancha, debido al riesgo que siempre[37] han representado en relación con la información de sus

37 *Op.cit.,* Nota 34*,* pp. 21-22. Tal es el caso de los operadores de televisión por cable a que se refiere Public Knowledge y que son importantes proveedores de banda ancha en la medida en que sus servicios están empaquetados, de modo que tanto sus competidores como sus suscriptores tienen preocupaciones legítimas

usuarios a la que tienen acceso, la FCC se ha preocupado por vigilar, investigar y sancionar dichas prácticas con base en el marco normativo vigente en el momento en que se comete alguna práctica que pueda considerarse atentatoria de la apertura en internet o de alguna de sus reglas y que en el siguiente capítulo se expone con detalle para entender el contenido obligacional tanto del concepto de transparencia como el de confidencialidad. Más allá de la autoridad competencial y legal que tiene la FCC para investigar este tipo de prácticas, resulta fundamental la presión que ejercen normalmente en este tipo de casos las organizaciones de la sociedad civil, las cuales influyen o pueden influir en la decisión de la autoridad reguladora toda vez que fungen como un complemento o contrapeso importante para la primera.

Así, como podrá observarse, en un contexto de la sociedad de la información, la cual hace más de 20 años se consideraba aún como emergente, en la que internet ha sido su exponente principal[38] gracias al crecimiento exponencial que ha tenido (no solo debido a la proliferación en cuanto al número de usuarios y a su presencia generalizada en todos los sectores de la producción y en las actividades, sino debido al enorme auge de los contenidos que a finales del siglo XX se predicaba como algo todavía en ciernes), surge la cuestión de si la transformación que conlleva el uso de Internet en la sociedad así como en las relaciones humanas y en los negocios, incluyendo los relativos a publicidad, resulta benéfica o no.

de que los datos de éstos se compartan con sus filiales de banda ancha sometiendo a sus clientes a prácticas invasivas de publicidad.

38 Como indica Pisanty, quien a su vez cita al español Manuel Castells: *Internet no es la sociedad de la información ni del conocimiento pero sí es la tecnología paradigmática de esta etapa de desarrollo de la humanidad. Op.cit.,* Nota 7, p. 53.

Capítulo 2

Marco Normativo de la neutralidad de la red en los Estados Unidos

Capítulo 2: Marco Normativo de la neutralidad de la red en los Estados Unidos.

2.1 Las reglas de internet abierto de la Comisión Federal de Comunicaciones de los Estados Unidos.

En el marco de las Reglas de Internet Abierto emitidas en 2010 por la autoridad regulatoria en materia de telecomunicaciones en los Estados Unidos de América, se buscaba proteger la apertura en internet en varios sentidos haciendo valer al menos tres principios,[39] entre los cuales destaca la transparencia en las prácticas de gestión y manejo del tráfico de Internet por parte de los proveedores del servicio de acceso a Internet, así como respecto de los términos y condiciones comerciales y técnicos bajo los cuales prestan el servicio de banda ancha a sus clientes.

Bajo el concepto de apertura en internet se busca salvaguardar en beneficio de los usuarios de internet principalmente tres características del servicio de banda ancha de Internet: el acceso a servicios, contenidos y aplicaciones sin limitaciones o restricciones no discriminatorias; su derecho a elegir los servicios, aplicaciones y contenidos de su preferencia, lo que implica el control del usuario final sobre sus actividades en línea, así como la transparencia en relación con el servicio que les es provisto por los ISP.

Cuando fueron emitidas las reglas de Internet abierto en 2015 por la FCC[40] se prohibió a los ISP el bloqueo de contenidos, la priorización pagada, la ralentización[41] y se mejoraron los requisitos de transparencia en beneficio de los

---

39 Actualmente en virtud de las nuevas Reglas de Internet Abierto de la FCC emitidas en diciembre de 2017, se anularon los principios de no bloqueo y no discriminación que estuvieron vigentes bajo las reglas de neutralidad de la red de 2010 y 2015, dejando vigente únicamente el principio de transparencia considerada por el órgano regulador como regla suficiente para proteger la apertura en Internet en beneficio de los usuarios. Véase Comisión Federal de Comunicaciones, *Federal Register*, "Restoring Internet Freedom; Final Rule", Vol. 83, No. 36, febrero 2018, p. 7852 disponible en https://www.federalregister.gov/documents/2018/02/22/2018-03464/restoring-internet-freedom, Última fecha de consulta el 23 de diciembre de 2018.

40 En virtud de las cuales se reclasificó el servicio de banda ancha como un servicio de telecomunicaciones sujeto al título II de la Ley de Comunicaciones.

41 El término ralentización corresponde al anglicismo *"throttling"*, práctica que se define en el sentido de que los ISP no deben degradar ni afectar el tráfico legal de Internet sobre la base de contenidos, aplicaciones o servicios en Internet, o el uso de dispositivos no dañinos. *Op. cit.*, Nota 16, p. 19740.

usuarios finales y de los *edge providers* haciendo notar esa autoridad que aun surgían preocupaciones importantes sobre las políticas de privacidad y el uso de datos por parte de los ISP.

En ese sentido bajo las Reglas de 2015, los ISP estaban obligados a divulgar tarifas promocionales, así como todas las tarifas y recargos e incluir en sus términos y condiciones de servicio información específica sobre todos los límites de datos o subsidios. Asimismo, con el objeto de que los usuarios estén mejor informados, se estableció que los ISP deben incluir información relativa a la pérdida de paquetes como una medida relacionada con el desempeño de la red. Los clientes deben ser notificados cuando una práctica de red pueda impactar significativamente el uso de acceso a Internet.[42]

2.1.1 La obligación de transparencia para los proveedores del servicio de acceso a internet de banda ancha

En diciembre de 2010 cuando se liberaron las Reglas de Internet Abierto de la FCC, la obligación de transparencia se hizo exigible no solo a los operadores fijos de banda ancha sino también a los operadores móviles de banda ancha respecto de los cuales se consideró en ese momento que se encontraban en una etapa temprana de desarrollo en relación con los primeros pero reconociéndose por parte de esa autoridad reguladora que estaban evolucionando de una manera muy rápida.[43] Así también se consideró que dicha regla de transparencia incluía obligaciones de divulgación en relación con los procesos de aprobación y certificación de dispositivos y aplicaciones móviles. Más allá de lo anterior, lo fundamental es que, debido a varias denuncias en contra de proveedores de banda ancha, respecto de las cuales la FCC recabó evidencia en su contra, en el sentido de que ralentizaban, priorizaban o bloqueaban a sus usuarios el tráfico de internet, dicha autoridad observó que tales preocupaciones, tanto por parte de los usuarios finales como de los *edge providers*, se debían particularmente a la falta de

42 *Op. cit.,* nota 16, p. 19741.
43 *Op. cit.,* nota 14, p. 59224.

transparencia.[44] De modo que, con el fin de preservar la apertura de internet y, simultáneamente, la capacidad de los proveedores de banda ancha de administrar y expandir sus redes, la FCC decidió adoptar en 2010 las reglas de internet abierto bajo cuatro principios torales: transparencia, no bloqueo, no discriminación irracional y administración de la red de manera razonable. Como se mencionó líneas arriba, en 2015 se añadió la prohibición de ralentizar el tráfico de internet y de priorización pagada y se mejoraron los requisitos de transparencia.

2.1.2 Análisis de la sección 8.3 de las Reglas de Internet Abierto

El artículo 8.3 de las Reglas de Internet Abierto de 2010 de la FCC establece el deber a cargo de los proveedores del servicio de acceso a internet de banda ancha de divulgar públicamente información precisa en relación con las prácticas de gestión y desempeño de la red, así como los términos comerciales bajo los cuales sea provisto dicho servicio de manera suficiente a efecto de que, por un lado, los consumidores tomen decisiones informadas en relación con el uso de dichos servicios y, por el otro, los proveedores de contenido, aplicaciones y servicios (*edge providers*) y proveedores de equipos puedan desarrollar, comercializar y mantener ofertas en Internet.[45] Es decir, dicha disposición protege tanto a los usuarios finales del servicio como a otros proveedores de servicios en internet que dependen del servicio de banda ancha por las razones que ya se han comentado en el sentido de que la FCC ha considerado que ambos extremos de esta plataforma[46] deben ser protegidos.

---

44 *Op. cit.,* nota 14, p. 59199.

45 "**§ 8.3 Transparency.** A person engaged in the provision of broadband Internet access service shall publicly disclose accurate information regarding the network management practices, performance, and commercial terms of its broadband Internet access services sufficient for consumers to make informed choices regarding use of such services and for content, application, service, and device providers to develop, market, and maintain Internet offerings." (Traducción propia). *Op. cit.,* Nota 14, p. 59232.

46 De hecho, se considera a Internet como una plataforma o mercado de dos lados en el que ambos extremos (usuarios y *edge providers*) pueden beneficiarse del acceso a Internet. Véase además Jean Tirole en el estudio que hace sobre los **efectos de red** en internet considerando a los consumidores, por un lado, y a los desarrolladores de software y publicistas, por el otro. Véase Rochet, Jean-Charles y Tirole, Jean, "Two Sided Market: a progress report", *The Rand Jornal of Economics*, volumen 37, número 3, septiembre 2006, pp. 645-667, disponible en https://www.researchgate.net/publication/227651905_Two-sided_Markets_A_Progress_Report, Última fecha de consulta 7 de diciembre de 2018.

Cabe indicar que con motivo de la emisión de las Reglas de internet abierto de 2015, la FCC señaló que todos los proveedores de acceso a internet, incluyendo los pequeños, permanecen sujetos a la regla de transparencia establecida en el numeral 8.3 de las Reglas de 2010,[47] de modo que la misma permaneció vigente y no fue modificada en 2015.

En 2010 la FCC estableció a modo de guía el tipo de información a ser divulgada en relación con las prácticas de desempeño y administración de la red y los términos y condiciones comerciales de los proveedores del servicio de acceso a Internet. Así, por ejemplo, en relación con las características de desempeño de la red, la FCC especificó, entre otros aspectos, el deber de divulgar la velocidad de acceso y latencia esperadas y reales, así como el impacto de servicios especializados. Se requirió que todas las divulgaciones fueran hechas de manera oportuna y visiblemente destacada, en un lenguaje simple y accesible para los actuales y futuros usuarios así como para los *edge providers*, la FCC y terceras partes (tales como las asociaciones que defienden los intereses de los consumidores, denominadas *consumer watchdogs)* que deseen monitorear las prácticas de administración de la red en relación con posibles violaciones a los principios de internet abierto.[48] Por lo que se refiere a los términos comerciales, dentro de los cuales se consideran a las políticas de privacidad, la FCC indicó que los ISP deben divulgar, por ejemplo, si sus prácticas de administración y manejo de la red conllevan inspección del tráfico y si dicha información es almacenada, o utilizada por el operador para propósitos no relacionados o distintos a la administración de la red.[49]

Como se mencionó, las reglas de internet de 2015 dejaron vigente el texto de la regla de transparencia adoptado por primera vez en 2010 por la FCC, sin embargo, se mejoraron algunos requisitos como lo es el relativo a la precisión de la información a divulgarse previsto en el numeral 8.3 ya citado, en el sentido de que debe mantenerse actualizada la información de modo que, cada vez que ocurra un

47 *Op. cit.,* Nota 16, p. 19763.
48 *Op. cit.,* Nota 14, p. 59203.
49 *Ídem.*

cambio sustancial en los términos comerciales, las prácticas de red o las características de desempeño del servicio, el proveedor tiene la obligación de actualizar la información de forma que la divulgación de la misma sea oportuna y de manera visiblemente destacada para los usuarios. Al respecto, la FCC no adoptó un plazo específico para llevar a cabo la actualización de la información después de ocurrido el cambio material (este último entendido como cualquier cambio que un consumidor o proveedor de servicios, contenidos y aplicaciones razonable consideraría importante para tomar una decisión sobre el proveedor, servicios o aplicaciones que deseen elegir).[50]

2.2 La protección de la privacidad de los consumidores de los servicios de acceso a internet de banda ancha

La protección a la privacidad de los consumidores se hace necesaria en un entorno como el de Internet debido a que la información se disemina y comparte fácilmente y en grandes cantidades, así como al hecho de que son los proveedores de banda ancha quienes proporcionan la vía de acceso a Internet y se encargan del tráfico que se genera con motivo de ello, lo que significa que, tratándose de actividades en línea que no estén cifradas o encriptadas, tienen una vista sin obstrucciones que les permite conocer las aplicaciones que utiliza un usuario, los sitios web que visita, así como las veces y las fechas en que realiza una actividad en línea. De acuerdo con la FCC, los proveedores de acceso a internet, debido a su condición de *gatekeepers*, ocupan una posición única dentro del ecosistema de Internet ya que a través de ellos se transporta toda la actividad en línea de los consumidores, dentro de la cual se encuentra una gran cantidad de información personal. En particular, dicha agencia regulatoria ha considerado que no basta que la información que manejamos en línea esté encriptada ya que, aun así, los proveedores de acceso a internet pueden ver los sitios web que un cliente visita, qué tan a menudo los visita,

50 *Op.cit.,* Nota 16, p. 19760.

así como el tiempo que invierte en cada sitio en línea.[51] Incluso si un usuario utiliza un dispositivo móvil, su proveedor de acceso a internet podría rastrear en tiempo real las actividades físicas y en línea que realiza.[52] Es por ello que la FCC, como resultado de haber reclasificado en 2015 el servicio de acceso a internet de banda ancha como un servicio de telecomunicaciones y no de información,[53] consideró que necesariamente el artículo 222 de la Ley de Comunicaciones de 1934, que impone obligaciones a los proveedores de servicios de telecomunicaciones para proteger la información que obtengan de sus usuarios con motivo de la prestación del servicio, debe aplicar asimismo a los proveedores de dicho servicio ya que éstos son un conducto necesario para la transmisión de la información entre un usuario de Internet y los sitios de internet que visita, o bien, entre uno y otros usuarios de internet, por lo que están en condiciones de obtener una gran cantidad de información personal y propietaria de sus clientes que debe ser protegida. Tal es la razón también por la que la FCC no tuvo la intención de que la regulación en materia de privacidad aplique a los *edge providers* o a los sitios web, puesto que éstos no cuentan con la visibilidad que sí tienen los ISP de manera detallada respecto de la información relativa al comportamiento en línea de un cliente, incluyendo una gran cantidad de información personal, aun cuando esté encriptada.[54] Es importante señalar además que la FCC cuando reclasificó el servicio de acceso a internet en 2015 como un servicio de telecomunicaciones, reconoció que no se trataba de

51 *Cfr.,* Swire, Peter, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, The Institute for Information Security & Privacy at Georgia Tech, 2016, p. 23, disponible en http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf. Última fecha de consulta: 23 de noviembre de 2018.

52 Véase el documento *Additional Questions for the Record* que contiene las respuestas que el ex-presidente de la Comisión Federal de Comunicaciones, Tom Wheeler, dio en relación con la audiencia que tuvo lugar en mayo de 2016 ante el subcomité de Privacidad, Tecnología y Derecho del Senado de los Estados Unidos en una audiencia titulada "Examining the Proposed FCC Privacy Rules". Disponible en: https://www.judiciary.senate.gov/imo/media/doc/Wheeler%20Responses%20to%20QFRs.pdf. Última fecha de consulta el 6 de diciembre de 2018.

53 Al haberse reclasificado el servicio de banda ancha como un servicio de telecomunicaciones se considera que el mismo debe estar sujeto a las obligaciones impuestas a los transportistas comunes (*common carriers),* dentro de los cuales se encuentran los proveedores de servicios de telecomunicaciones. Dichas obligaciones se encuentran en el Título II de la Ley de Comunicaciones de 1934, entre las cuales destaca la relativa a la protección de la confidencialidad de la información de los consumidores contenida en el artículo 222.

54 *Op.cit.,* Nota 52, p. 9.

regular internet *per se*, o los contenidos o aplicaciones en internet como tales, sino que, por el contrario, su reclasificación únicamente implicaba el componente de transmisión del servicio de acceso a internet. Así, según esa agencia regulatoria, al igual que en el servicio de telefonía, *"los consumidores tienen las mismas expectativas de privacidad que cuando utilizan redes de internet de banda ancha, la red de comunicaciones del siglo XXI. Adicionalmente, un gran porcentaje de consumidores recibe el servicio de acceso a internet de compañías que tradicionalmente les han proporcionado el servicio de telefonía (como AT&T y Verizon). Los consumidores han confiado en estos proveedores de comunicaciones para mantener su información de comunicaciones de manera privada y segura durante décadas, por lo que esa confianza no debería cambiar solo porque están utilizando el servicio de acceso a internet de banda ancha*".[55] Lo anterior se considera que resulta absolutamente consistente puesto que lo se busca es proteger la privacidad dependiendo no tanto de la plataforma tecnológica o del tipo de información transmitida, sino de quién recolecta la información; a quién o cómo es transmitida y con qué fines.

En este apartado es importante destacar, por un lado, el ámbito material de protección de las regulaciones en materia de privacidad en línea en los Estados Unidos, así como, por el otro, el ámbito competencial de la autoridad que puede intervenir para la defensa de la privacidad de los usuarios en Internet. Así, por lo que se refiere al ámbito de protección de privacidad que se da en los Estados Unidos de América, a diferencia del Reglamento General de Protección de Datos[56] que aplica directamente a todos los Estados miembros de la Unión Europea respecto de

55 *Íbidem,* p. 11. En el original se lee: *"Consumers have the same expectations of privacy when using broadband internet networks, the communications network of the 21st Century. Additionally, a large percentage of consumers receive internet access service from companies that have traditionally provided them telephone service (such as AT&T and Verizon). Consumers have relied upon these communications providers to keep their communications information private and secure for decades. That reliance should not change just because they are using BIAS."* (Traducción propia).

56 El Reglamento General de Protección de Datos europeo entró en vigor a partir del 25 de mayo de 2018 y sustituyó a la Directiva 95/46/CE de Protección de Datos de 1995. Publicado en el Diario Oficial de la Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Última fecha de consulta 16 de diciembre de 2018.

cualquier actividad que implique el tratamiento de datos de carácter personal de las personas físicas (incluidas las actividades en línea), en los Estados Unidos de América algunos sectores específicos de la industria cuentan con su propio régimen jurídico en materia de privacidad, como es el caso de las instituciones financieras o agencias de información crediticia, de instituciones de salud o educativas, así como el caso del sector de las telecomunicaciones, incluidos los servicios de banda ancha, en este último caso hasta 2017 (Cuadro 1).

En cuanto al ámbito competencial en materia de protección a la privacidad, tanto la Comisión Federal de Comercio (en adelante FTC, por sus siglas en inglés) como la FCC, han intervenido para hacer valer la regulación aplicable en beneficio de los consumidores. Mientras que la primera es una agencia con jurisdicción amplia que se encarga de perseguir, con base en la autoridad que le otorga el artículo 5 de la Ley de la Comisión Federal de Comercio, actos o prácticas desleales de competencia por parte de empresas así como actos o prácticas desleales o engañosos, en o que afecten el comercio,[57] e incluso contra aquellas que no cumplen sus promesas de privacidad o que carecen de prácticas de seguridad razonables respecto de información sensible de los consumidores,[58] la FCC cuenta a nivel federal con autoridad de manera exclusiva para regular el tratamiento de datos de carácter personal que los operadores de telecomunicaciones obtengan de sus clientes en virtud de la provisión de sus servicios de telecomunicaciones.[59] Lo anterior se debe a que el artículo 5 de la Ley de la FTC explícitamente excluye a la Comisión Federal de Comercio de la posibilidad de ejercer cualquier autoridad o acción en contra de los transportistas comunes (*common carriers*) como lo son los proveedores de servicios de telecomunicaciones sujetos a la Ley de

57 Actualmente el artículo 5 (a)(1) de la Ley de la Comisión Federal de Comercio indica en su idioma original*: Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.* Véase United States Code, 2017, 15 U.S.C. § 45(a)(1), p.40, Disponible en https://www.govinfo.gov/content/pkg/USCODE-2017-title15/pdf/USCODE-2017-title15.pdf, Última fecha de consulta el 23 de noviembre de 2018.

58 Comisión Federal de Comercio, Privacy and Security Enforcement. Disponible en: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement. Fecha de consulta: 23 de noviembre de 2018.

59 *Op.cit.,* Nota 31, pp. 157-158.

Comunicaciones de 1934 y, en consecuencia, a la autoridad competencial de la FCC.[60]

Por lo que se refiere a los servicios de internet de banda ancha (los cuales son provistos en varios casos por empresas que tienen a su vez la calidad de operadores de telecomunicaciones, como es el caso de AT&T, Verizon o Sprint, entre otros), la FCC también ha gozado de autoridad de manera exclusiva para proteger a los usuarios de estos servicios contra actos que atenten contra la confidencialidad de su información. A su vez, tratándose de servicios provistos por los *edge providers*, éstos no se encuentran sujetos a la jurisdicción de la FCC sino de la FTC, de modo que cuando un usuario en virtud de sus actividades en línea tiene acceso al sitio de internet de un proveedor de contenidos o de alguna aplicación (por ejemplo, leer noticias en la página web del *Washington Post*, o ver un programa de *Netflix* a través de la aplicación en línea correspondiente) las actividades de éste serán regidas por la FTC puesto que no se tratan de operadores que provean servicios de telecomunicaciones (*common carriers*) sino que solo proveen contenidos y servicios (noticias, entretenimiento) en línea a los cuales se tiene acceso a través de un ISP.

Cabe resaltar al respecto la necesidad de contextualizar en este apartado la problemática de la privacidad en internet de los usuarios debido a los constantes cambios que han ocurrido en la legislación americana con motivo de este tema y de la neutralidad de la red. La FCC siempre ha regulado las actividades de los *common carriers* de conformidad con la Ley de Comunicaciones de 1934. Como se mencionó anteriormente,[61] en 2015 dicha autoridad decidió reclasificar el servicio de internet de banda ancha como un servicio de telecomunicaciones, el cual era considerado antes de ese año como un servicio de información sujeto a las disposiciones del Título I de la Ley de Comunicaciones de 1934, consideradas como menos estrictas que las aplicables a los *common carriers* bajo el Título II del mismo ordenamiento.

---

60 Al tenor del artículo 5 de la ley de la Comisión Federal de Comercio, los *common carriers* se encuentran exentos de la jurisdicción y aplicación de las leyes de la FTC, el cual dispone que esta agencia tiene autoridad para perseguir *"unfair or deceptive acts or practices in or affecting commerce ..., except… common carriers subject to the Acts to regulate commerce." Op.cit.,* Nota 57. Véase 15 U.S.C. § 45(a)(1), (2). No obstante, a partir de 2018, los ISP se encuentran sujetos a la autoridad de la FTC.

61 *Op.cit.*, Nota 53.

En ese momento, la FCC decidió dejar de aplicar a los ISP algunas disposiciones del Título II por considerarlas demasiado estrictas con excepción, entre otras, de las relativas a la confidencialidad de la información contenidas en el artículo 222 de la Ley citada.

Actualmente con motivo de la emisión de las reglas de internet abierto en diciembre de 2017,[62] la FCC reclasificó nuevamente el servicio de internet de banda ancha como un servicio de información, de modo que los ISP no se encuentran sujetos a las disposiciones contempladas en el artículo 222 que regula la confidencialidad de la información y que forma parte del Título II de la Ley citada.

Al momento de la investigación realizada por la FCC en contra de Verizon, los hechos objeto de la investigación, descritos en el Capítulo III de este trabajo, ocurrieron antes de la entrada en vigor de la orden de internet abierto de 2015. No obstante, la FCC al momento de cerrar la investigación consideró que Verizon había violado el artículo 222 de la Ley de Comunicaciones junto con la regla de transparencia establecida en el numeral 8.3 de las reglas de internet abierto, según se verá en el apartado correspondiente del capítulo siguiente.

2.2.1 Análisis de la sección 222 de la Ley de Comunicaciones de 1934

El artículo 222 de la Ley de Comunicaciones de 1934 regula a todos los operadores de telecomunicaciones, incluyendo los proveedores de servicios de acceso a Internet de banda ancha, en cuanto al uso, divulgación y protección de información propietaria que obtengan con motivo de la prestación de sus servicios. Inicialmente el contenido de dicho artículo fue creado para su aplicación a los servicios de telecomunicaciones como la voz y la telefonía; no obstante, la FCC lo ha aplicado en virtud de la convergencia de servicios a proveedores de servicios de televisión restringida por cable, así como a proveedores de servicios de acceso a internet de banda ancha con el fin de que se proteja la privacidad de la información de los clientes. Esta disposición legal permite que los clientes, en adición a cualquier otra protección legal que puedan tener en su calidad de consumidores frente a otras

62 Véase Nota 38.

autoridades,[63] reclamen la protección a su privacidad con motivo de la contratación de servicios de acceso a internet a un proveedor de servicios de banda ancha y las prácticas de publicidad que no hayan sido consentidas y, por lo mismo, resulten intrusivas.

Uno de los principios que subyacen al artículo 222 de la Ley de Comunicaciones es asegurar que los usuarios tengan la capacidad de mantener el control sobre su propia información aunque también tiene por objeto promover la competencia protegiendo la información propietaria de los competidores ya que establece un deber general de proteger la información propietaria tanto de clientes como de otros operadores de telecomunicaciones; lo anterior se verificará en subsiguientes apartados incluyendo lo relativo a la necesidad de obtener válidamente el consentimiento del usuario para el uso de su información en ciertos casos. Es así que, no obstante que son los operadores quienes tienen el control sobre las redes, se busca que los usuarios sean quienes tengan el control sobre su propia información, tomando como base el principio de transparencia que debe tener como objetivo no afectar a los usuarios ni crear efectos anticompetitivos hacia el resto de agentes involucrados.

En particular, dicho artículo 222, intitulado “Privacidad de la Información del Cliente”, impone la obligación a todos los operadores de telecomunicaciones de proteger la información propietaria de sus clientes y de utilizarla únicamente para propósitos autorizados.

El artículo 222 (a) exige a los operadores de telecomunicaciones (incluidos los proveedores de servicios de banda ancha) como deber fundamental que se

63 Como es el caso de la Comisión Federal de Comercio (*Federal Trade Commission*). Actualmente bajo las reglas de internet abierto vigentes, emitidas por la FCC en diciembre de 2017, se estableció la necesidad de restaurar la autoridad de la FTC para vigilar también las prácticas de privacidad por parte de los ISP; lo anterior como resultado de haberse reclasificado el servicio de internet de banda ancha como un servicio de información. Véase Nota 38. Sin embargo, considero que, si bien actualmente la FTC tiene competencia para vigilar y sancionar las prácticas engañosas por parte de las corporaciones en materia de comercio, habrá que ver en los próximos años, en el corto y mediano plazo, en virtud de violaciones que puedan tener lugar si resulta conveniente que la FCC, como agencia especializada en el sector de las telecomunicaciones, es quien deba mantener competencia exclusiva en este rubro relativo a la privacidad.

proteja la confidencialidad de la información propietaria de, o relacionada con un cliente.[64]

La sección 222 (b) concretamente protege a los operadores de prácticas anticompetitivas mediante la imposición del requisito de confidencialidad de la información propietaria del operador, ya que prohíbe expresamente a los operadores que obtienen información propietaria de otros operadores para la provisión de servicios de telecomunicaciones, de usar dicha información para un propósito distinto. Es decir, los operadores que reciben u obtienen información propietaria de otro operador para propósitos de prestar cualquier servicio de telecomunicaciones deberán utilizar dicha información únicamente para dicho fin y no para sus propios esfuerzos de publicidad.[65] No obstante que así no se prevé en la disposición legal en comento, debiera considerarse como una violación al artículo 222 (b) el hecho que un proveedor de acceso a Internet comparta la información propietaria de sus clientes incluso entre sus afiliadas.

Por su parte, la sección 222(c) define un tipo específico de información propietaria denominada "información de red propietaria del cliente" (CPNI, por sus siglas en inglés), la cual se encuentra definida en el artículo 222(h)(1). Este artículo 222(c) en su apartado (1) protege información de red propietaria del cliente individualmente identificable y establece que, a no ser que se cuente con la aprobación del cliente, un operador de telecomunicaciones que recibe u obtiene CPNI con motivo de la provisión de un servicio de telecomunicaciones, únicamente podrá utilizar o divulgar dicha información para la prestación del servicio del cual deriva dicha información, o bien, para servicios necesarios para, o utilizados en, la provisión de dicho servicio, incluyendo la publicación de directorios.[66] Como podrá

64 Véase United States Code, 2017, Title 47 U.S.C. § 222(a), p.55 La disposición completa señala lo siguiente en el idioma original: *"Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."* Disponible en https://www.govinfo.gov/content/pkg/USCODE-2017-title47/pdf/USCODE-2017-title47.pdf. Última fecha de consulta 30 de noviembre de 2018.

65 *Ídem.*

66 *Ídem.* En el idioma original, la disposición completa prevé lo siguiente: *"222(c) Confidentiality of customer proprietary network information (1) Privacy Requirements for telecommunications carriers. Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only*

apreciarse, si bien el lenguaje de la disposición señalada remite al servicio telefónico, la FCC consideró que a través de la misma bien se pueden proteger las necesidades o expectativas de privacidad de los clientes en relación no solo con los registros de sus llamadas sino cualquier información que se considere propietaria e individualmente identificable,[67] mediante el requisito de confidencialidad de la CPNI. Es decir, que sin importar la tecnología o si el servicio es de telefonía fijo o móvil, o bien, es un servicio de banda ancha de Internet, el requisito exigible a los operadores no es otro más que obtener el consentimiento del cliente antes de utilizar, compartir, divulgar o permitir el acceso a información propietaria del cliente identificable individualmente.

El término "información de red propietaria del cliente" o CPNI se refiere a la información relacionada con la cantidad, configuración técnica, tipo, destino, ubicación y cantidad de uso de un servicio de telecomunicaciones a la que se encuentra suscrito cualquier cliente de un proveedor de telecomunicaciones y que se hace disponible al operador únicamente por virtud de su relación con el cliente.[68] Es decir, al ser definida la CPNI en la Ley de Comunicaciones como aquella información que se hace disponible a los operadores solo en virtud de su relación comercial con el cliente (como por ejemplo, el tipo de servicio al que se encuentra suscrito el cliente, así como cierta información contenida en las facturas), significa que la información propietaria efectivamente es información que una persona posee de manera exclusiva, es decir, con exclusión de otros sujetos, de modo que si otros

---

use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories." (traducción propia). Recordemos que el artículo 222 de la Ley de Comunicaciones de 1934 inicialmente fue creado para regular los servicios de telefonía, razón por la cual hace referencia a los directorios telefónicos que incluyen datos personales de los clientes de proveedores de dicho servicio.

67 *Op.cit.,* Nota 31, p.142.

68 *Op.cit.*, Nota 64, p. 56. El artículo 222(h)(1) del título 47 del Cadge de los Estados Unidos (*U.S.C.*) que en el idioma original indica: "*the term ''customer proprietary network information'' means (a) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (b) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier*."

pueden acceder a esa información y utilizarla para sus fines comerciales pues ya no es propietaria, con o sin consentimiento del usuario.

Finalmente, el apartado 222(f) de la Ley de Comunicaciones de 1934 requiere, para los propósitos del apartado 222(c)(1), que el proveedor de acceso a internet de banda ancha obtenga la autorización previa y expresa del cliente para el uso o divulgación de datos o información relativa a la localización geográfica del usuario.[69]

Cabe señalar que al amparo del artículo 222 de la Ley de Comunicaciones de 1934 y a fin de implementar de un modo más específico su contenido, la FCC emitió en noviembre de 2016 una orden para regular la privacidad exclusivamente en el contexto de la provisión de servicios de internet de banda ancha (Orden de Privacidad).[70] Esta orden nunca entró en vigor puesto que fue anulada por el congreso estadounidense en abril de 2017[71] prohibiendo a la FCC emitir una regla substancialmente similar como la que fue anulada.[72] No obstante, bajo la Orden de Privacidad, la FCC llegó a establecer a modo de guía, tratándose de servicios de banda ancha, algunos elementos de información que pueden ser considerados como CPNI. Originalmente, en virtud de que el artículo 222 de la multicitada ley fue concebido para la protección de la privacidad bajo el contexto de los servicios de telefonía provistos por los operadores de telecomunicaciones, la FCC ha considerado como CPNI el detalle de los registros de las llamadas (los números telefónicos de la persona llamante y de la que recibe la llamada, la duración y frecuencia de las mismas), así como cualquier servicio adicional adquirido por el

69 *Op.cit.*, Nota 64, p.55. Como se verá más adelante, en la orden de privacidad de la FCC anulada por el Congreso en 2017, la Comisión consideró que contar con 2 niveles de aprobación distintos, basados en el hecho de si la información es sensible o no, permitiría implementar el contenido del artículo 222; tal es el caso de la información relativa a la geolocalización de una persona.

70 *Op.cit.,* Nota 31.

71 115th Congress Public Law 22, *Joint Resolution, S.J. Res. 34*, U.S. Government Publishing Office, abril de 2017, disponible en https://www.congress.gov/115/plaws/publ22/PLAW-115publ22.pdf, última fecha de consulta el 2 de diciembre de 2018.

72 Bajo la denominada Ley de Revisión del Congreso (*Congressional Review Act)*, codificada en el Título 5 U.S.C. §§ 801, cualquier agencia federal en los Estados Unidos está obligada a someter ante ambas cámaras del Congreso antes de su entrada en vigor cualquier regla. Disponible en https://www.govinfo.gov/content/pkg/USCODE-2017-title5/pdf/USCODE-2017-title5.pdf, última fecha de consulta 2 de diciembre de 2018.

usuario como por ejemplo el servicio de llamadas en espera. En ese contexto, la FCC consideró, con base en el artículo 222(h)(1) de la Ley de Comunicaciones ya citado, que ciertos tipos de información relacionados con la cantidad, configuración técnica, tipo, destino, ubicación y la cantidad de uso de un servicio de telecomunicaciones al que se encuentre suscrito un usuario, constituyen CPNI cuando un proveedor de servicios de acceso a internet de banda ancha adquiere o tiene acceso a esa información con motivo de la provisión del servicio. Así, bajo la Orden de Privacidad y, tomando en cuenta la arquitectura en capas que se da en las comunicaciones en Internet,[73] se consideró por parte de la FCC como CPNI, entre otros, los siguientes elementos:

- la información relativa a los planes de servicios de banda ancha;
- la geolocalización;
- los nombres de dominio y las direcciones IP;
- la utilización de aplicaciones;
- los encabezados de aplicaciones, y
- los dispositivos y equipos del usuario final.[74]

Por ejemplo, respecto del supuesto relativo a la geolocalización de las personas, el congreso estadounidense a través de la Ley de Comunicaciones en su artículo 222(f) ya había considerado que este tipo de información requiere la aprobación previa del usuario del servicio, según se señaló líneas arriba. Para el caso que se analizará en el siguiente capítulo es interesante tomar en cuenta lo que la FCC señaló respecto de las direcciones IP para considerarlas como CPNI. Es decir, en virtud de que una dirección IP, tanto en el origen como en el destino, está relacionada con la configuración técnica, el destino y/o la ubicación de un servicio de telecomunicaciones, fue considerada por esa autoridad como CPNI; lo anterior debido a que en una red IP, al igual que los números telefónicos de origen y destino en una llamada de voz tradicional, el tráfico de datos entre un usuario final y las

73 Al respecto, la FCC proporciona una explicación general de carácter técnico sobre el funcionamiento de las comunicaciones en internet representado por una multiplicidad de capas, apiladas una sobre otra, en las que cada una cumple una función lógica particular respecto dela información que se transmite y utiliza un protocolo de red que estandariza la comunicación entre sistemas, lo que permite una rápida innovación en los protocolos y aplicaciones basados en Internet. *Op.cit.,* Nota 31, pp. 20-21.

74 *Ibidem.*, pp. 23-32.

páginas web a las que accede, se enruta por los proveedores de acceso a internet de modo que dichas direcciones IP se relacionan con el destino del uso de un servicio de telecomunicaciones, en tanto que ambas direcciones IP se vinculan con el destino, tanto para el tráfico entrante como saliente. Incluso las direcciones IP permiten ubicar geográficamente tanto al usuario como al servicio al que accede.[75]

Lo mismo ocurre con los nombres de dominio en Internet (*vgr.,* ift.org; google.com; sat.gob, etc.) puesto que permiten identificar el punto de destino al que los usuarios buscan conectarse, en el entendido de dichos nombres se traducen o convierten directamente en una dirección IP, en virtud de lo cual se relacionan con el destino y la configuración técnica de un servicio de telecomunicaciones.[76]

Por lo que se refiere a los encabezados[77] que se insertan en el tráfico de Internet, la FCC también los consideró como información que califica como CPNI en tanto que es información que un ISP, en virtud de su relación con el cliente, puede crear y agregar al tráfico de internet de éste. Este es el caso en que un operador inserta un encabezado de identificador único (*UIDH*, por sus siglas inglés), el cual es considerado como CPNI porque se trata de información que se encuentra en el encabezado de la capa de aplicación (*application layer header*) que tiene que ver con la configuración técnica, tipo, destino y cantidad de uso de un servicio de telecomunicaciones. Es decir, cuando un usuario de internet ejecuta una

---

75 *Ibidem.*, p. 25. En el idioma original se lee: "*We conclude that source and destination IP addresses constitute CPNI in the broadband context because they relate to the destination, technical configuration, and/or location of a telecommunications service. An IP address is a routable address for each device on an IP network, and BIAS providers use the end user's and edge provider's IP addresses to route data traffic between them. As such, source and destination IP addresses are roughly analogous to telephone numbers in the voice telephony context. … IP addresses a customer uses and those with which she exchanges packets constitute CPNI because both source and destination IP addresses relate to the destination of use of a telecommunications service; one links to the destination for inbound traffic while the other links to the destination for outbound traffic. IP addresses are also frequently used in geo-location". (*Traducción propia).

76 *Ibidem.,* pp. 26-27.

77 Como se mencionó, en las comunicaciones sobre Internet, la información generalmente se transmite verticalmente a través de varias capas. Cuando una aplicación envía datos a través de Internet, el proceso comienza con los datos de la aplicación moviéndose hacia abajo a través de las capas. Cada capa agrega información y funcionalidad de red adicional, envolviendo la salida de las capas que están sobre ella con un "encabezado". La comunicación enviada a través de Internet, consistente en los datos de la aplicación envueltos en los encabezados de cada capa, se denomina "paquete". Cuando un dispositivo recibe datos a través de Internet, ocurre el proceso inverso. Los datos se mueven hacia arriba a través de las capas; cada capa desenvuelve su información asociada y pasa hacia arriba, hasta que la aplicación en el dispositivo del destinatario recupera los datos de la aplicación original. *Ibidem*, p. 22.

aplicación,[78] ésta agrega uno o más encabezados a la información transmitida, los cuales contienen información sobre la carga útil que la aplicación está enviando o solicitando. Por ejemplo, en la navegación web, el "localizador uniforme de recursos" (URL, por sus siglas en inglés) de una página web constituye información del encabezado de la aplicación. En una conversación por correo electrónico, mensaje instantáneo o chat de video, el encabezado de una aplicación puede revelar a las partes de la conversación.

Como puede observarse, más allá de lo que preveía la Orden de Privacidad, la FCC ya había considerado previamente, con motivo del caso que es objeto de análisis en este trabajo, que la información que un proveedor hace que se genere o almacene en el dispositivo de un cliente, incluyendo dispositivos móviles, o que se agregue al tráfico de internet de un cliente, con el objeto de permitir que el proveedor recolecte, acceda o utilice dicha información, se considera o califica como CPNI[79] si cae en alguna de las categorías descritas en el artículo 222 de la Ley de Comunicaciones.

Aun cuando la Orden de Privacidad nunca entró en vigor, la FCC ha considerado que el artículo 222 contiene por sí mismo importantes protecciones en materia de privacidad tratándose de servicios de banda ancha[80] y para efectos del caso que se analiza en el Capítulo 3 ello fue suficiente junto con la regla de transparencia para motivar la decisión de esa autoridad.

2.2.2 Consentimiento del usuario para el uso y divulgación de su información

Tratándose del uso y compartición de la información de las personas físicas que realizan actividades en línea, tanto en Europa como en los Estados Unidos se ha

78 *Ídem.* La información transmitida desde y hacia una aplicación es conocida como la carga útil de la aplicación (*application payload*); se trata de la esencia de una comunicación entre un usuario de internet y la entidad a la cual desea comunicarse. Ejemplos de este tipo de información son el cuerpo de una página web; el texto de un correo electrónico o de un mensaje instantáneo; un video de un servicio audiovisual o los mapas que se obtienen de una aplicación de navegación.

79 Comisión Federal de Comunicaciones, *Consent Decree, In the Matter of Cellco Partnership, d/b/a Verizon Wireless*, DA 16-242, Washington, D.C., marzo de 2016, p.3, disponible en: https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0307/DA-16-242A1.pdf. Última fecha de consulta 3 de enero de 2019.

80 *Op.cit,* Nota 16, p. 19815.

propugnado porque exista un consentimiento informado por parte de los consumidores previo a su decisión de compartir su información personal.[81] El consentimiento informado está relacionado con el derecho a la información y, en consecuencia, a la libertad de elección; implica que el usuario de internet conozca antes de tomar una decisión la información precisa y adecuada relativa a un servicio y que además la comprenda, como, por ejemplo, quién es el responsable del tratamiento de su información, así como los fines para los cuales se desea usar o compartir la misma.[82] Es decir, el objetivo es que el consentimiento esté basado en una verdadera elección y que además la decisión sea adoptada libremente, lo cual puede interpretarse, entre otros supuestos, como el hecho de que la decisión del consumidor no esté sujeta a condiciones ni amenazas en cuanto a la prestación del servicio que haya contratado o al cual desea acceder y, además, que pueda revocar su consentimiento sin que el interesado sufra alguna consecuencia negativa.

En el caso de la regla de transparencia de las reglas de internet abierto, como se indicó en el apartado anterior, se prevé que con el objeto de que los consumidores (así como de otros interesados como sería el caso de los *edge*

81 A fin de delimitar el uso de los datos personales, es de gran importancia que el consentimiento por parte de los usuarios sea informado y estén conscientes de lo que realmente se encuentran autorizando lo cual constituye un desafío, es decir, que las personas como titulares de los datos conozcan y entiendan los alcances de dicho consentimiento. En relación con el tratamiento de los datos personales, cabe resaltar que en Europa a través de los avisos de privacidad que las empresas comunican, el consentimiento de los usuarios se perfecciona, en tanto que en los Estados Unidos de América basta una cláusula de adhesión para obtener dicho consentimiento sin que el mismo pueda modificarse. El que se profundice en la forma de obtener el consentimiento o en la manera en que deben estar regulados los avisos de privacidad depende de la legislación de cada país.

82 Una vez que un usuario de internet otorga su autorización para el tratamiento y uso de sus datos personales, la responsabilidad por parte del proveedor que obtiene dichos datos es uno de los principios en materia de protección de datos personales, de modo que es responsable del uso no autorizado de los mismos. En cualquier caso, la responsabilidad de un proveedor de servicios (como lo puede ser un ISP o un portal de internet) varía dependiendo de las circunstancias concretas del caso de que se trate; por ejemplo, en el caso de algunos países miembros de la Unión Europea, como es el caso de Hungría, el tribunal civil nacional determinó la existencia de responsabilidad objetiva a cargo de un portal de noticias en Internet por permitir la publicación en su sitio web de comentarios generados por usuarios que presumiblemente afectaban la reputación de una tercera empresa. En este caso, el Tribunal Europeo de Derechos Humanos consideró que tal determinación de responsabilidad no era válida cuando se afectaba el derecho a la libertad de expresión (que incluye la libertad de difundir información) previsto en el artículo 10 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales considerando además que dicho derecho estaba por encima de cualquier otro criterio que proteja, por ejemplo, la reputación comercial de una empresa. Véase Caso Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, No. 22947/13, 2016.

providers) realicen una elección de manera informada, los proveedores del servicio de acceso a internet deben divulgar información precisa acerca de sus prácticas de red y los términos y condiciones del servicio.

Ahora bien, los avisos de privacidad tienen por objeto dar a conocer y explicar a los usuarios que tienen el derecho de elegir si otorgan su aprobación o revocan la misma tratándose del uso y compartición de su información. Por supuesto, para lograr que los usuarios tomen verdaderas decisiones de manera informada, los proveedores deberían incluso explicar cómo es que recolectan la información de los usuarios y los derechos que éstos tendrían para controlar esa recopilación, uso y compartición de información. De hecho, en términos de la orden de internet abierto de 2015 de la FCC, con el fin de hacer valer el requisito de transparencia, se estableció que los cambios sustantivos a los términos comerciales[83] bajo los cuales es provisto un servicio deben ser notificados a efecto de que se respete el derecho de los usuarios a realizar una decisión informada. Lo anterior resulta relevante en la medida en que, si un proveedor realiza cambios importantes a su política de privacidad una vez que un usuario ya había manifestado su consentimiento respecto de cierto conjunto de prácticas de dicho proveedor, y dicho cambio no se notifica al cliente debidamente, ello iría claramente en contravención a lo dispuesto en el artículo 222 puesto que no hay un consentimiento informado propiamente dicho.

Existen al menos dos formas válidas de obtener el consentimiento del usuario para que su información sea utilizada e incluso compartida. La primera, implica el consentimiento previo y expreso del usuario (*opt-in*), como es el caso en que una aplicación móvil requiere permiso para utilizar información relativa a la geolocalización del usuario del dispositivo móvil. La segunda, implica un consentimiento tácito que puede ser revocado después de su otorgamiento (*opt-out*).[84]

---

83 Las políticas de privacidad forman parte de los términos comerciales en la provisión de servicios de telecomunicaciones. *Op.cit.,* Nota 79, p. 19760.

84 Tratándose de información sensible, la Orden de Privacidad de 2016 de la FCC requería de los ISP obtener el consentimiento expreso e informado del usuario *(opt-in)*, así como para cambios sustantivos retroactivos de las políticas de privacidad de los operadores; mientras que, tratándose de información no sensible del usuario, bastaría la opción de revocación del consentimiento (*opt-out*). *Op.cit.,* Nota 31, p. 5, p. 68.

Así, bajo la orden de privacidad de 2016 que fue anulada por el congreso estadounidense, la FCC pretendió categorizar como sensible la información obtenida en virtud del historial de navegación en internet de una persona, así como del uso de aplicaciones y, por lo tanto, sujetas a un aviso o al consentimiento expreso opt-in.[85]

Por lo que se refiere a los usuarios en internet menores de edad vale la pena mencionar que la agencia estadounidense de protección al consumidor (FTC, por sus siglas en inglés) se encarga de velar por el respeto y cumplimiento a la Ley de Protección a la Privacidad en Internet de los Niños (COPPA,[86] por sus siglas en inglés) y, como su nombre lo indica, protege la privacidad en internet de las personas pero únicamente de aquellas que sean menores de 13 años de edad. En particular, el artículo 6502 de dicha Ley exige el consentimiento expreso que debe ser otorgado por los padres del menor de manera previa e informada para la mayoría de los usos de la información de los niños y únicamente permite ciertos usos con divulgaciones. Lo anterior permite evitar que un determinado sitio web o servicios y aplicaciones en línea recolecten información personal[87] de los niños menores de 13 años e incluso que la comercialicen, sin el consentimiento previo de sus padres, el cual debe ser verificable, de modo que el control de la información del menor lo tienen éstos. Dentro de la información personal se considera también a cualquier "identificador persistente"[88] que pueda ser utilizado para reconocer a un usuario a lo largo del tiempo y a través de diferentes sitios web o servicios en línea;

85 *Ibidem.,* p. 215.

86 El acrónimo COPPA corresponde a *Children's Online Privacy Protection Act* emitida en 1998 por el congreso estadounidense. La regla de protección a la privacidad en línea de los niños se encuentra prevista en el artículo 312 del título 16 del Código de Regulaciones Federales (16 CFR § 312), la cual fue emitida bajo la Ley COPPA, 15 U.S.C. 6501 y subsiguientes, misma que entró en vigor en abril de 2000 y fue modificada en julio de 2013 para actualizarla en relación con las actividades en línea. United States Civil Code, 2017, Título 15 U.S.C. §6501 y subsiguientes, pp. 2038-2043, disponible en: https://www.govinfo.gov/content/pkg/USCODE-2017-title15/pdf/USCODE-2017-title15.pdf, última fecha de consulta 24 de noviembre de 2018.

87 De acuerdo a la regla de protección a la privacidad en línea de los niños *(Children's Online Privacy Protection Rule)* se considera como información personal aquella individualmente identificable sobre un individuo recogida en línea como, por ejemplo, el nombre, domicilio, teléfono, correo electrónico, ubicación geográfica, archivos que contengan imágenes o voz del menor, así como direcciones IP que utilice el menor y que permitirían identificar y rastrear sus hábitos. *Ibidem,* p. 2038-2039.

88 *Ídem*.

tal identificador persistente se refiere, por ejemplo, a un número de cliente en una *cookie*; una dirección IP; un número de serie de un equipo, o bien, un identificador único de un dispositivo. Así, sin el consentimiento expreso de los padres, los operadores de sitios web no pueden utilizar los identificadores persistentes con el propósito de enviar al menor de edad publicidad dirigida basada en sus gustos y comportamientos. Tampoco pueden utilizar tales identificadores para conformar el perfil de un menor, basado en la recopilación de tales identificadores a lo largo del tiempo y de distintos sitios web con objeto de tomar decisiones u obtener información del menor.

En cualquier caso, los padres reciben un aviso o notificación que a su vez remite a la política de privacidad del responsable del sitio web al cual desea tener acceso el menor.

El párrafo 3 del artículo 312.2 del Código de Regulaciones Federales[89] define la recopilación de información personal de un niño como aquella que se realiza por cualquier medio e incluye no solo el hecho de solicitar o alentar a un menor de 13 años a entregar su información personal en línea, sino también al rastreo o seguimiento pasivo de un niño en internet. Así es como también la información relativa a los niños menores de 13 años que fuese recopilada por los proveedores de acceso a internet fue considerada con el apoyo de la FTC por la Orden de Privacidad como sensible.

El enfoque que la FTC ha sostenido en relación con el respeto a las decisiones y el derecho de elección de los consumidores se ha basado en el hecho de si la recopilación y el uso de la información es consistente con el contexto en el que un consumidor interactúa con la empresa que le proporciona el servicio y con las expectativas razonables que un consumidor tiene derivado de lo anterior. En relación con las prácticas que resultan inconsistentes con tales expectativas e interacciones, la FTC ha propugnado que las empresas proporcionen opciones significativas a los consumidores, con un nivel de elección que esté relacionado con

89 Comisión Federal de Comercio, *Federal Register*, "Children's Online Privacy Protection Rule; Final Rule", Vol. 78, No. 12, enero 2013, p. 4009, disponible en https://www.ftc.gov/system/files/2012-31341.pdf, última fecha de consulta 28 de noviembre de 2018.

esas expectativas. Bajo esta aproximación, la FTC apoya el uso de la opción que conlleva un consentimiento voluntario y expreso (*opt-in*) cuando se trata de obtener información sensible que pudiera ser recopilada por los ISP, incluyendo: a) el contenido de las comunicaciones y b) información relacionada con los números de seguridad social de una persona, información financiera o relacionada con la salud, información relacionada con los niños, o bien, datos que precisan la ubicación geográfica de una persona. Incluso esa Comisión Federal de Comercio considera que, sin importar si la empresa es la parte proveedora de un servicio, una afiliada o una tercera parte, en cualquier caso, se requiere el uso de la opción voluntaria (*opt-in*) cuando se desee obtener información relacionada con el contenido de las comunicaciones de los consumidores (es decir, contenido de los correos electrónicos, comunicaciones en redes sociales, términos de búsqueda, comentarios en sitios web, artículos de compras en línea, así como documentos, fotos, videos, libros leídos o películas vistas por los consumidores, independientemente de si éstos tienen acceso a internet desde una computadora tradicional o a través de un dispositivo conectado a internet. La razón de lo anterior se debe a que la información relacionada con el contenido de las comunicaciones de un usuario puede ser altamente personalizada lo que permitiría un análisis muy completo que de otra forma no sería posible con datos o información menos precisos. Incluso, de acuerdo a la FTC, el uso del contenido de las comunicaciones permitiría inferir información adicional de carácter sensible que permitiría tomar decisiones acerca de los consumidores que les puede causar un daño en el supuesto de que tales inferencias o datos no sean precisos.[90]

Ahora bien, contrariamente a la opinión de la FTC, la FCC no considera que la compartición de información personal del cliente por parte de un operador con sus propios agentes filiales constituya compartición con terceras partes que requiera ya sea de un consentimiento expreso o tácito. Es decir, los ISP de acuerdo al

90 Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission: In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Federal Trade Commission,* mayo de 2016, pp. 20-22, disponible en: https://www.ftc.gov/news-events/press-releases/2016/05/ftc-staff-provides-comment-fccs-proposed-privacy-rulemaking, última fecha de consulta 25 de noviembre de 2018.

enfoque de la FCC pueden utilizar el contenido de las comunicaciones para propósitos de publicidad internos o de sus afiliadas de servicios relacionados con comunicaciones, sin necesidad de obtener el consentimiento previo y expreso de los consumidores. Lo anterior podría significar que un ISP puede utilizar la información de búsqueda en línea que haga una persona o su historial de compras en línea, sujeto únicamente a la opción de exclusión (*opt-out*), y una vez que el ISP haya podido determinar con base en esa información si un consumidor es capaz o no de comprar determinado monto o calidad de productos, o bien, una vez que ya haya compartido esa información con sus filiales.

A diferencia de la Orden de Privacidad de 2016 en la que el tipo de consentimiento que se pretendía exigir obtener del usuario estaba basado en el hecho de si la información es sensible o no, en las reglas actuales, el tipo de consentimiento del usuario depende únicamente del propósito para el cual la información será utilizada o compartida, es decir, si será o no con fines de publicidad interna o de sus filiales o si se compartirá con terceras partes sin que se tenga conocimiento de los fines para los cuales se empleará su información. Ahora bien, también es claro que al categorizar una información como sensible o no, es un hecho subjetivo puesto que habrá usuarios que de acuerdo a sus expectativas personales desean que se proteja de manera efectiva su información personal que no necesariamente es considerada como “sensible” por la regulación aplicable, de modo que bajo este supuesto podría considerarse que la privacidad de la información se encuentre comprometida si se disemina o comparte sin el consentimiento previo de un usuario.

Por otro lado, cabe destacar, que aun cuando un usuario configure su navegador buscando la privacidad de su comportamiento en línea, el hecho es que, si otorgó a algún proveedor de acceso a internet su consentimiento expreso bajo algún programa específico que permita el rastreo de su historial de navegación, el proveedor continuará recolectando información independientemente de las configuraciones que se hagan en el navegador. Tal es el caso del programa denominado Verizon Selects del operador inalámbrico Verizon Wireless que trabaja sobre la base de la obtención previa de un consentimiento expreso (*opt-in*) para

utilizar información relativa al historial de navegación y al uso de aplicaciones de los usuarios móviles junto con la ubicación geográfica, con el objeto de desarrollar y personalizar información y ofertas publicitarias dirigidas a sus clientes, de modo que aun cuando el usuario configure su navegador para borrar o eliminar las *cookies*[91] y dejar de participar en ese programa de publicidad, ello no constituye una manera efectiva de excluirse (*opt-out*) del envío de publicidad.[92] Con base en lo anterior, se considera que la opción relativa a obtener el consentimiento voluntario y expreso de un usuario permite que éste pueda aprovechar de manera oportuna ese momento para decidir previamente acerca de la compartición de su información, independientemente de si ésta es sensible o no, ya que en el supuesto de la opción de exclusión no se garantiza en todos los casos que la elección o decisión de un usuario para compartir su información haya sido razonada e informada. La forma de otorgar el consentimiento para autorizar el uso de los datos depende de la legislación de cada país; en general, cuando se trata de datos sensibles se requiere la obtención del consentimiento expreso por parte del titular de los mismos. Solo en caso de que la ley aplicable indique que no es necesario el consentimiento, no será necesaria su obtención por parte del responsable de su manejo y tratamiento lo obtenga, pero la regla general es la obtención del consentimiento. Con la mera aceptación del aviso de privacidad que comunican los responsables de los datos se entendería que el titular de los datos no se opondría a su tratamiento, no obstante que ello no refleje necesariamente un consentimiento informado.

---

91 Las *cookies* son pequeños archivos de texto que las páginas web que visitamos como usuarios instalan en nuestro navegador de modo que se alojan en éste o en el disco duro de las computadoras; permiten almacenar contenidos e incluso compartir información entre los distintos navegadores de Internet y, en principio, se pueden controlar mediante la configuración de privacidad del navegador. Las hay de varios tipos entre las que destacan las cookies de seguimiento o de publicidad comportamental que constituyen una herramienta que los anunciantes y los sitios web emplean para el envío de ofertas personalizadas con fines exclusivamente publicitarios. Para mayor detalle, véase López Jiménez, David, "Las cookies como instrumento para la monitorización del usuario en la Red: la publicidad personalizada"*, Revista de Ciencias Económicas,* San José, Vol. 29, núm. 2, julio 2011, pp. 175-190, disponible en línea en https://revistas.ucr.ac.cr/index.php/economicas/article/view/7018/6703, última fecha de consulta el 9 de diciembre de 2018.

92 Véase *How Verizon Selects from Verizon Wireless Works*, diciembre de 2012, disponible en https://www.verizon.com/about/news/vzw/2012/12/verizon-selects y https://es.verizonwireless.com/support/verizon-selects-faqs/, última fecha de consulta: 25 de noviembre de 2018.

Capítulo 3

Análisis del Caso Verizon Wireless

Capítulo 3: Análisis del Caso Verizon Wireless

3.1 Competencia de la Comisión Federal de Comunicaciones para la aplicación y ejecución de las reglas de internet abierto

La competencia de la FCC para aplicar y vigilar la debida observancia de las reglas de internet abierto entre las cuales destaca, para el caso objeto de análisis en el presente trabajo de investigación, la regla de transparencia, data desde 2010 con la emisión de las primeras reglas de neutralidad de la red por parte de esa autoridad. Sin embargo, por lo que se refiere a la privacidad y confidencialidad de la información de los usuarios del servicio de acceso a Internet de banda ancha, la cual puede verse afectada con motivo de la violación a la regla de transparencia, durante los últimos años y al día de hoy, ha estado en constante debate la jurisdicción en cuanto a qué autoridad federal es en los Estados Unidos la encargada de vigilar y ejecutar las reglas que protegen la misma, en el sentido de si es la FTC o la FCC. Lo anterior ha dependido de si los servicios de internet de banda ancha se encuentran, al amparo de las reglas de internet abierto, bajo la clasificación de servicios de información, o bien, si se encuentran catalogados como actividades provistas por operadores comunes sujetos siempre a la jurisdicción de la FCC.

Es así, como se vio en el capítulo anterior, que el artículo 5 de la Ley de la Comisión Federal de Comercio exenta de su ámbito de aplicación a los operadores comunes que proveen servicios de telecomunicaciones, tales como la telefonía, (*common carriers*) por encontrarse sujetos al ámbito de aplicación de la Ley de Comunicaciones de 1934. Actualmente, la FTC cuenta con el liderazgo para vigilar la privacidad en Internet bajo la autoridad que deriva de la Ley citada para proteger a los consumidores de las prácticas engañosas e injustas en materia de comercio. Sin embargo, las pocas regulaciones en materia de privacidad que ha emitido esa Comisión federal se refieren únicamente a la protección de la privacidad en línea de financiera.[93]

93 Disponible en https://www.ftc.gov/enforcement/rules/rules-and-guides, última fecha de consulta 28 de diciembre de 2018.

En los últimos 10 años la FTC ha ejercido numerosas acciones legales en contra de empresas que han violado los derechos de privacidad de los consumidores o debido a prácticas engañosas en contra de éstos al no respetar ni mantener la seguridad respecto de su información sensible que obtienen en línea. En la mayoría de los casos la FTC ha investigado a los demandados por violar el artículo 5 de la Ley de la Comisión Federal de Comercio, anteriormente citada, que prohíbe los actos y prácticas injustos y engañosos que afectan el comercio. Por ejemplo, esta Comisión ha ejercido acciones legales en contra de proveedores de aplicaciones móviles por violaciones a la Ley de Protección a la Privacidad de los Niños en Línea (Coppa).[94] Asimismo, en la mayoría de los casos las acciones iniciadas por la FTC concluyen en un acuerdo con las empresas objeto de investigación, mediante el cual se les obliga a llevar a cabo determinado tipo de acciones para solucionar la afectación a los consumidores; sin embargo, la FTC carece de autoridad para imponer sanciones de tipo civil por violaciones cometidas en primera instancia a la Ley de la Comisión Federal de Comercio y únicamente las impone en caso de incumplimiento a los términos y condiciones de algún acuerdo mediante el cual dicha agencia impuso obligaciones a una empresa para dar por terminada una investigación.

Por su parte, la FCC ha contado con un papel muy limitado para supervisar el respeto a la privacidad en línea. Fue durante el periodo que abarca de 2015 a 2017 que la FCC ejerció jurisdicción sobre las prácticas de los ISP en materia de privacidad en Internet, precisamente durante el tiempo en que se llevó a cabo la investigación por parte de dicha agencia federal en contra de Verizon Wireless a que se refiere el presente caso (esto es, de diciembre de 2014 a marzo de 2016).

Así, durante la vigencia de las Reglas de Internet Abierto 2015 en virtud de las cuales los proveedores del servicio de acceso a Internet de banda ancha fueron

94 United States District Court Northern District Of California, *United States v. Yelp Inc.*, No. 3:14-CV-04163, *Stipulated order for permanent injunction and civil penalty judgment filed* (N.D. Cal. Sept. 16, 2014). En su demanda ante una corte de distrito del estado de California en contra de la empresa Yelp, Inc., la Comisión Federal de Comercio alegó la recopilación ilegal de información personal de niños menores de 13 años sin haber notificado y obtenido el consentimiento previo de los padres. Disponible en https://www.ftc.gov/system/files/documents/cases/140917yelpstip.pdf, última fecha de consulta 27 de enero de 2019.

considerados como *common carriers* catalogando tales servicios como servicios de telecomunicaciones (sujetos al ámbito de aplicación de la Ley de Comunicaciones), la FCC contaba con la autoridad y jurisdicción para regular y vigilar las prácticas y el manejo de la privacidad por parte de dichos proveedores así como de las empresas de telecomunicaciones; por su parte, la FTC tenía autoridad y jurisdicción únicamente en relación con los proveedores de servicios, contenidos y aplicaciones (*edge providers*) puesto que bajo el artículo 5 de la Ley de la Comisión Federal de Comercio, los ISP estaban exentos de su ámbito de aplicación.

Como se manifestó en el capítulo anterior, después de que el Congreso de los Estados Unidos anuló, antes de que entraran en vigor, las reglas de privacidad aplicables a los ISP que emitió la FCC en 2016, fue hasta junio de 2018 (cuando entraron en vigor las nuevas reglas de internet abierto emitidas por la FCC en diciembre de 2017) que la FTC recuperó la jurisdicción para supervisar las actuaciones en materia de privacidad en línea de los proveedores de acceso a Internet. En virtud de lo anterior, empresas como AT&T se han visto involucradas en procesos judiciales frente a la FTC ya que ésta inició investigaciones bajo la autoridad que le concede el artículo 5 de la Ley de la FTC por prácticas engañosas realizadas por AT&T que ralentizaban el tráfico de sus usuarios haciendo casi imposible que éstos hicieran uso del servicio de acceso a Internet que tenían contratado con ese operador. En este caso, AT&T manifestó que se encontraba exento de la jurisdicción de la FTC por ser un prestador de servicio de telecomunicaciones.[95]

Así, en febrero de 2018, un tribunal de apelaciones del noveno circuito en Estados Unidos concluyó que la exención a que se refiere el artículo 5 de la Ley de la Comisión Federal de Comercio impide que la FTC regule a los operadores comunes únicamente en la medida en que éstos realizan actividades que corresponden precisamente a un proveedor de servicios de telecomunicaciones,[96]

95 Véase https://www.ftc.gov/enforcement/cases-proceedings/122-3253/att-mobility-llc-mobile-data-service, Última fecha de consulta 22 de febrero de 2019.

96 Tribunal de Apelaciones de Estados Unidos del Noveno Circuito, Federal Trade Commission v. AT&T Mobility LLC, No. 15-16585 D.C., 26 de febrero de 2018, disponible en https://www.ftc.gov/system/files/documents/cases/att_enbanc_5-16585.pdf, última fecha de consulta 22 de febrero de 2019. En el caso descrito, el tribunal manifestó lo siguiente: Una empresa telefónica ya no es más

como lo es el servicio de telefonía. En consecuencia, se interpretó que la FTC cuenta con jurisdicción para vigilar las prácticas engañosas que los proveedores de servicios de telecomunicaciones realicen cuando se trate de actividades que no conllevan la prestación de un servicio de telecomunicaciones como es el servicio de acceso a Internet de banda ancha que actualmente se encuentra considerado, bajo la última reclasificación de la FCC realizada en diciembre de 2017, como un servicio de información.

Tomando en cuenta que la FCC a partir de diciembre de 2017 reclasificó el servicio de internet de banda ancha como un servicio de información, actualmente, para aquellas compañías que tradicionalmente han ofrecido servicios de telefonía como Verizon o AT&T y que simultáneamente proveen servicios de internet de banda ancha, se considera que, no obstante que una compañía telefónica se encuentre sujeta a la jurisdicción de la FCC, si adicionalmente presta servicios de internet inalámbricos o de banda ancha, se encontrará sujeta, por lo que se refiere a esta última actividad, a la jurisdicción de la FTC. Lo anterior, en tanto la decisión del tribunal de apelaciones del noveno circuito no sea revertida.

Si bien a raíz de la emisión de las Reglas de internet abierto en diciembre de 2017 en virtud de las cuales se reclasificó el servicio de acceso a internet como un servicio de información, la FCC dejó de contar con autoridad para vigilar a los proveedores de servicios de acceso a Internet con motivo de violaciones a la privacidad en línea de sus usuarios, tanto la FTC como la FCC suscribieron a través de sus respectivas oficinas de asuntos del consumidor y gobierno (*FTC Consumer and Governmental Affairs Bureau*) y de cumplimiento (*FCC Enforcement Bureau*),

---

una simple empresa telefónica. La transformación de los servicios de información y la ubicuidad de la tecnología digital significa que los operadores de telecomunicaciones se han expandido a sitios web, distribución de videos, producción de noticias y entretenimiento, servicios y dispositivos de entretenimiento interactivos, seguridad del hogar y más. Al reafirmar la jurisdicción de la Comisión Federal de Comercio sobre actividades que caen fuera de los servicios de telecomunicaciones, se evitan vacíos regulatorios y se provee de consistencia y previsibilidad en el cumplimiento de la regulación. En el idioma original se lee: *A phone company is no longer just a phone company. The transformation of information services and the ubiquity of digital technology mean that telecommunications operators have expanded into website operation, video distribution, news and entertainment production, interactive entertainment services and devices, home security and more. Reaffirming FTC jurisdiction over activities that fall outside of common-carrier services avoids regulatory gaps and provides consistency and predictability in regulatory enforcement.* (Traducción libre).

un memorando de entendimiento[97] (MOU, por sus siglas en inglés) con el objeto de coordinarse para proteger la privacidad de los consumidores en línea. A través de dicho documento se estableció que, por un lado, la FCC se encargará de revisar las quejas informales relativas al incumplimiento por parte de los proveedores de acceso a internet de las obligaciones de divulgación establecidas en la nueva regla de transparencia prevista en las reglas de internet abierto de 2017. De hecho, la FCC deriva su autoridad competencial para imponer a los ISP la obligación de transparencia del artículo 257 de la Ley de Comunicaciones que le faculta a identificar y eliminar barreras a la entrada en la provisión de servicios de información, así como reportar al Congreso Federal sobre la necesidad de cambios en la ley con el fin de atender tales barreras.[98]

Tales obligaciones incluyen el deber de divulgar públicamente información relativa a las prácticas de los ISP en relación con el bloqueo, la ralentización, la priorización pagada, la administración y manejo de la congestión del tráfico en Internet, así como los términos comerciales bajo los cuales se proveen los servicios de banda ancha. De modo que, en caso de que un proveedor de acceso a internet no cumpla con los requerimientos de divulgación ya sea, en todo o en parte, la FCC podrá ejercer facultades de ejecución en contra de dichos proveedores. Por su parte, la FTC investigará y llevará a cabo sus facultades de ejecución en contra de los proveedores de acceso a internet en tanto las divulgaciones de información hacia los consumidores no sean precisas ni adecuadas, así como por otros actos engañosos o injustos o por prácticas relativas a la prestación de los servicios de banda ancha.

Cabe precisar en relación con lo anterior que, a raíz de la nueva regla de transparencia aplicable a los proveedores de servicios de acceso a internet de

97 Comisión Federal de Comunicaciones y Comisión Federal de Comercio, Decision, *Restoring internet freedom FCC-FTC memorandum of understanding*, diciembre 2017, Disponible en https://www.fcc.gov/document/fccftc-sign-mou-coordinate-online-consumer-protection-efforts, última fecha de consulta 23 de febrero de 2019.

98 Codificado en el Código de los EE.UU. United States Code, 2017, Title 47 U.S.C. § 257(a), p. 97, disponible en https://www.govinfo.gov/content/pkg/USCODE-2017-title47/pdf/USCODE-2017-title47.pdf, última fecha de consulta el 24 de febrero de 2019.

banda ancha con motivo de la emisión de las reglas de internet abierto de 2017,[99] basta con que éstos divulguen su política de transparencia para que puedan, por ejemplo, bloquear el acceso a ciertos servicios o contenidos sin considerarse lo anterior como una violación. Si bien la FCC ha sostenido que la regla de transparencia es suficiente por sí sola (habiendo eliminado las reglas de no bloqueo y no ralentización) para garantizar la apertura en internet tomando en cuenta que los proveedores de acceso a internet han manifestado su compromiso voluntariamente para no bloquear contenidos legales[100] a sabiendas de que tienen incentivos para ello puesto que su negocio depende por supuesto del hecho de que los usuarios tengan acceso a los contenidos y servicios provistos por los *edge providers*, en cuyo caso será la FTC quien hará valer su autoridad bajo el artículo 5 multicitado; lo anterior ha constituido el mayor temor o preocupación entre aquellos actores que se han opuesto a que sea la FTC la única agencia que pudiera ejercitar alguna acción legal en contra de aquellas empresas que violan la confianza de los consumidores en línea.[101]

---

99 La nueva regla de transparencia contenida en el numeral 8.1 de las reglas de internet abierto de 2017 establece lo siguiente: "Cualquier persona que provea el servicio de acceso a internet de banda ancha deberá divulgar información precisa en relación con las prácticas de administración de la red, desempeño de red, así como los términos comerciales de sus servicios de manera suficiente que permita a los consumidores hacer elecciones informadas en relación con la compra y uso de tales servicios y a los empresarios y otros pequeños negocios desarrollar, comercial y mantener sus ofertas en Internet. Tales divulgaciones deberán realizare a través de un sitio web disponible públicamente y fácilmente accesible o a través de su transmisión a la Comisión". (Traducción propia). En el idioma original se lee: *Any person providing broadband Internet access service shall publicly disclose accurate information regarding the network management practices, performance, and commercial terms of its broadband Internet access services sufficient to enable consumers to make informed choices regarding the purchase and use of such services and entrepreneurs and other small businesses to develop, market, and maintain Internet offerings. Such disclosure shall be made via a publicly available, easily accessible website or through transmittal to the Commission. Op.cit.,* Nota 39, p.7922.

100 *Op.cit.,* Nota 39, pp. 7478, 7901 y 7911. De ahí que la FCC a partir de finales de 2017 consideró: "esto es, hemos determinado que remplazar las prohibiciones sobre bloqueo y ralentización con una regla de transparencia implementa un método de menor costo para asegurar que las amenazas a la apertura en internet son expuestas y disuadidas por las fuerzas del mercado, el oprobio público, así como por la ejecución de las leyes de protección al consumidor". En el idioma original se lee: *That is, we have determined that replacing the prohibitions on blocking and throttling with a transparency rule implements a lower-cost method of ensuring that threats to Internet openness are exposed and deterred by market forces, public opprobrium, and enforcement of the consumer protection laws.*

101 Cooper, Tyler, *FCC vs FTC: Who polices the Internet after net neutrality?* Broadband now, marzo de 2018, disponible en https://broadbandnow.com/report/fcc-vs-ftc-police-internet/. Última fecha de consulta 2 de febrero de 2019.

Tal como se encuentra hoy redactada la regla de transparencia, basta con que los ISP divulguen públicamente cualquier bloqueo, ralentización o práctica que resulte importante para un consumidor razonable, para que se considere que cumplen con dicha obligación de transparencia tal como se puede observar de las consideraciones realizadas por la FCC[102] en relación con el contenido que deben divulgar al respecto los ISP. Así también, considerando que se eliminó el requisito de notificar directamente a un usuario final cualquier práctica que atente contra las reglas de internet abierto por considerarlo una carga indebida para los ISP, la regla de transparencia vigente de la FCC exige a los ISP cumplir alguna de las dos formas que establece la Comisión para hacer del conocimiento de sus clientes sus prácticas: a) incluir sus divulgaciones en un sitio web disponible al público y fácilmente accesible, o b) enviar a la FCC tales divulgaciones quien, a su vez, las hará disponibles en un sitio web al cual pueda tener acceso el público de manera fácil.[103] Mediante estas dos opciones, de acuerdo con la FCC, se evita que los ISP tenga una carga innecesaria para hacer públicas sus prácticas de manejo de red así como los términos comerciales de sus servicios que incluyen las políticas de privacidad y se asegura que los consumidores puedan tomar decisiones informadas respecto de la compra y uso del servicio de acceso a internet de banda ancha; que las empresas y otros pequeños negocios tengan acceso a la información técnica que necesitan para crear y mantener contenido, servicios y aplicaciones en línea, y que la Comisión por su parte pueda llevar a cabo la obligación que tiene de identificar barreras a la entrada en el mercado de banda ancha.

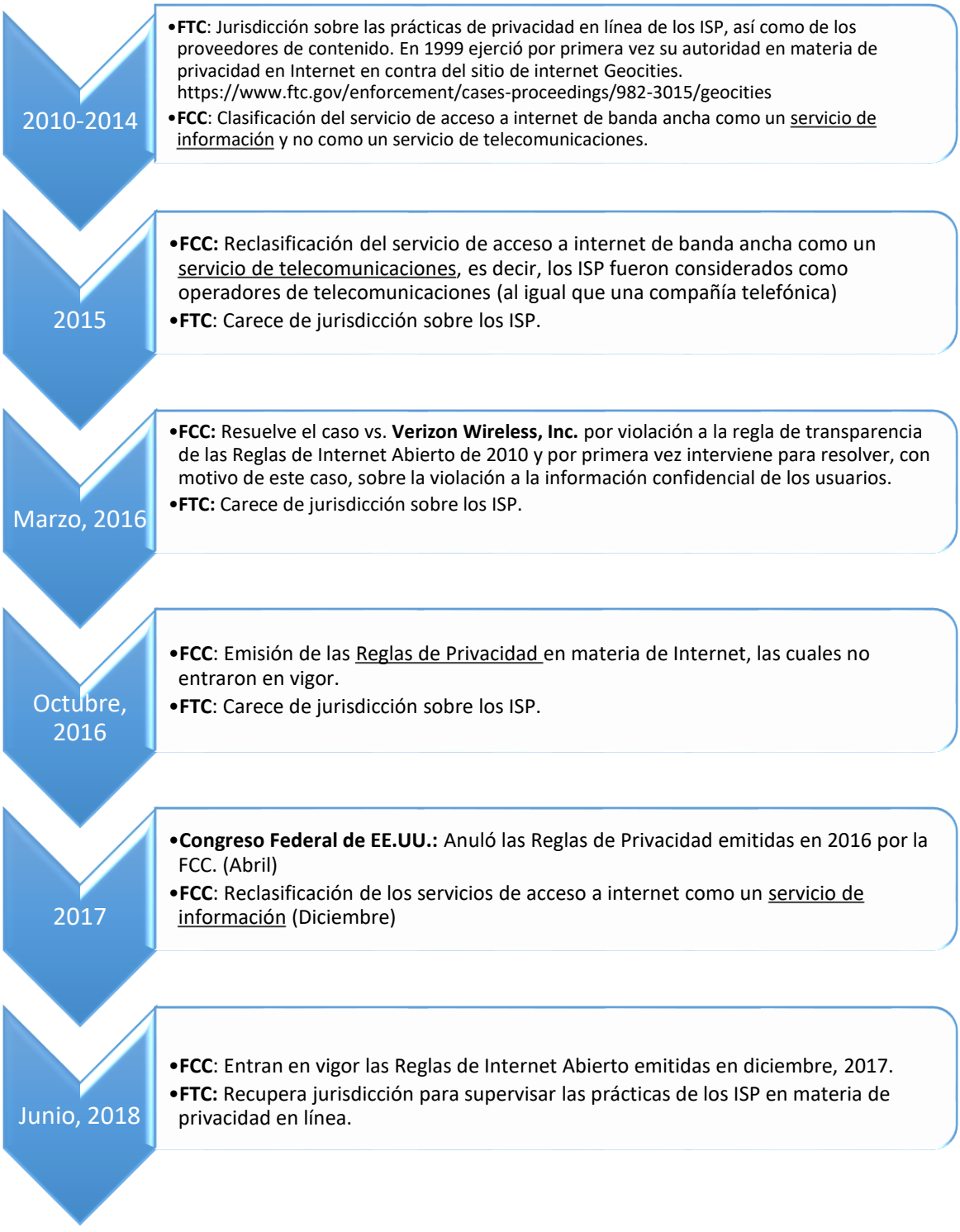
En caso de violación a esta regla de transparencia, será la FTC quien intervenga con motivo de cualquier conducta engañosa por parte de un ISP, mientras que la FCC seguirá un procedimiento informal de quejas interpuestas por los consumidores por violaciones aparentes a la regla de transparencia con el fin de que esa Comisión monitoree el mercado de banda ancha e identifique posibles barreras a la entrada.[104] En adición a lo anterior, la Comisión considera que los

102 *Op.cit.,* Nota 39, pp.7893-7894.
103 *Ídem.*
104 *Ibidem.,* p.7914

consumidores, así como cualquier otra entidad potencialmente afectada por la conducta de un ISP (como por ejemplo, los denominados *edge providers*), cuentan con otros remedios disponibles fuera del ámbito de la FCC bajo las leyes de protección al consumidor que permiten hacer cumplir las promesas hechas por los ISP bajo la regla de la transparencia.[105]

Para el caso que nos ocupa en el presente trabajo de investigación, lo relevante es que la FCC contaba con la facultad de vigilar y sancionar violaciones a la privacidad y confidencialidad de los usuarios en línea con motivo del incumplimiento por parte de los proveedores de acceso a internet a la regla de transparencia establecida en el numeral 8.3 de las reglas de internet abierto. Si bien la investigación a que se refiere el presente caso concluyó a inicios de 2016, las prácticas de rastreo en línea de Verizon Wireless tuvieron lugar antes de que la FCC clasificara el servicio de internet como un servicio de telecomunicaciones; en consecuencia, la investigación practicada por la Oficina de Cumplimiento de la FCC no se basó tanto en la autoridad que la FCC afirmó tener sobre las prácticas de privacidad de los ISP, sino en parte debido más que nada a la violación a la regla de transparencia. De cualquier forma, para el presente apartado resulta útil consultar el siguiente cuadro en el que se esquematiza la competencia que en materia de privacidad han tenido la FTC y la FCC en relación con las prácticas de los ISP.

105 *Ibidem.*, p. 7908.



Cuadro 1. ***Competencia para supervisar las prácticas de privacidad de los ISP en los EE.UU. a partir del 2010***
Fuente: Elaboración propia

3.2 La violación a la obligación de transparencia por parte de Verizon Wireless

En el presente apartado se explicará la conducta realizada por la empresa de servicios de telecomunicaciones inalámbricos, Verizon Wireless, en perjuicio de sus clientes cuya actividad en línea, realizada desde sus dispositivos móviles, comenzó a ser rastreada y monitoreada por el operador inalámbrico con el objeto de conocer sus gustos, preferencias e intereses y poder enviarles posteriormente anuncios personalizados a través de dos programas de publicidad denominados por la empresa como Publicidad Móvil Relevante (*Relevant Mobile Advertising*) y Verizon Selects.

En octubre de 2014, Jonathan Mayer, un científico de la universidad de Stanford, con base en las pruebas que realizó en relación con el hecho de que Verizon Wireless insertaba el identificador UIDH en el tráfico web de sus clientes móviles, señaló respecto del funcionamiento de dicho encabezado que tiene la característica de que no desaparece aun cuando Verizon ofrezca configuraciones de privacidad; al respecto indicó lo siguiente:

> "Cualquier sitio web puede rastrear a un usuario independientemente del bloqueo de las *cookies* o de las opciones de privacidad. No se requiere una relación con Verizon".[106]

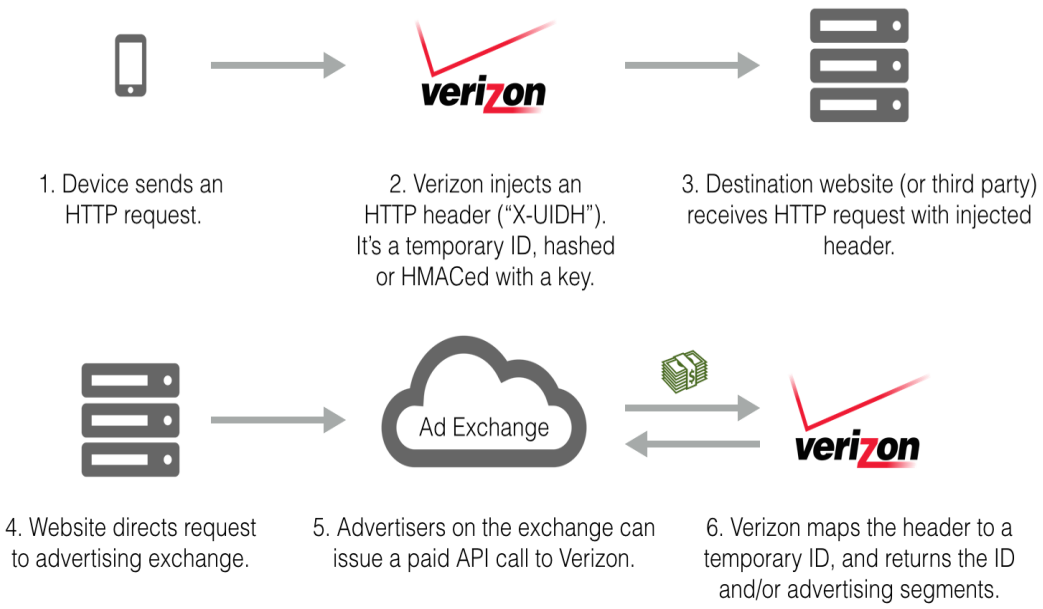
Asimismo, se documentó en relación con el uso de este encabezado UIDH que:

> "Numerosos investigadores en materia de seguridad señalaron que este "supercookie" podría usarse de manera trivial para rastrear a los suscriptores móviles, incluso si hubieran optado por no participar, hubieran eliminado sus cookies o entrado en un modo de navegación privada".[107]

106 Mayer, Jonathan, *How Verizon´s Advertising Header Works,* octubre de 2014, disponible en http://webpolicy.org/2014/10/24/how-verizons-advertising-header-works/, última fecha de consulta el 6 de diciembre de 2018. En el idioma original se lee: Any website can easily track a user, regardless of cookie blocking and other privacy protections. No relationship with Verizon is required. (Traducción propia).

107 Véase Mayer, Jonathan, *The Turn-Verizon zombiecookie*, enero de 2015, disponible en http://webpolicy.org/2015/01/14/turn-verizon-zombie-cookie/, última fecha de consulta el 3 de marzo de 2019. En el idioma original se lee: Numerous security researchers pointed out that this "supercookie" could

En el siguiente cuadro se ejemplifica el funcionamiento del encabezado UIDH que Verizon inserta en el tráfico de internet (en tanto no esté encriptado) de sus clientes móviles, de modo que una vez que el operador inalámbrico inyecta el encabezado que permite identificar a un cliente que esté visitando un sitio web (el cual puede ser del propio Verizon o de un tercero) y recopilar su información (la cual incluye patrones de comportamiento del usuario en la web), el sitio web de destino podrá ver el encabezado de rastreo y hacer ofertas personalizadas al usuario sin que éste tenga conocimiento de lo anterior.



Cuadro 2. *Cómo funciona el encabezado de publicidad de Verizon.* Fuente: *How Verizon´s Advertising Header Works*, webpolicy.org, octubre de 2014.

1. El dispositivo móvil de cliente de Verizon envía una petición de navegación a través del protocolo HTTP; 2. Verizon inyecta el encabezado (X-UIDH); 3. El sitio web de destino (o tercera parte) recibe la petición de navegación HTTP con el encabezado inyectado; 4. El sitio web dirige la petición de navegación del usuario con su información a aquellos anunciantes que estén interesados en obtenerla; 5. Los anunciantes pueden generar un pago a Verizon mediante una llamada API; 6. Verizon asigna el encabezado a un identificador temporal y devuelve el identificador y/o los segmentos de publicidad. (traducción propia).

---

trivially be used to track mobile subscribers, even if they had opted out, cleared their cookies, or entered private browsing mode. (Traducción propia).

En los siguientes apartados se explicará el inicio de la investigación realizada por la Oficina de Cumplimiento de la FCC, la forma en que se acordó dar por terminada dicha investigación, los términos y condiciones impuestos a Verizon Wireless, así como las políticas de privacidad que actualmente maneja dicho operador en relación con el uso del encabezado UIDH. Cabe resaltar nuevamente que el caso que a continuación se explicará no solo se investigó y resolvió en virtud de las denuncias y quejas de los consumidores, la prensa, asociaciones de protección a consumidores, sino también gracias al punto de vista de los científicos y académicos que conocen sobre tecnologías de rastreo en línea, lo cual dio lugar a que la FCC iniciara la investigación respectiva en contra de Verizon Wireless.

3.2.1 Actuación de la autoridad investigadora de la Comisión Federal de Comunicaciones

Como antecedente de la investigación que la Oficina de Ejecución de la FCC inició en diciembre de 2014 en contra de Verizon Wireless, bajo el expediente número EB-TCD-14-00017601, existieron una gran cantidad de noticias en la prensa que resaltaban la consternación con motivo de la práctica de rastreo de información personal realizada por Verizon Wireless a partir de 2012, sin el conocimiento ni consentimiento de sus clientes de banda ancha móvil (mediante la inserción de identificadores en el tráfico de Internet cuando navegan, conocidos como UIDH, según ya se mencionó anteriormente), así como las quejas de los consumidores que la FCC recibió relacionadas con el hecho anterior.[108] A partir de octubre y noviembre de 2014 tanto la prensa como organizaciones de la sociedad civil que defienden los intereses y libertades en internet de los usuarios estadounidenses así como la propia privacidad de las personas, documentaron la práctica realizada por Verizon que le permitía mediante el uso de *cookies* monitorear los sitios web que visitaban sus clientes[109] e incluso catalogar sus gustos e intereses, exponiendo el

108 *Op.cit.,* Nota 79, p.1.

109 Alrededor de 106 millones de clientes minoristas fueron rastreados a partir de noviembre de 2012, en el entendido de que no estaban comprendidos entre aquellos los clientes corporativos ni gubernamentales de Verizon. Además, se reportó que la única forma de evitar el rastreo sería mediante la encriptación no

comportamiento de los usuarios a personas externas, al grado que se señaló que incluso ni siquiera los usuarios de internet conocedores podían evitar el rastreo de su información puesto que el bloqueo mediante la configuración del navegador no era suficiente.[110]

Adicionalmente se confirmó por parte de la autoridad investigadora de la FCC que en octubre de 2012 Verizon comenzó a probar un servicio de publicidad dirigida y a ofrecerlo a sus suscriptores en diciembre de 2012. En ese momento, de acuerdo al escrito de manifestaciones enviado por el departamento jurídico de Verizon[111] a la FCC, la empresa de comunicaciones operaba dos programas de publicidad que utilizaban el UIDH: a) el programa denominado Publicidad Móvil Relevante (RMA por sus siglas en inglés), el cual comenzó a ofrecer en 2012 y b) el programa Verizon Selects, cuyo lanzamiento inició en 2014. De acuerdo con Verizon la diferencia entre los 2 programas radica en el tipo de información que utiliza de sus clientes para enviarles publicidad dirigida. Es decir, Verizon utiliza cierta información personal de sus clientes para identificar y enviar junto con sus socios anunciantes, anuncios publicitarios a los equipos móviles de sus suscriptores.

Para el caso del programa Verizon Selects, la empresa afirmó durante el proceso de investigación de la FCC que recopila la siguiente información de los clientes que navegan por internet para desarrollar perfiles de los clientes participantes en dicho programa con el fin de enviarles publicidad dirigida:

- las direcciones de los sitios web que visitan;
- la ubicación del equipo móvil;
- las aplicaciones (*apps*) y aspectos del dispositivo empleados;

---

obstante que otras nuevas tecnologías de rastreo están apareciendo. Véase Craig Timberg, *Verizon, AT&T Track Their Users with 'Supercookies*,*'* Washington Post, noviembre de 2014, disponible en http://www.washingtonpost.com/business/technology/verizon-atandt-tracking-their-users-with-supercookies/2014/11/03/7bbbf382-6395-11e4-bb14-4cfea1e742d5_story.html, última fecha de consulta 11 de enero de 2019.

110 Véase Hoffman-Andrews, Jacob, *Verizon Injecting Perma-Cookies to Track Mobile Customers, By-Passing Privacy Controls*, Electronic Frontier Foundation, 3 de noviembre de 2014, disponible en: https://www.eff.org/deeplinks/2014/11/verizon-x-uidh, última fecha de consulta 4 de diciembre de 2018. En la publicación referida la organización EFF advirtió sobre el peligro que representa para la privacidad el uso de los encabezados UIDH que Verizon inserta en el tráfico de datos móviles generado por sus usuarios ya que los identifica de manera única en los sitios que visitan en internet; adicionalmente la organización EFF indicó que el UIDH no puede ser removido no obstante que los usuarios ajusten la configuración de su navegador.

111 *Op.cit.,* Nota 79, p.2, parágrafo 4.

- direcciones electrónicas;
- información acerca de los productos y servicios de Verizon que sus clientes utilizan, incluyendo la información de red propietaria del cliente (CPNI), e
- información demográfica y de interés provista por terceras partes (género, rango de edad e intereses personales, por ejemplo, si el cliente tiene mascotas, le gustan los deportes o con qué frecuencia sale a comer a restaurantes).[112]

Desde que se lanzó el programa Verizon Selects en 2014, a efecto de que los clientes de Verizon participaran en dicho programa, debían de manera afirmativa elegir participar en el programa ya fuera a través de sus cuentas en línea o siguiendo los vínculos provistos por Verizon en su política de privacidad.[113]

Asimismo, de acuerdo a Verizon Wireless, el programa RMA también utiliza varios tipos de información de sus clientes que le permiten enviar publicidad dirigida, tales como: las direcciones electrónicas y dirección postal; cierta información acerca de los productos y servicios de Verizon, como por ejemplo, el tipo de dispositivo que utilizan los usuarios, así como ciertas categorías de interés personal y demográficas que Verizon obtiene de otras empresas, tales como el género, rango de edad e intereses personales.[114] En este caso los clientes reciben un aviso una vez activado el servicio, pero tienen la oportunidad de salirse (*opt out*); no obstante, los suscriptores elegibles son automáticamente inscritos en el programa RMA. Desde su lanzamiento en 2012, los suscriptores tienen la opción de exclusión del programa RMA o de optar por no recibir información relacionada con éste, ya sea a través de sus cuentas en línea o siguiendo los vínculos provistos por Verizon en su política de privacidad.[115] En relación con ambos programas descritos, Verizon inserta el

112 *Ibídem,* p.3, parágrafo 5.

113 Véase la política de privacidad de Verizon Wireless en http://www.verizon.com/about/privacy/policy/ y las preguntas frecuentes en relación con el programa Verizon Selects, Verizon Wireless, disponible en http://www.verizonwireless.com/support/mobile-ads-faqs/, fecha de consulta 30 de noviembre de 2018.

114 *Ídem.*

115 *Op.cit.,* Nota 79, p.3, parágrafo 6.

identificador único UIDH en el tráfico HTTP[116] generado por sus clientes móviles elegibles[117] transmitiéndose sobre la red de Verizon.

En virtud de la investigación realizada se encontró que, aunque Verizon comenzó a insertar el identificador UIDH en el tráfico de Internet de sus clientes a inicios de diciembre de 2012, la empresa comenzó a divulgar la realización de esta práctica hasta octubre de 2014. La FCC también constató que fue hasta marzo de 2015 que Verizon actualizó su política de privacidad para incluir información acerca del UIDH. De hecho, una de las cuestiones que causó aún más preocupación fue que la oficina encargada de la investigación también encontró que al menos uno de los socios de publicidad de Verizon utilizaba el UIDH para propósitos no autorizados con el fin de eludir las opciones de privacidad de los consumidores mediante el restablecimiento de las *cookies* ya borradas. En ese momento Verizon Wireless sostuvo que era poco probable que las empresas de publicidad utilizaran las denominadas *supercookies* para construir perfiles de los consumidores o para cualquier otro propósito, afirmación que fue revertida por parte de la autoridad puesto que con base en diversos informes y reportes de noticias elaborados en 2015,[118] constató que las *cookies* que los usuarios ya habían borrado de sus navegadores fueron restauradas por Turn, Inc., el socio de publicidad en línea de Verizon, asociándolas con los identificadores únicos UIDH de Verizon Wireless. Así, de acuerdo con tales reportes, Turn, Inc. se estaba aprovechando del identificador que utiliza Verizon para monitorear, a su vez y en su propio beneficio, los hábitos de sus clientes en sus dispositivos móviles (*smartphones* y *tablets*) inclusive cuando

116 Las siglas HTTP corresponden a *Hypertext Transfer Protocol*, es decir, de acuerdo a la propia definición de la FCC es el protocolo de aplicación para sistemas distribuidos, colaborativos, hipermedia. HTTP es un método de transporte de datos, textuales o multimedia, a través de internet. Define cómo se formatean y se transmiten los mensajes, y qué acciones deben tomar los servidores web y los navegadores en respuesta a varios comandos. *Op.cit.,* Nota 79, p.1, apartado de Definiciones.

117 Son clientes elegibles para los programas de publicidad descritos, en particular para el programa RMA, la mayoría de los suscriptores y pequeñas empresas, en el entendido de que las líneas celulares de los clientes gubernamentales, corporativos y los operadores móviles virtuales no son elegibles para ser incluidos en el programa RMA. *Op.cit.,* Nota 79, p. 4, especialmente la nota al pie 15.

118 Angwin, Julia y Tigas, Mike, *Zombie Cookie: The Tracking Cookie That You Can't Kill*, Propublica, Enero 14, 2015, disponible en https://arstechnica.com/information-technology/2015/01/zombie-cookie-the-tracking-cookie-that-you-cant-kill/ última fecha de consulta 27 de febrero de 2019.

ya habían hayan sido borrados por los usuarios, ya que Turn, Inc. reaparecía las *cookies* empleadas por el operador inalámbrico.

Adicionalmente también se constató por parte de la autoridad investigadora que el UIDH insertado en el tráfico de Internet desde las líneas móviles, abarcaba clientes corporativos, de gobierno y operadores móviles virtuales de Verizon, los cuales no eran elegibles para participar en los programas de publicidad dirigida de Verizon.[119]

3.2.2 Resolución del caso mediante la imposición del plan de cumplimiento a Verizon Wireless

Concluida la investigación de la FCC, una vez comprobada la práctica de rastreo descrita, la misma fue considerada como una violación por parte de Verizon Wireless a la regla de transparencia prevista en el numeral 8.3 de las Reglas de Internet Abierto de 2010, así como a la regla de privacidad establecida en el artículo 222 de la Ley de Comunicaciones de 1934 cuyo contenido fue objeto de análisis en el capítulo anterior, toda vez que la conducta señalada tenía por objeto conocer por parte del propio Verizon, así como dar a conocer a terceras partes, sin el consentimiento de sus clientes, sus hábitos de consumo y preferencias en virtud de sus actividades en línea, con el único fin de enviarles publicidad dirigida.

De acuerdo con lo dispuesto por la Oficina de Cumplimiento de la FCC, los términos y condiciones a los que se obligó Verizon Wireless a cumplir en virtud del Decreto de Consentimiento (*Consent Decree*) adoptado el 7 de marzo de 2016, se refieren específicamente al uso del UIDH en los programas de publicidad de dicha empresa.[120] En concreto, conviene aclarar que el decreto de cumplimiento aquí señalado no impuso obligaciones al programa Verizon Selects o a aquellos programas de publicidad de Verizon Wireless que requieren el consentimiento previo y expreso del cliente de tipo *opt-in*. Es decir, en cualquier caso, es válida cualquier acción por parte del proveedor de servicios de acceso a internet que implique obtener información propietaria del cliente o compartirla si se cuenta con

119 *Op.cit.,* Nota 79, p.2, parágrafo 4.
120 *Op.cit.,* Nota 79, p.6.

el consentimiento previo del usuario, por lo que evidentemente ello no constituiría una invasión a la privacidad.

Así, en términos del numeral 18(a) del decreto de consentimiento que contempla un plan de cumplimiento al que se obligó a sujetarse Verizon ante la Comisión, el operador de telecomunicaciones inalámbrico se comprometió a no compartir el encabezado UIDH de ningún cliente con una tercera parte con el objeto de enviar publicidad dirigida, a menos que Verizon obtenga el consentimiento previo del cliente (*opt-in*). Al respecto la FCC, por conducto de la Oficina de Cumplimiento, señaló que la opción *opt-in* de participar en el programa Verizon Selects satisface el requisito antes descrito. Asimismo, como parte del plan de cumplimiento, la FCC impuso a Verizon otras restricciones en el siguiente sentido:

> Verizon Wireless mantendrá su práctica actual de (1) eliminar el UIDH de cualquier línea no elegible dentro de un periodo razonable después de la activación y de no utilizar estos UIDHs para ningún propósito; (2) permitir a los clientes elegibles para participar en el programa RMA, de excluirse de no tener insertado un UIDH en su tráfico HTTP; (3) permitir a sus clientes que opten por participar sujeto a lo dispuesto en la subsección 18(a), de salirse posteriormente en cualquier momento, y (4) divulgar las prácticas de Verizon Wireless y el empleo del UIDH en sus políticas de privacidad y en las preguntas frecuentes, así como a actualizar dichas divulgaciones según corresponda.[121]

Cabe recordar que las líneas móviles no elegibles son las que corresponden a clientes de gobierno, corporativos y operadores de redes móviles virtuales, de modo que, en relación con estas líneas, la oficina de cumplimiento de la FCC previó en el mismo decreto objeto de análisis que en el supuesto de que hubiese usos temporales de un UIDH en seguida de la activación de estas líneas, Verizon Wireless debía eliminarlos dentro de los 60 días siguientes a la fecha de inicio de

---

121 *Op.cit.,* Nota 79, p. 10. En el original se lee: *"18. … (c) Verizon Wireless shall maintain its current practice of (1) removing the UIDH from an ineligible line within a reasonable period after activation and not use these UIDHs for any purpose; (2) allowing customers eligible to participate in the RMA program to opt out of having UIDH inserted in their HTTP traffic; (3) allowing customers who opt in pursuant to subsection 18(a) to subsequently opt out at any time, and (4) disclosing Verizon Wireless practices and use of the UIDH in its privacy policies and FAQs and update such disclosures as appropriate".* (Traducción propia).

vigencia del Decreto de Consentimiento. Asimismo, se previó por parte de la FCC que si en el futuro Verizon Wireless quisiese incluir estas líneas en sus programas de publicidad que utilizan UIDH, debía asegurarse de que sus clientes tuviesen las mismas opciones a que se refiere el Decreto de Consentimiento incluyendo las posibilidades relativas a *opt in* y *opt out*.[122]

Adicionalmente, la FCC sujetó a Verizon Wireless a la obligación de designar a un gerente corporativo de alto nivel con autoridad organizacional suficiente para actuar como ejecutivo de cumplimiento para implementar y hacer cumplir los términos y condiciones del Plan de Cumplimiento y del Decreto de Consentimiento. Dicho ejecutivo, además de contar con el conocimiento general de las leyes aplicables en el sector de comunicaciones, deberá tener conocimiento específico acerca de los principios y prácticas en materia de seguridad de la información necesarios para implementar los requisitos del mencionado Decreto de Consentimiento, así como del artículo 222 de la Ley de Comunicaciones y de la regla de transparencia, antes de asumir su cargo. En virtud de lo anterior, la FCC exigió que el ejecutivo de cumplimiento así designado cuente con una certificación en materia de privacidad otorgada por alguna organización certificadora reconocida en la industria y mantenerse al día a través de cursos de educación en materia de privacidad.

Finalmente, en adición al Plan de Cumplimiento señalado, con objeto de resolver y dar por concluido el asunto, la FCC impuso a Verizon Wireless una multa por un monto equivalente a la cantidad de $1,350,000 dólares de los Estados Unidos de América, pagadera a más tardar a los 30 días siguientes a la fecha efectiva del Decreto de Consentimiento suscrito entre Verizon y la FCC.

Como se podrá observar, en relación con el encabezado UIDH cabe precisar que, aun cuando su uso no fue prohibido por la FCC en tanto la empresa investigada sea transparente respecto de su uso frente a los usuarios, siendo precisamente en esa medida que se cumpliría con el objetivo de la neutralidad de la red, al ser las corporaciones que administran la red, responsables de notificar de manera

122 *Op.cit.,* Nota 79, p. 7, en específico la nota al pie 36.

informada a sus clientes las implicaciones que conlleva aceptar su uso con motivo de la navegación por internet que éstos realicen.[123]

3.3 Políticas de privacidad y transparencia de Verizon Wireless

La política de privacidad que Verizon Wireless da a conocer actualmente en su sitio web hace referencia a la utilización del encabezado de identificador único UIDH por lo que se refiere a sus programas de publicidad denominados Publicidad Móvil Relevante y Verizon Selects.[124] Cabe especificar que Verizon hace hincapié en la sección de preguntas frecuentemente realizadas (FAQs por sus siglas en inglés) de su sitio web en el sentido de que el UIDH no contiene datos de identificación personal ni transmite el historial de navegación en Internet de sus clientes a anunciantes u otras personas. Adicionalmente indica que dicho UIDH cambia de manera automática y frecuente como una forma de proteger la privacidad de las personas.

Al respecto, la empresa de comunicaciones móviles explica en la sección de preguntas frecuentes de su página web que el encabezado UIDH únicamente se inserta en circunstancias específicas en las direcciones http de peticiones de datos o contenido de Internet que hace el cliente desde su navegador al servidor web (las cuales no detalla) y, por otro lado, indica que dicho encabezado se inserta en todo el tráfico web a fin de identificar el tipo de dispositivo empleado por el cliente que desea acceder a un determinado contenido o sitio web, el idioma preferido y el contenido compatible, con el fin de que el sitio de destino que recibe la solicitud de

123 Al respecto, el Dr. Lefranc al analizar las implicaciones y consecuencias del ciberespacio en la vida de las personas resalta la importancia de que la técnica esté al servicio de los seres humanos, por lo que, si bien la regulación podría considerarse en algún momento como un impedimento para el desarrollo y la innovación tecnológica cuando a través de ella se limita su uso (como lo podría ser el empleo del UIDH), tal desarrollo no podría estar por encima de la dignidad humana, lo cual conlleva el respeto a la privacidad de las personas y a la protección de sus datos. Así, de acuerdo a Lefranc es a través de la técnica, considerada como un medio al servicio y en beneficio de los seres humanos, que éstos pueden hacer valer los fines que cada uno persiga buscando que se respete siempre la dignidad de las personas; lo contrario es aceptar el denominado imperativo tecnológico que a través de su mandato hace que las personas se diluyan frente a la técnica al no ser las primeras el principal eje rector. Véase Lefranc, César, Terra Incógnita. Bases para una política criminal pro persona en la Sociedad digital, México, Infotec, 2015, p. 51.

124 Véase https://es.verizonwireless.com/support/unique-identifier-header-faqs/. Última fecha de consulta: 10 de octubre de 2018.

datos pueda mostrar el contenido del sitio de la mejor manera en el teléfono o dispositivo móvil que emplea el usuario.

En cuanto a las opciones de consentimiento que puede ejercer un cliente de Verizon se tiene lo siguiente:

Únicamente si el cliente ejerció la opción de exclusión (*opt-out*) del programa de Publicidad Móvil Relevante, Verizon deja de insertar el UIDH en el tráfico de internet, a no ser que también el cliente haya optado por inscribirse o participar (*opt-in*) en el Programa Verizon Selects. En este último caso, el identificador UIDH continuará estando presente aun cuando el cliente haya optado por salirse del programa de Publicidad Móvil Relevante.[125]

Asimismo, en caso de que el cliente opte por seleccionar o participar en el programa Verizon Selects, se entiende que el UIDH puede ser compartido con socios anunciantes de Verizon que proporcionan servicios de publicidad y que están autorizados a utilizar ese encabezado únicamente como parte de los servicios de Verizon y no para sus propios usos.

Cabe precisar que de acuerdo al programa de publicidad dirigida Verizon Selects, en su sección de preguntas frecuentes[126] indica que la información personal que obtiene de sus usuarios es compartida con Oath, la empresa que se formó en virtud de la fusión entre AOL y Yahoo cuya adquisición realizó Verizon en 2015 y 2017, respectivamente, a través de la cual busca incrementar su negocio en publicidad móvil aprovechando el acceso a las cuentas de correo electrónico de millones de usuarios que tenía Yahoo.[127]

Entre la información que utiliza de sus clientes a través del programa Verizon Selects se encuentran las direcciones web de los sitios que visitan, información sobre las aplicaciones que tienen instaladas en sus dispositivos móviles, identificadores de dispositivos y publicidad; información sobre la ubicación del dispositivo móvil; direcciones postales y de correo electrónico; asimismo emplea

125 *Ídem.*

126 Véase https://www.verizonwireless.com/support/verizon-selects-faqs/, última fecha de consulta el 11 de enero de 2019.

127 Ruiz de Gauna, C, *¿Por qué Verizon compra Yahoo!?*, Expansión, 25 de julio de 2016, disponible en http://www.expansion.com/empresas/tecnologia/2016/07/24/579517f622601de2228b45a2.html, última fecha de consulta el 27 de febrero de 2019.

información que obtiene de otras empresas como sexo, rango de edad, intereses y preferencias de compra así como respuestas a anuncios que proporcionan los mismos clientes.

Actualmente Verizon Wireless cuenta con un programa de recompensas denominado *Verizon-Up*,[128] el cual únicamente aplica para sus clientes de telefonía móvil de pospago que se hayan registrado previamente en el programa de publicidad dirigida Verizon Selects. De acuerdo con dicho programa de recompensas, por cada 300 dólares de consumo mensual en la factura de sus servicios, Verizon otorga un crédito canjeable por una recompensa (ofertas que abarcan desde un café, hasta boletos para un concierto, eventos deportivos o programas de televisión, así como descuentos y beneficios en la compra de servicios o accesorios proporcionados por Verizon). Como podrá observarse, al estar asociado y condicionado el programa de recompensas a la inscripción del programa Verizon Selects, implica que Verizon está solicitando el consentimiento previo de sus clientes para el uso de su información personal relativa a su historial de navegación, intereses, ubicación, etc., a cambio de participar en el programa de recompensas, además de que emplea dicha información para orientar de manera personalizada las propias recompensas y beneficios de su programa Verizon-Up. Lo anterior va acorde con las consideraciones regulatorias que la FCC impuso a Verizon Wireless en marzo de 2016 lo que denota, al menos en este aspecto, que el operador inalámbrico busca alinearse al objetivo de respetar la confianza de sus clientes respecto a la confidencialidad de su información personal.

No obstante lo anterior, de acuerdo con las sección de preguntas frecuentes de Verizon Selects, la información recolectada por parte de Verizon de aquellos clientes que aceptaron participar en este programa de publicidad dirigida, a pesar de que retiren su consentimiento para dejar de formar parte del mismo, puede ser conservada por tres años.[129] Incluso se indica, no obstante que se haya solicitado a Verizon por parte de un cliente que se abstenga de utilizar información recopilada

128 https://www.verizonwireless.com/support/verizon-up-faqs/, última fecha de consulta el 5 de enero de 2019.

129 *Op.cit.,* Nota 126.

previamente con su consentimiento, relativa a la localización de su dispositivo móvil y a la navegación que haya realizado a través de Internet, que la misma podrá seguir utilizándose "para fines analíticos y de modelado"[130] sin que se explique a qué se refiere lo anterior. Al respecto podríamos considerar debido al lenguaje ambiguo y poco preciso del operador inalámbrico que, ni la información personal de los usuarios es borrada de manera inmediata o automática ni que vaya a dejar de ser utilizada por el operador con el objeto de continuar creando perfiles personalizados de sus clientes para el envío de publicidad dirigida, lo cual genera incertidumbre en cuanto al manejo de la información conservada por parte de Verizon Wireless.

Otro aspecto que generó consternación fue el hecho de que para dejar de participar en un programa de publicidad como es el de Verizon Selects o el de Oath, no basta con que un cliente utilice los controles de su navegador para borrar las *cookies* de seguimiento de su dispositivo móvil ni tampoco mediante la eliminación de su historial de navegación como tradicionalmente creen los usuarios que es un modo efectivo de evitar ser rastreados, sino que deben seguirse los pasos señalados específicamente por el operador en su página web.[131]

Así también para optar por evitar que su información personal continúe siendo utilizada para propósitos de publicidad por parte de Oath, un cliente debe seleccionar la opción de exclusión *opt-out* en cada uno de los dispositivos que emplea y para cada uno de los navegadores que utiliza debiendo realizar el mismo proceso en todos ellos, lo cual no otorga en modo alguno certeza al usuario puesto que éste puede no recordar o estar confundido sobre el uso de todos los navegadores que ha empleado. Además, el hecho de que un cliente bloquee o borre las *cookies* de seguimiento de su navegador, de acuerdo a Verizon respecto de la publicidad dirigida de Oath, puede cancelar la opción que se haya realizado

130 *Ídem.* En el numeral 8 de la información general provista en las FAQs del programa Verizon Selects se lee: Usted puede indicar a Verizon que deje de utilizar la información recolectada con anterioridad acerca de su navegación por internet y su ubicación en el programa Verizon Selects visitando el Centro de Preferencias de Verizon Selects. La información previamente recopilada puede continuar siendo utilizada para fines analíticos y de modelado. (énfasis añadido) En el idioma original: *You can also instruct Verizon to stop using past data it has collected about your web browsing and location in the Verizon Selects program by visiting the Verizon Selects Preference Center. Information previously collected may continue to be used for analytics and modeling purposes.* (traducción propia).

131 *Op.cit.,* Notas 114 y 126.

mediante la selección del mecanismo de *opt-out* empleado por parte de un cliente, lo cual resulta absolutamente injustificado.[132]

Por lo que se refiere al UIDH que Verizon comparte con la empresa Oath y las opciones que ésta ofrece a los usuarios en relación con el uso de su información para propósitos del envío de publicidad personalizada, resulta bastante confuso. Por un lado, Oath permite a los usuarios excluirse de la recepción de anuncios publicitarios basados en la información que recopila de ellos mediante un procedimiento largo y confuso para lo cual tienen que utilizar la herramienta de elección para los consumidores a través de la página web de la Alianza de Publicidad Digital (*Digital Advertising Alliance*) y seleccionar tanto a la empresa AOL como Yahoo. Esta opción de exclusión únicamente aplica al navegador específico que el usuario utiliza cuando hace valer dicha opción, de modo que, en el supuesto de que utilice múltiples navegadores o equipos, debe repetir este procedimiento para cada uno. Además, el hecho de que el usuario bloquee o elimine las *cookies* de su navegador, de acuerdo con las propias instrucciones de Oath, dicha circunstancia puede cancelar la elección de exclusión que haya ejercido previamente. También indica dicha empresa que el usuario puede elegir la opción de exclusión que evite la recepción de anuncios personalizados en su equipo móvil mediante el uso de la alternativa denominada “Limitar el Seguimiento de Anuncios” (*Limit ad tracking*) o cualquier capacidad similar que permita el equipo del usuario. Lo anterior genera incertidumbre debido a que las opciones para evitar el rastreo en virtud de la navegación que realizan los usuarios todos los días, son varias y conllevan la necesidad de leer y entender las extensas políticas de privacidad que las empresas unilateralmente imponen a los primeros.[133]

Adicionalmente, cabe resaltar que el lenguaje empleado no es claro y tratándose de la traducción del mismo al idioma español presenta varias deficiencias por lo que las consecuencias de elegir una determinada opción de exclusión no garantizan que el usuario haya entendido de manera inmediata y clara que

132 *Op.cit.,* Nota 126, en específico el numeral 12 de la información general provista en las FAQs del programa Verizon Selects.

133 *Ídem.*

efectivamente una empresa dejará de rastrear sus movimientos en línea para crear perfiles personalizados.

Como se podrá observar, el problema de las opciones de exclusión que habilitan las empresas a través de los sitios web o las aplicaciones que proveen servicios es que, cuando establecen una configuración predeterminada respecto de algún servicio o aplicación (mecanismo por *default*), como por ejemplo la ubicación geográfica, las personas no lo cancelan puesto que no conocen que existen otras opciones a elegir y prefieren permitir la recolección de sus datos, más aún cuando las empresas de una u otra forma coercen a los usuarios para que estén dispuestos a ceder su información a cambio de permitirles acceso al contenido que buscan en internet o hacer uso de aplicaciones o servicios.[134]

Así, no obstante la investigación realizada por la FCC en contra de Verizon Wireless, el plan de cumplimiento al cual se le sujetó y la multa que se le impuso, el problema que subyace en torno a este tema es que, tal como lo reportan recientemente los propios consumidores y los medios,[135] hoy en día las empresas telefónicas, los ISP así como los proveedores de aplicaciones continúan invadiendo la privacidad sin que los usuarios tengan conocimiento de ello o entiendan realmente cómo funciona el rastreo de su información en línea.

3.4. Análisis y reflexiones en torno a la neutralidad de la red desde una visión del autor

La política de neutralidad de la red en los Estados Unidos de América ha pasado durante los últimos años por constantes cambios al grado de generar confusión con motivo de las posturas un tanto divergentes que ha sostenido la propia FCC, así como debido a la diversidad de opiniones y puntos de vista de los múltiples actores que en dicho país han tenido una gran influencia sobre este tema e incluso sobre

134 Véase King, Jen, *Change your phone settings so Apple, Google can't track your movements,* The Conversation, 14 de enero de 2019, https://theconversation.com/change-your-phone-settings-so-apple-google-cant-track-your-movements-109059, última fecha de consulta 26 de febrero de 2019.

135 Jennifer Valentino-Devries, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret,* diciembre, 2018. Disponible en: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html, última fecha de consulta 27 de febrero de 2019.

las decisiones de la FCC, como ya se ha mencionado. Por un lado, la transparencia ha sido un tema fundamental para la FCC el cual se ha mantenido intacto para proteger y preservar la neutralidad de la red, mientras que, por otro lado, la protección a la privacidad en internet que durante solo poco más de un par de años fue competencia de la FCC, ha pasado nuevamente a la jurisdicción de la FTC, lo que reflejó durante 2018 la tensión entre el Congreso Federal de los Estados Unidos y la FCC en virtud de la cual el primero ha logrado que se evite el control sectorial de la FCC sobre este tema al anularse las reglas de privacidad de 2016 aplicables a los ISP.[136]

Únicamente la resolución de nuevos casos podrá demostrar si el nuevo enfoque adoptado por la FCC, vigente a partir de junio de 2018, resulta efectivo para considerar que solo mediante la aplicación de la regla de transparencia, bien implementada por los proveedores de acceso a internet (lo que implica divulgar información precisa y completa sobre cualquier práctica que realicen), permitirá el respeto a la libertad de elección de los usuarios en internet.

Indudablemente, el camino que ha seguido la neutralidad de la red en los Estados Unidos tendrá una gran influencia sobre lo que se decidirá al respecto por parte de la autoridad regulatoria en nuestro país. Al respecto, más allá de lo que prevé actualmente la Ley Federal de Telecomunicaciones y Radiodifusión en México que consagra en su artículo 145 los principios de la neutralidad de la red tales como transparencia e información, libertad de elección, privacidad y gestión de tráfico y administración de la red, entre otros, en nuestro país aún no se ha realizado la consulta pública necesaria para la emisión y publicación de los lineamientos de carácter general que prevé dicha disposición legal en materia de neutralidad de la red y que deberán regular lo dispuesto en la ley señalada. La falta de regulación en México conlleva a que los operadores de redes que proporcionan el servicio de acceso a Internet puedan actuar sin sujetarse a parámetros de transparencia que al efecto se definan en cuanto a la forma en que manejan y gestionan el tráfico de datos que se transmite a través de sus redes. De ahí que resulta importante dar seguimiento a nuevos casos que surjan en los Estados

136 Véanse notas al pie 70 y 71.

Unidos en los que únicamente se considerará como aplicable la regla de transparencia en materia de neutralidad de la red, ya que la resolución de los mismos constituye un punto de referencia necesario para México ante la necesidad o no de imponer medidas de carácter obligatorias para impedir la falta de transparencia derivada del manejo arbitrario o engañoso, tratándose de la gestión de tráfico y administración de la red por parte de los operadores responsables de su manejo.

No sobra mencionar que, ante el surgimiento de un nuevo tratado de libre comercio entre México, Estados Unidos y Canadá (T-MEC), que sustituiría al vigente, se reconocerá en dicho instrumento internacional la necesidad de proteger la información personal de los consumidores en línea basado en la adopción de medidas transparentes, así como también tendría lugar el reconocimiento al acceso y uso de internet, de los servicios y aplicaciones provistos por los proveedores de contenido de información que sean de la elección del consumidor, todo ello, sujeto a una administración razonable de la red, lo cual no es otra cosa que el respeto al principio de la neutralidad de la red.[137]Lo anterior implica a su vez que los usuarios tendrán derecho a "acceder a información sobre las prácticas de administración de redes del proveedor del servicio de acceso a Internet",[138] de modo que la capacidad de éstos de gestionar el tráfico e incluso la posibilidad que tienen de restringir el acceso a contenidos o materiales que consideren perjudicial u objetable,[139] debe equilibrarse mediante la aplicación adecuada de medidas transparentes en beneficio de los usuarios a fin de garantizar el respeto a libre elección de los consumidores.

Bajo mi perspectiva, la nueva orden de internet abierto de los Estados Unidos emitida en diciembre de 2017 no significa que la neutralidad de la red haya

137 Véase el capítulo 19 sobre Comercio Digital conforme al texto aprobado por los tres países, sujeto aún a ratificación por parte del Senado, disponible en https://www.gob.mx/cms/uploads/attachment/file/401191/19ComercioDigital.pdf, última fecha de consulta el 14 de marzo de 2019.

138 Artículo 19.10 inciso c) del T-MEC.

139 Véase el contenido del artículo 19.17.3 del texto del T-MEC, así como el anexo 19-A en el que se establece que el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión de México no resultaría incompatible con lo dispuesto en el artículo 19.17.3 citado. Lo anterior solo es posible interpretarlo en la medida en que los ISP respeten el principio de transparencia, fundamental para la neutralidad de la red.

terminado, en la medida en que la regla de transparencia vigente efectivamente lleve a una mayor apertura en internet, lo cual depende del compromiso serio por parte de los ISP de divulgar sus prácticas que puedan significar afectación o limitación al derecho de los usuarios de acceder a contenidos en línea o cualquier otra que conlleve una afectación a la velocidad del servicio provisto por ellos; el incumplimiento a lo anterior se verá reflejado indudablemente a corto plazo en los casos que lleguen a plantearse ante la propia FCC, la FTC e incluso las cortes judiciales de ese país.

Conclusiones

Conclusiones

La violación a la regla de transparencia a que se refieren las Reglas de Internet Abierto conlleva, necesariamente para el caso analizado, la violación a la confidencialidad y privacidad de las personas en tanto que se priva a éstos de la oportunidad de decidir de manera razonada y anticipada si desean que su información personal sea recolectada y, por ende, de la posibilidad de seleccionar si desean o no recibir información publicitaria con base en sus intereses y preferencias.

Como se explicó en este trabajo de investigación, la violación fundamental por parte de Verizon Wireless consistió en inyectar encabezados de seguimiento en el tráfico de sus usuarios móviles al momento de acceder a una determinada página web sin que tuvieran conocimiento de ello y sin que hubiere mediado consentimiento al respecto, es decir, tal conducta ocurrió fuera del control del usuario. Si bien durante el curso de la investigación Verizon Wireless cambió sus prácticas al actualizar su política de privacidad frente a sus clientes y el público en general, para dar a conocer el uso del encabezado único UIDH, e incluso para permitir a sus clientes, mediante la opción de exclusión (*opt-out*) de su programa de publicidad relevante, lo cual implica que dejaría de inyectar los encabezados y que no utilizaría los perfiles de sus clientes para el envío de publicidad móvil, no obstante, ello no significa que el operador se abstenga de retener o recopilar la información de los clientes o que emplee otros mecanismos para rastrear su actividad en línea.

Ahora bien, el hecho de que la FCC haya permitido como forma válida el mecanismo de exclusión (*opt-out*) para que los usuarios móviles de Verizon decidan, de manera posterior a la afectación a su privacidad, oponerse a la posibilidad de ser rastreados en virtud de su actividad en línea mediante la inserción del identificador único UIDH, ello no garantiza la privacidad de las personas ya que únicamente refleja que mientras no se oponga un usuario de internet o no anule el consentimiento tácito cuyo otorgamiento se da por sentado, resulta válido el uso y compartición de su información entre sus filiales y subsidiarias para el envío de publicidad móvil; es así que considero que en cualquier caso el envío de publicidad personalizada según los intereses específicos de cada persona debiera operar bajo

un mecanismo de consentimiento previo e informado ya que esta sería la única forma en que, sin afectar o poner en riesgo la privacidad, se pueda enviar o compartir información respecto de aquellos usuarios o consumidores que efectivamente han manifestado su interés en que se creen perfiles personalizados y recibirla.

De acuerdo con el nuevo enfoque regulatorio que tiene la FCC respecto a la implementación de la regla de transparencia, la mera obligación impuesta a los ISP para divulgar de manera pública sus prácticas en relación con el manejo y administración de la red así como sobre los términos y condiciones comerciales bajo los cuales ofrecen el servicio de acceso a internet de banda ancha, resulta suficiente por sí sola, debido a que los consumidores tiene además la posibilidad de solicitar la protección que otorgan las leyes de protección al consumidor bajo la autoridad que le compete actualmente a la FTC.

Como se ha mencionado a lo largo de este trabajo, en los Estados Unidos de América ha habido una inmensa cantidad de argumentos en favor y en contra en relación con: a) la necesidad de mantener o no vigentes las reglas de internet abierto (no bloqueo, no ralentización y transparencia) y b) la autoridad que debe vigilar la privacidad en línea de los usuarios con motivo de la prestación de los servicios de internet de banda ancha, a falta de una ley federal. Lo anterior ha sufrido en muy pocos años considerables cambios en la regulación relativa a la apertura en internet y a los servicios de banda ancha, como ya se ha explicado, no obstante, tomando en cuenta las expectativas que cualquier usuario de internet puede tener, de manera razonable, sobre el manejo de su información, se concluye lo siguiente:

1. Mantener al día de hoy la obligación de transparencia como parte de las reglas de internet abierto emitidas por la FCC desde 2010 a cargo de los ISP, es fundamental para contribuir al carácter abierto de internet, así como para aminorar, sin que se elimine, la posibilidad de que estos actores afecten los derechos de los consumidores e incluso para mejorar la confianza que éstos tienen en sus proveedores de acceso a internet.

2. Con independencia de que la autoridad competencial en materia de privacidad recaiga actualmente en la FTC por lo que se refiere a aquellos operadores de telecomunicaciones que proveen servicios de internet de banda ancha, resulta apropiado que la actual orden de internet continúe imponiendo a éstos obligaciones de transparencia respecto a los términos y condiciones de la provisión de sus servicios, lo cual abarca la obligación de divulgar prácticas que impliquen el bloqueo a contenidos provistos por terceros o la degradación del tráfico de sus usuarios de internet. De ahí la importancia de que tanto la FCC como la FTC actúen de manera coordinada en los supuestos de violaciones a la obligación de transparencia.
3. No obstante lo anterior, incluso bajo el caso descrito mediante el cual la FCC impuso a Verizon Wireless un plan de cumplimiento para divulgar de manera adecuada sus prácticas y los mecanismos de elección que tienen sus clientes, los usuarios carecen de control absoluto sobre su información debido, por un lado, a la adecuada implementación de la regla de transparencia a través de las políticas de privacidad de los ISP y, por el otro, a la falta de entendimiento en relación con los términos y condiciones relativos a la provisión del servicio de acceso a internet, entre ellos, la forma en que su información es recolectada y utilizada y la manera en que esto puede evitarse. Por lo tanto, los usuarios de Internet no pueden tener de manera exclusiva la carga del control sobre su propia información mientras carezcan de un entendimiento claro y completo sobre las implicaciones de su recolección y uso por parte de las empresas de internet. La falta de consistencia entre el contenido de las políticas de privacidad de los ISP y los requisitos que les impone la regla de transparencia (información precisa y completa) impiden un control real y efectivo por parte del usuario.
4. Aun cuando algunos usuarios estén dispuestos a ceder a los ISP su información o incluso a tolerar el bloqueo o degradación del contenido y velocidad en internet a cambio de otro tipo de beneficios, en su

mayoría de tipo comercial, el control que deben tener sobre su información y los usos que de ella se hagan debe traducirse en decisiones valiosas y significativas ya que, el supuesto contrario, no significa que no exista una violación a la apertura en internet; lo anterior implica un entendimiento claro y completo mediante una explicación breve por parte de las empresas que recopilan sus datos acerca de los riesgos y consecuencias que conllevan su ingreso en línea a cualquier página de internet, así como sus actividades en línea; en consecuencia, los avisos y políticas de privacidad deben ser breves, claros y completos sin que ello implique confusión alguna para los usuarios de Internet puesto que la mayoría de dichos avisos no resultan de ayuda para los usuarios como se ha explicado.

5. Los actores que participan en el ecosistema de Internet constituyen, cada uno por separado, una pieza fundamental para vigilar o monitorear dicho entorno, de modo que cualquier conducta que violente la regla de transparencia en perjuicio de los derechos de los usuarios será inevitablemente denunciada e incluso lo anterior permite que la opinión de la autoridad, en este caso, la FCC, se informe de esa variedad de puntos de vista al momento de resolver un caso. En el caso Verizon Wireless, debido a la presión ejercida por múltiples actores (quejas de consumidores, prensa, organizaciones de protección al consumidor, etc.), el operador inalámbrico optó por evitar un conflicto judicial, así como en la medida de lo posible la pérdida de confianza de sus usuarios y llegar a un acuerdo con la FCC. Así, la gran variedad de puntos de vista y perspectivas en relación con el internet abierto, así como respecto a la privacidad en línea, ha incrementado de algún modo el balance entre los intereses comerciales de las empresas para obtener los datos e información personal de los usuarios; el derecho de éstos a acceder a cualquier tipo de contenido y servicios en internet, y las expectativas que tienen en relación con el manejo de sus datos e información de carácter personal.

6. La industria y demás actores involucrados deben implementar herramientas de bloqueo basadas en estándares de seguridad razonables en el sentido de que cumplan las expectativas que un usuario promedio tiene, en la medida que impidan de una sola vez, de manera segura, sencilla y consistente, no solo el seguimiento de las actividades en línea sino incluso la recopilación de datos, sin que lo anterior condicione bajo ningún supuesto o ralentice el acceso por parte de los usuarios al contenido en internet, a menos que el usuario otorgue su consentimiento para ello; esto último no impide que se afecte la libertad de información y de expresión ya que en este supuesto la noción de consentimiento informado resulta bastante cuestionable incluso desde el punto de vista ético puesto que la elección del usuario no es absolutamente libre.
7. Más allá de la existencia de reglas sectoriales en materia de privacidad en los Estados Unidos de América, frente a la falta de una legislación general en este ámbito, la auto regulación honesta a través de las políticas de privacidad por parte de los diversos actores que conforman el entorno en internet resulta fundamental para proveer a los usuarios de manera efectiva y lo más transparente posible de opciones que permitan realizar una elección real conforme a sus intereses.
8. Si bien Internet debe mantenerse neutral en el sentido de no favorecer determinados tipos de tráfico o contenidos sobre otros con el objeto de no afectar la competencia, también debe mantenerse neutral para no favorecer los modelos de negocios de las empresas y de sus socios anunciantes en tanto ello lleve aparejado, en pro de un mercado sumamente lucrativo, un riesgo a la invasión de la privacidad de las personas. De ahí que, en el caso concreto, se observa que el hecho de no garantizar la neutralidad de la red, así como el respeto a la regla de transparencia, constituye un riesgo al ejercicio y salvaguarda de los derechos humanos como la protección a la información personal de los usuarios.

Referencias

Bibliografía

BERNERS-LEE, Tim, *30 years on, what's next #ForTheWeb?*, disponible en https://webfoundation.org/2019/03/web-birthday-30/, última fecha de consulta 14 de marzo de 2019.

Comisión Federal de Comercio, *Federal Register*, "Children's Online Privacy Protection Rule; Final Rule", Vol. 78, No. 12, enero 2013, Washington, D.C., 2013, disponible en https://www.ftc.gov/system/files/2012-31341.pdf, última fecha de consulta 28 de noviembre de 2018.

_____, *Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission: In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 27 de mayo de 2016, pp. 20-22, disponible en: https://www.ftc.gov/news-events/press-releases/2016/05/ftc-staff-provides-comment-fccs-proposed-privacy-rulemaking, última fecha de consulta 25 de noviembre de 2018.

Comisión Federal de Comunicaciones, *Federal Register*, "Preserving the Open Internet; Final Rule", Vol. 76, No. 185, septiembre 2011, Washington, D.C., 2011, disponible en https://www.federalregister.gov/documents/2011/09/23/2011-24259/preserving-the-open-internet. Última fecha de consulta 3 de febrero de 2019.

_____, *Federal Register*, "Protecting and Promoting the Open Internet; Final Rule", Vol. 80, No. 70, abril 2015, Washington, D.C., 2015, disponible en https://www.federalregister.gov/documents/2015/04/13/2015-07841/protecting-and-promoting-the-open-internet. Última fecha de consulta 23 de febrero de 2019.

_____, *Federal Register*, “Restoring Internet Freedom; Final Rule”, Vol. 83, No. 36, febrero 2018, disponible en https://www.federalregister.gov/documents/2018/02/22/2018-03464/restoring-internet-freedom, Última fecha de consulta el 23 de diciembre de 2018.

_____, *Consent Decree, In the Matter of Cellco Partnership, d/b/a Verizon Wireless*, DA 16-242, Washington, D.C., 2016, disponible en https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0307/DA-16-242A1.pdf, Última fecha de consulta 3 de enero de 2019.

_____, *In the Matter of Use of the Carterfone Device in Message Toll Telephone Service*, 13 F.C.C. 2d 420, Washington, D.C., junio de 1968, disponible en https://web.archive.org/web/20150120021035/http://www.uiowa.edu/~cyberlaw/FCCOps/1968/13F2-420.html, última fecha de consulta 16 de septiembre de 2018.

_____, *Policy Statement*, FCC 05-151, Washington DC, 2005, disponible en https://docs.fcc.gov/public/attachments/FCC-05-151A1.pdf. Última fecha de consulta 26 de septiembre de 2018.

_____, *Privacy Order, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Washington, D.C., 2016. Disponible en: https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy. Última fecha de consulta 7 de enero de 2019.

Comisión Federal de Comunicaciones y Comisión Federal de Comercio, *Decision, Restoring internet freedom FCC-FTC memorandum of understanding*, diciembre 2017. Disponible en https://www.fcc.gov/document/fccftc-sign-mou-coordinate-online-consumer-protection-efforts, última fecha de consulta 23 de febrero de 2019.

COOPER, Tyler, *FCC vs FTC: Who polices the Internet after net neutrality?,* Broadbandnow, 6 de marzo de 2018, disponible en https://broadbandnow.com/report/fcc-vs-ftc-police-internet/, última fecha de consulta 2 de febrero de 2019.

HOFFMAN-ANDREWS, Jacob, *Verizon Injecting Perma-Cookies to Track Mobile Customers, By-Passing Privacy Controls,* Electronic Frontier Foundation, 3 de noviembre de 2014, disponible en: https://www.eff.org/deeplinks/2014/11/verizon-x-uidh, última fecha de consulta 4 de diciembre de 2018.

Internet Society, disponible en: http://InternetSociety.org. Última fecha de consulta el 20 de agosto de 2018.

_____, *The Open Internet, What is, and how to avoid mistaking it for something else*, Estados Unidos, 2014. Disponible en: https://www.internetsociety.org/resources/doc/2014/the-open-internet-what-it-is-and-how-to-avoid-mistaking-it-for-something-else/. Última fecha de consulta el 20 de agosto de 2018.

_____, *Open Inter-networking: Getting the fundamentals right: access, choice, and transparency*, Estados Unidos, 2010. Disponible en: http://www.internetsociety.org/open-inter-networking-getting-fundamentals-right-access-choice-and-transparency. Última fecha de consulta el 20 de agosto de 2018.

KING, Jen, “Change your phone settings so Apple, Google can’t track your movements”, en The Conversation, 14 de enero de 2019, https://theconversation.com/change-your-phone-settings-so-apple-google-cant-track-your-movements-109059, última fecha de consulta 26 de febrero de 2019.

LÓPEZ JIMÉNEZ, David, “Las cookies como instrumento para la monitorización del usuario en la Red: la publicidad personalizada”, *Revista de Ciencias Económicas*, San José, Vol. 29, núm. 2, julio 2011, disponible en línea en https://revistas.ucr.ac.cr/index.php/economicas/article/view/7018/6703, última fecha de consulta el 9 de diciembre de 2018.

MAYER, Jonathan, *How Verizon´s Advertising Header Works*, octubre de 2014, disponible en http://webpolicy.org/2014/10/24/how-verizons-advertising-header-works/, última fecha de consulta el 6 de diciembre de 2018.

_____, *The Turn-Verizon zombiecookie*, enero de 2015, disponible en http://webpolicy.org/2015/01/14/turn-verizon-zombie-cookie/, última fecha de consulta el 3 de marzo de 2019.

MAYER, Jonathan R. y Mitchell, John C., *Third Party Web Tracking. Policy and Technology*, Foro Mundial sobre Seguridad y Privacidad del Instituto de Ingenieros Eléctricos y Electrónicos, California, 2012, Disponible en https://jonathanmayer.org/publications/trackingsurvey12.pdf, Última fecha de consulta el 1 de marzo de 2019.

Organización para la Cooperación y el Desarrollo Económicos, *Perspectivas de la OCDE sobre la economía digital 2015*, París, 2015, disponible en línea en: http://dx.doi.org/10.1787/9789264259256-es, última fecha de consulta el 6 de septiembre de 2018.

PISANTY, Alejandro, “Principios fundamentales de la gobernanza de Internet”, *Pensar Internet*, México, Universidad Iberoamericana, 2016.

PISANTY, Alejandro y Huesca, Erik, *Neutralidad de la red en Internet*, México, 2015, disponible en línea en: https://www.isoc.mx/wp-content/uploads/2017/11/Neutralidad_de_la_Red_en_Internet-1.pdf. Última fecha de consulta 3 de septiembre de 2018.

PUBLIC KNOWLEDGE, *Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World*, Washington, D.C., 2016, disponible en https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper.pdf. Última fecha de consulta el 1 de marzo de 2019.

ROCHET, Jean-Charles y Tirole, Jean, "Two Sided Market: a Progress Report", *The Rand Journal of Economics*, Volumen 37, número 3, Septiembre 2006, pp. 645-667 disponible en https://www.researchgate.net/publication/227651905_Two-sided_Markets_A_Progress_Report, Última fecha de consulta 7 de diciembre de 2018.

RUIZ DE GAUNA, C, *¿Por qué Verizon compra Yahoo!?*, Expansión, 25 de julio de 2016, disponible en http://www.expansion.com/empresas/tecnologia/2016/07/24/579517f622601de2228b45a2.html, última fecha de consulta el 27 de febrero de 2019.

Senado de los Estados Unidos, Subcomité de Privacidad, Tecnología y Derecho, "Examining the Proposed FCC Privacy Rules", mayo de 2016, disponible en https://www.judiciary.senate.gov/imo/media/doc/Wheeler%20Responses%20to%20QFRs.pdf. Última fecha de consulta el 6 de diciembre de 2018.

SOMMER, Jeff, *Defending the Open Internet*, New York Times, 10 de mayo de 2014, disponible en https://www.nytimes.com/2014/05/11/business/defending-the-open-internet.html, última fecha de consulta 5 de septiembre de 2018.

SWIRE, Peter, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, The Institute for Information Security & Privacy at Georgia Tech, 2016, disponible en http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf. Última fecha de consulta: 23 de noviembre de 2018.

TIMBERG, Craig, *Verizon, AT&T Track Their Users with 'Supercookies',* Washington Post, 3 de noviembre de 2014, disponible en http://www.washingtonpost.com/business/technology/verizon-atandt-tracking-their-users-with-supercookies/2014/11/03/7bbbf382-6395-11e4-bb14-4cfea1e742d5_story.html, última fecha de consulta 11 de enero de 2019.

VALENTINO-DEVRIES, Jennifer *et al.*, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret,* New York Times, 10 de diciembre de 2018, disponible en: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html, última fecha de consulta 27 de febrero de 2019.

VERIZON WIRELESS, *How Verizon Selects from Verizon Wireless Works*, diciembre de 2012, disponible en *https://www.verizon.com/about/news/vzw/2012/12/verizon-selects*, última fecha de consulta: 25 de noviembre de 2018.

_____, Política de Privacidad Completa, disponible en *http://www.verizon.com/about/privacy/policy/*, última fecha de consulta 30 de noviembre de 2018.

_____, Preguntas Frecuentes Publicidad Móvil Relevante, disponible en *http://www.verizonwireless.com/support/mobile-ads-faqs/*, fecha de consulta 30 de noviembre de 2018.

_____, Preguntas Frecuentes UIDH, disponible en *https://es.verizonwireless.com/support/unique-identifier-header-faqs/*. Última fecha de consulta el 10 de octubre de 2018.

_____, Preguntas Frecuentes Verizon Selects, disponible en *https://www.verizonwireless.com/support/verizon-selects-faqs/*, última fecha de consulta el 11 de enero de 2019.

_____, Preguntas Frecuentes Verizon-up, *https://www.verizonwireless.com/support/verizon-up-faqs/*, última fecha de consulta el 5 de enero de 2019.

WU, Tim, Net neutrality, *Broadband discrimination,* Estados Unidos de América, 2003, disponible en línea en http://dx.doi.org/10.2139/ssrn.388863, Última fecha de consulta 16 de septiembre de 2018.

WU, Tim y Yoo, Christopher, "Keeping the Internet neutral?: Tim Wu and Christopher Yoo Debate", *Federal Communications Law Journal*, 2007, Vol. 59: Iss. 3, artículo 6, disponible en: http://www.repository.law.indiana.edu/fclj/vol59/iss3/6. Última fecha de consulta el 10 de octubre de 2018.

Recursos Jurídicos

Joint Resolution, S.J. Res. 34, 115th Congress Public Law 22, 2017, Estados Unidos de América.

Ley Federal de Telecomunicaciones y Radiodifusión, 2018, México.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Última fecha de consulta 16 de diciembre de 2018.

Tratado entre México, Estados Unidos y Canadá (T-MEC), capítulo 19 sobre Comercio Digital, disponible en https://www.gob.mx/cms/uploads/attachment/file/401191/19ComercioDigital.pdf, última fecha de consulta el 14 de marzo de 2019.

United States Code, 2017, Estados Unidos de América.

Resoluciones judiciales

Corte de Distrito de los Estados Unidos del Distrito Norte de California, United States v. Yelp Inc., No. 3:14-CV-04163, Stipulated order for permanent injunction and civil penalty judgment, 16 de septiembre de 2014. Disponible en: https://www.ftc.gov/system/files/documents/cases/140917yelpstip.pdf, última fecha de consulta 27 de enero de 2019.

Tribunal de Apelaciones de Estados Unidos del Noveno Circuito, Federal Trade Commission v. AT&T Mobility LLC, No. 15-16585 D.C., 26 de febrero de 2018, disponible en https://www.ftc.gov/system/files/documents/cases/att_enbanc_5-16585.pdf, última fecha de consulta 22 de febrero de 2019.

Tribunal Europeo de Derechos Humanos, Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, No. 22947/13, 2016, disponible en https://hudoc.echr.coe.int/eng#{%22appno%22:[%2222947/13%22],%22itemid%22:[%22001-160314%22]}, última fecha de consulta 15 de mayo de 2019.